

**ENTERPRISE SECURITY ARCHITECTURE
FRAMEWORK (ESAF) FOR BANKING INDUSTRY**

MAHATHELGE NICHOLAS RUWAN DIAS

**FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR**

2017

**ENTERPRISE SECURITY ARCHITECTURE
FRAMEWORK (ESAF) FOR BANKING INDUSTRY**

MAHATHELGE NICHOLAS RUWAN DIAS

**THESIS SUBMITTED IN FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY**

**FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR**

2017

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: Mahathelge Nicholas Ruwan Dias

Matric No: WHA 100037

Name of Degree: Doctor of Philosophy

Title of Thesis: Enterprise Security Architecture Framework (ESAF) for Banking Industry

Field of Study: Software Architecture (Computer Science)

I do solemnly and sincerely declare that:

- (1) I am the sole author/writer of this Work;
- (2) This Work is original;
- (3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
- (4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
- (5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
- (6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature

Date:

Subscribed and solemnly declared before,

Witness's Signature

Date:

Name:

Designation:

ABSTRACT

Enterprise Security Architecture (ESA) is the practice of translating business security vision and strategy into effective enterprise change by creating, communicating and improving the key security requirements, principles and models that describe the enterprise's future security state and enable its evolution. Besides, ESA must ensure confidentiality, integrity, and availability throughout the enterprise and be aligned with the corporate business objectives. ESA plays a pivotal role in the enterprise nowadays, especially in complex business scenarios and mission critical applications such as banks and financial institutions, where multiple business lines and operations are to be managed and integrated. Currently, practitioners in banks and financial institutions have to use several enterprise architecture (EA) frameworks such as TOGAF and Zachman to model and meet their security requirements. Nonetheless, the frameworks are insufficient to fully cover security attributes and practices needed by the institutions. This research aims at bridging the gaps between existing EA frameworks and the security requirements of banks and financial institutions. Problems related to security in the banking industry were identified using several brainstorming sessions with stakeholders. It was followed by a study on associated work in previous literature, carrying out interviews with industrial experts, and studying relevant case studies to articulate the problem statement, research objectives, and research scope. A systematic literature review (SLR) was conducted that resulted in retrieving 729 research papers published between 1993 and 2015 from 7 databases of which 88 primary studies were selected for further analysis. From the studies, 37 security practices and 17 enterprise securities attributes were identified. A detailed comparison between the practices and attributes with 33 enterprise architecture framework (EAF), 10 security architecture frameworks, and 12 banking frameworks, was conducted. The comparison found out

that on an average, the coverage of enterprise security practices is below 40% by the existing frameworks. A questionnaire survey was carried out with several departmental heads to validate and prioritize the security requirements before a holistic Enterprise Security Architecture Framework (ESAF) for banking software development was designed. The framework is designed based on Sherwood Applied Business Security Architecture (SABSA), Control Objectives for Information and related Technology (COBIT) and National Institute of Standards and Technology (NIST). The proposed ESAF defines six key layers, which include ESA fundamentals, ESA requirements, enterprise security core, enterprise security assets, security integration and security governance. Then the 28 selected security practices in the proposed ESAF are aligned with the 15 selected securities attributes to ensure the ESAF covers a full spectrum of the security practices and attributes. In order to evaluate the comprehensiveness, effectiveness and ease of use of the proposed ESAF in a banking environment, extensive interviews have been performed with 23 industry experts to assess the proposed ESAF. The experts also assessed the ESAF based on some selected scenarios. Results of the evaluation concluded that the proposed ESAF is comprehensive, effective and easy to use.

ABSTRAK

Seni bina keselamatan perusahaan (ESA) adalah amalan menterjemahkan visi dan strategi keselamatan perniagaan menjadi perubahan perusahaan yang berkesan dengan mewujudkan, menyampaikan dan meningkatkan keperluan, prinsip dan model utama keselamatan yang menggambarkan keadaan keselamatan perusahaan pada masa hadapan dan membolehkan evolusinya. Selain itu, ia perlu memastikan kerahsiaan, integriti, dan ketersediaan di seluruh perusahaan itu serta keselarasan ciri-citi tersebut dengan objektif perniagaan korporat. ESA memainkan peranan penting dalam perusahaan pada masa kini, terutamanya dalam senario perniagaan yang kompleks dan aplikasi misi kritikal seperti bank dan institusi kewangan, di mana banyak aliran dan operasi perniagaan perlu diurus dan disepadukan. Pada masa ini, pengamal di bank-bank dan institusi kewangan perlu menggunakan beberapa rangka kerja seni bina perusahaan (EAF) seperti TOGAF dan Zachman untuk memodelkan serta memenuhi syarat-syarat keselamatan mereka. Walau bagaimanapun, rangka kerja-rangka kerja yang sedia ada tidak mencukupi untuk memenuhi sepenuhnya sifat dan amalan keselamatan yang diperlukan oleh institusi. Kajian ini bertujuan untuk merapatkan jurang antara EAF sedia ada dan keperluan keselamatan bank dan institusi kewangan. Masalah yang berkaitan dengan keselamatan dalam industri perbankan telah dikenal pasti melalui beberapa sesi percambahan fikiran dengan pihak berkepentingan. Ia diikuti oleh kajian mengenai kerja yang berkaitan dalam kesusasteraan sebelumnya, menjalankan temu bual dengan pakar-pakar industri, dan kajian kes yang berkaitan untuk menentukan kenyataan masalah, objektif kajian, dan skop penyelidikan. Suatu kajian ilmiah sistematik (SLR) telah dijalankan dan mendapatkan 729 kertas penyelidikan yang diterbitkan di antara 1993 dan 2015 dari 7 pangkalan data, di mana 88 kajian utama telah dipilih untuk analisis lanjut.

Dari kajian ini, 37 amalan keselamatan dan 17 sifat-sifat keselamatan syarikat telah dikenal pasti. Satu perbandingan terperinci antara amalan dan sifat-sifat keselamatan yang telah dikenalpasti dengan 33 EAF, 10 rangka kerja seni bina keselamatan, dan 12 rangka kerja perbankan, telah dijalankan. Perbandingan itu mendapati bahawa secara purata, liputan amalan keselamatan perusahaan adalah di bawah 40% oleh EAF yang sedia ada. Tinjauan soal selidik telah dijalankan dengan beberapa ketua jabatan untuk mengesahkan dan menyusun keperluan keselamatan mengikut kepentingan sebelum satu ESAF holistik bagi pembangunan perisian perbankan direka bentuk. Rangka kerja ini direka berdasarkan Sherwood Applied Business Security Architecture (SABSA), Control Objectives for Information and Related Technology (COBIT) dan National Institute of Standards and Technology (NIST). ESAF yang dicadangkan mentakrifkan enam lapisan utama yang termasuk asas-asas ESA, keperluan ESA, teras keselamatan perusahaan, aset keselamatan perusahaan, integrasi keselamatan dan tadbir urus keselamatan. Kemudian 28 amalan keselamatan yang terpilih dalam ESAF yang dicadangkan diselaraskan dengan 15 sifat-sifat sekuriti yang terpilih untuk memastikan ESAF tersebut meliputi spektrum penuh amalan dan sifat-sifat keselamatan. Dalam usaha untuk menilai kelengkapan, keberkesanan dan kemudahan penggunaan ESAF yang dicadangkan dalam persekitaran perbankan, sesi temu bual yang menyeluruh telah dilakukan dengan 23 pakar industri untuk menilai ESAF yang dicadangkan. Pakar-pakar berkenaan juga menilai ESAF berdasarkan beberapa senario yang dipilih. Keputusan penilaian itu menyimpulkan bahawa ESAF yang dicadangkan itu adalah lengkap, berkesan dan mudah untuk digunakan.

ACKNOWLEDGEMENTS

First and foremost I would like to express my special appreciation and gratitude to my supervisor Assoc. Prof. Dr. Chiew Thiam Kian, for being a tremendous mentor throughout completion of my research. I would like to thank you for always encouraging my research and also motivating me to grow as a research scientist. I deeply appreciate all contributions of his quality time, ideas, guidance, and direction in ensuring successful completion of my Ph.D. I shall treasure your invaluable advice on my research as well as on my career. In addition, I want to thank my committee members, Prof. Dr. Lee Sai Peck and Dr. Su Moon Ting, for the memorable moment of my defence and your invaluable comments and suggestions. I owe my deepest gratitude to my dearest wife, for her caring, love, patience and support throughout the completion of this study. A special thanks to my parents. No words can express to my mother and father for their sacrifices made for me.

TABLE OF CONTENTS

Abstract	ii
Abstrak	iv
Acknowledgements	vi
Table of Contents	vii
List of Figures	xv
List of Tables	xvii
List of Abbreviations	xxi
List of Appendices	xxiii
CHAPTER 1: INTRODUCTION.....	1
1.1 Overview	1
1.2 Background	1
1.2.1 Enterprise Architecture Framework (EAF).....	2
1.2.2 Security Architecture Framework (SAF)	3
1.2.3 Business Security Framework (BSF)	3
1.3 Current Challenges on ESA in the Banking Environment	3
1.4 Problem Statement	6
1.5 Research Objectives	7
1.6 Research Questions	7
1.7 Research Scope.....	8
1.8 Thesis Layout	8
CHAPTER 2: LITERATURE REVIEW	10
2.1 Introduction	10

2.2	Taxonomy of Attacks and Cases	10
2.2.1	Identify ES Practices and ESA Attributes.....	16
2.2.2	Review Design	16
2.2.2.1	SLR Research Questions.....	17
2.2.2.2	Search Process.....	17
2.2.3	Review Conducted	19
2.2.3.1	Inclusion and Exclusion Criteria.....	19
2.2.3.2	Range of Research Papers.....	19
2.2.3.3	Study Selection Procedure	19
2.2.3.4	Quality Assessment.....	20
2.2.3.5	Data Extraction Form.....	21
2.2.3.6	Synthesis	22
2.3	SLR Results	25
2.3.1	Overall Quality Assessment Results	25
2.3.2	Discussion and Highlights on RQ1.1 What are the Effective ES Practices recommended for use in ESAF?	28
2.3.3	Discussion and Highlights on RQ1.2 What are the Effective ESA Attributes that Affect the Effectiveness of ESAF?	33
2.4	Existing Frameworks.....	37
2.4.1	Type of Enterprise and Security Architecture Frameworks.....	37
2.4.2	Overall Analysis and Discussion	38
2.5	Framework Assessment.....	39
2.5.1	Criteria for Framework Assessment in Relation to ES Practices.....	39
2.5.2	Assessment of Generic EAF, SAF and BSF against ES Practices.....	40
2.5.3	Criteria for Framework Assessment in Relation to ES Attributes	42
2.5.4	Assessment of Generic EAF, SAF and BSF against ESA Attributes	42

2.6	Summary	43
CHAPTER 3: RESEARCH METHODOLOGY		44
3.1	Introduction	44
3.2	Problem Identification	45
3.3	Literature Review	46
3.4	Validate ES Practices and ESA Attributes	47
3.4.1	Questionnaire	47
3.5	Frameworks Assessment	48
3.6	ESAF Baseline	48
3.6.1	SABSA	49
3.6.2	COBIT	49
3.6.3	NIST	49
3.7	ESAF Design	50
3.8	ESAF Implementation	50
3.9	ESAF Evaluation	50
3.9.1	Interview	51
3.9.2	Interview Strategy	52
3.9.3	Interview Guidelines	52
3.9.4	Selection of Interviewees	53
3.9.5	Conducting and Transcribing Interviews	53
3.10	Ethical Considerations	53
3.10.1	Reliability and Validity	53
3.10.2	Bias	54
3.11	Summary	54

CHAPTER 4: DESIGN OF ENTERPRISE SECURITY ARCHITECTURE	
FRAMEWORK.....	55
4.1 Introduction	55
4.2 Prioritisation of ES Practices and ESA Attributes	55
4.2.1 Validation by Stakeholders	55
4.2.1.1 Survey Respondents' Demographics	55
4.2.1.2 Age Group.....	56
4.2.1.3 Work Experience.....	56
4.2.1.4 Education Background	57
4.2.2 Validated and Prioritised Requirements.....	57
4.3 Overview of the Proposed ESAF	60
4.4 Detailed EASF.....	61
4.5 Components in the Enterprise Security Architecture Framework for Banking Environment	64
4.5.1 ESA Fundamentals.....	64
4.5.2 Enterprise Security Architecture Fundamental	64
4.5.2.1 Security Principles	64
4.5.2.2 Security Strategy	67
4.5.2.3 Security Roles	67
4.5.2.4 Security Baselines	68
4.5.2.5 Security Concepts	69
4.5.3 ESA Requirements	69
4.5.3.1 Risk Analysis and Assessment.....	69
4.5.3.2 Gap Analysis	70
4.5.3.3 Security Requirements	70
4.5.3.4 Security Threat Models.....	71

4.5.4	Enterprise Security Core	73
4.5.4.1	Application Security	74
4.5.4.2	Data Security	76
4.5.4.3	Network Security	77
4.5.4.4	Infrastructure Security	80
4.5.5	Enterprise Security Assets	81
4.5.5.1	Security Policy	81
4.5.5.2	Security Metrics	81
4.5.5.3	Access Controls	82
4.5.5.4	Security Patterns	83
4.5.5.5	Security Models	83
4.5.5.6	Reference Models	83
4.5.5.7	Security Frameworks	84
4.5.6	Security Integration	84
4.5.6.1	Security Technology	85
4.5.6.2	Secure Integration	86
4.5.6.3	Security Protocol and Binding	87
4.5.7	Security Governance	87
4.5.7.1	Security Mechanism (Control)	88
4.5.7.2	Security Standards, Guidelines and Best Practices	89
4.5.7.3	Law & Regulations	93
4.5.7.4	U.S Laws Pertaining to Hacking	94
4.5.7.5	Regulatory Laws	94
4.5.7.6	Non-U.S. Laws Pertaining to Hacking	95
4.5.7.7	Cyber Laws of Malaysia	95
4.5.7.8	Security Incident Management	97

4.5.7.9 Security Awareness.....	97
4.6 Relationships between Components in the ESAF for Banking Environments	97
4.7 Banking Top Issues and Countermeasures from ESAF	98
4.8 Summary	102

CHAPTER 5: IMPLEMENTATION OF ESAF IN BANKING ENVIRONMENTS..... 103

5.1 Introduction	103
5.2 ESAF Components and Artefacts.....	103
5.3 ESAF Incorporated with SDLC	104
5.3.1 SDLC Phase 1-Initiation	105
5.3.2 SDLC Phase 2- Development and Acquisition.....	106
5.3.3 SDLC Phase 3: Deployment Assessment	108
5.3.4 SDLC Phase 4: Operation /Maintenance	108
5.4 Setting up the ESAF Development Environment.....	110
5.4.1 Setting up the Development Tools	111
5.4.2 Configuring Security Modules and Components.....	112
5.4.2.1 Configuring Identity Access Controls.....	112
5.4.2.2 Access Control Filter (ACF)	113
5.4.2.3 Access Rules	114
5.4.3 Access Control List (ACL)	115
5.4.4 Hashing and Verifying Passwords	115
5.4.5 Safeguarding XSS	116
5.4.6 Generating Pseudorandom Data.....	116
5.4.7 Data Encryption and Decryption.....	117
5.4.8 Data Integrity	118

5.4.9	Cookies Validation, Cache, and Error Handling	118
5.5	Summary	119
CHAPTER 6: RESULTS EVALUATION AND DISCUSSION		120
6.1	Introduction	120
6.2	ESAF Evaluation Criteria.....	120
6.3	Interviewees' Demographics	121
6.3.1	Work Experience.....	121
6.3.2	Geographical Location	122
6.3.3	Interview Methods	122
6.4	Assessment One	123
6.4.1	Comprehensiveness of ESAF.....	123
6.4.1.1	Overall Comprehensiveness of EASF.....	126
6.4.2	Effectiveness of ESAF	127
6.4.2.1	Overall Effectiveness of EASF	129
6.4.3	Ease of Use of ESAF.....	131
6.4.3.1	Overall Ease of Use of EASF	134
6.5	Assessment Two- Based on Scenario.....	136
6.5.1	Summary of the Countermeasures Interview Results	139
6.6	Summary	140
CHAPTER 7: CONCLUSION		141
7.1	Introduction	141
7.2	Contributions and Achievement of the Objectives.....	141
7.3	Limitations and Future Work	143
References.....		145

Appendix A-SLR (Data Source).....	165
Appendix B- Characteristic and Analysis of Frameworks	176
Appendix C- Enterprise Security Practice Publication by Year	184
Appendix D- Security Attributes by Publication by Year	185
Appendix E- Assessment of Frameworks Against ES Practices	186
Appendix F- Scores of Frameworks in relation to ES Practices.....	187
Appendix G- Assessment of Frameworks Against ESA Attributes	188
Appendix H- Scores of Frameworks in relation to ESA Attributes.....	189
Appendix I- Fishbone Diagram	190
Appendix J- Consent Form	191
Appendix K- ESAF Components and Artefacts	192
Appendix L- Interviewees' Responses	212
Appendix M- Evaluation Template (Assessment Two).....	216

LIST OF FIGURES

Figure 1.1: Current Challengers on ESA	4
Figure 2.1: Study Selection Procedure.....	23
Figure 2.2: A Number of Studies by Year	24
Figure 2.3: Qualitative Assessment Score	27
Figure 2.4: Types and Categorisation of EAF	38
Figure 3.1: Research Methodology.....	45
Figure 3.2: Evaluation Flow	51
Figure 4.1: High Level ESA Framework.....	61
Figure 4.2: Components of ESAF.....	62
Figure 4.3: ESA Fundamentals	64
Figure 4.4: ESA Requirements	69
Figure 4.5: Enterprise Security Core	74
Figure 4.6: Application Security.....	74
Figure 4.7: Data Security	76
Figure 4.8: Network Security.....	78
Figure 4.9: Enterprise Security Assets.....	81
Figure 4.10: Security Integration	84
Figure 4.11: Security Technology Stack.....	86
Figure 4.12: Security Governance	88
Figure 4.13: Relationships between Components in the Enterprise Security Architecture Framework for Banking Environments	98
Figure 5.1: SDLC Phase 1 –Initiation.....	106
Figure 5.2: SDLC Phase 2- Development & Acquisition.....	107

Figure 5.3: SDLC Phase 3: Deployment Assessment.....	108
Figure 5.4: SDLC Phase 4: Operation /Maintenance.....	109
Figure 5.5: Yii MVC Framework	110
Figure 5.6: Set up XAMPP Environment	111
Figure 5.7: Yii Environment Set up.....	112
Figure 5.8: Yii Config/Web	112
Figure 5.9: Sample Code of the User Model	113
Figure 5.10: Snippet of Code of Access Control	114
Figure 5.11: Access Control Filters	115
Figure 5.12: Snippet of Code of Hashing	115
Figure 5.13: Snippet of Code of Hashing Validating	116
Figure 5.14: Plain Text Escaping and HtmlPurifier.....	116
Figure 5.15: Snippet of Code of Pseudorandom Code Generation.....	117
Figure 5.16: Code Snippet of Secret Key Generation.....	117
Figure 5.17: Users Database Table	117
Figure 5.18: Helper Function to Generate Secret Key.....	118
Figure 5.19: Cookies Validation, Cache, and Error Handling.....	118
Figure 6.2: Overall Comprehensiveness of ESAF	126
Figure 6.2: Overall Effectiveness of ESAF	130
Figure 6.3: Overall Ease of Use of ESAF	134
Figure 6.4: Summary of Countermeasures Interview Results	139

LIST OF TABLES

Table 2.1: Various Banking Attacks and Reported Cases	11
Table 2.2: Quality Assessment Questions	20
Table 2.3: Quality Assessment Questions Categorisation	21
Table 2.4: Data Extraction Form	22
Table 2.5: Data Source.....	23
Table 2.6: Study Categories by Source Type.....	24
Table 2.7: Qualitative Assessment Results.....	25
Table 2.8: Security Practices.....	29
Table 2.9: Number of Studies by ES Practices	32
Table 2.10: Security Attributes	35
Table 2.11: Number of Studies by ESA Attributes.....	36
Table 2.12: Quality Assessment Questions	39
Table 2.13: Quality Assessment Questions	42
Table 3.1: Research Methodology	44
Table 4.1: Summary of the Survey Respondents.....	56
Table 4.2: Age Group of the Survey Respondents	56
Table 4.3: Work Experience of the Survey Respondents	56
Table 4.4: Educational Background of the Survey Respondents.....	57
Table 4.5: Mapping of Responses to Scores.....	58
Table 4.6: Total Level of Importance	59
Table 4.7: Ranking of ESA Attributes.....	59
Table 4.8: Ranking of ES Practices	60

Table 4.9: Mapping between ESAF Layers and ESA Attributes.....	62
Table 4.10: Mapping between ESAF Layers and ES Practices	63
Table 4.11: Security Roles and Responsibilities.....	67
Table 4.12: Threats and Countermeasures.....	72
Table 4.13: Type of Access Control	82
Table 4.14: Mapping between ESAF Layers and Banking Attacks	98
Table 5.1: Mapping of SDLC Stages with Artefacts	103
Table 5.2:SDLC Phases Notations.....	105
Table 5.3: Identity Interface Methods.....	113
Table 5.4: Access Rules.....	114
Table 6.1: Distribution of Interviewees based on Roles.....	121
Table 6.2: Work Experience of the Interviewees.....	121
Table 6.3: Interviewees' Geographic Locations	122
Table 6.4: Interview Methods Used.....	122
Table 6.5: Interviewees' (CIO/CTO/CA) Response of Comprehensiveness of ESAF	124
Table 6.6: Interviewees' (VP/SVP) Response of Comprehensiveness of ESAF.....	124
Table 6.7: Interviewees' (ESA/SA/TA) Response of Comprehensiveness of ESAF ...	124
Table 6.8: Interviewees' (SME) Response of Comprehensiveness of ESAF	124
Table 6.9: Interviewees' (PM/PMO) Response of Comprehensiveness of ESAF.....	125
Table 6.10: Interviewees' (Technical Lead) Response of Comprehensiveness of ESAF	125
Table 6.11: Interviewees' (BA) Response of Comprehensiveness of ESAF.....	125
Table 6.12: Interviewees' (SE) Response of Comprehensiveness of ESAF	125
Table 6.13: Interviewees' Comments on Comprehensiveness of ESAF	126

Table 6.14: Interviewees' Response (CIO/CTO/CA) of Effectiveness of ESAF	128
Table 6.15: Interviewees' Response (VP/SVP) of Effectiveness of ESAF	128
Table 6.16: Interviewees' Response (ESA/SA/TA) of Effectiveness of ESAF	128
Table 6.17: Interviewees' Response (SMEs) of Effectiveness of ESAF	128
Table 6.18: Interviewees' Response (PM/PMO) of Effectiveness of ESAF	128
Table 6.19: Interviewees' Response (Technical Lead) of Effectiveness of ESAF	129
Table 6.20: Interviewees' Response (BA) of Effectiveness of ESAF	129
Table 6.21: Interviewees' Response (SE) of Effectiveness of ESAF	129
Table 6.22: Interviewees' Comments on Effectiveness of ESAF	130
Table 6.23: Interviewees' Response (CIO/CTO/CA) of Ease of Use of ESAF	132
Table 6.24: Interviewees' Response (VP/SVP) of Ease of Use of ESAF	132
Table 6.25: Interviewees' Response (ESA/SA/TA) of Ease of Use of ESAF	132
Table 6.26: Interviewees' Response (SMEs) of Ease of Use of ESAF	132
Table 6.27: Interviewees' Response (PM/PMO) of Ease of Use of ESAF	133
Table 6.28: Interviewees' Response (Technical Lead) of Ease of Use of ESAF	133
Table 6.29: Interviewees' Response (BA) of Ease of Use of ESAF	133
Table 6.30: Interviewees' Response (SE) of Ease of Use of ESAF	133
Table 6.31: Interviewees' Comments on Ease of Use of ESAF	133
Table 6.32: Interviewees' Response of Malware Attack Countermeasures from ESAF	136
Table 6.33: Interviewees' Response of DDOS Countermeasures from ESAF	137
Table 6.34: Interviewees' Response of Injection Flows Countermeasures from ESAF	137
Table 6.35: Interviewees' Response of Social Engineering Countermeasures from ESAF	137

Table 6.36: Interviewees' Response of Network Eavesdropping Countermeasures from ESAF.....	137
Table 6.37: Interviewees' Response of Data Disruption Countermeasures from ESAF	138
Table 6.38: Interviewees' Response of Identity Theft Countermeasures from ESAF .	138
Table 6.39: Interviewees' Response of XSS Countermeasures from ESAF	138
Table 6.40: Interviewees' Response of Security Misconfiguration Countermeasures from ESAF	138
Table 6.41: Interviewees' Response of Phishing Countermeasures from ESAF.....	138
Table 6.42: Scenario Responses	139

LIST OF ABBREVIATIONS

AERA	:	Application of Enterprise Reference Architecture
AFUCIFS	:	Architectural Framework for User-Centric Information-Flow Security
AGATE	:	France DGA Architecture Framework
ARIS	:	Architecture of Integrated Information Systems
BBSF	:	Biometrics in Banking Security Framework
BHOs	:	Browser Helper Objects
BSF	:	Banking Security Architecture
C4ISR	:	Command Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CIMOSA	:	Computer Integrated Manufacturing Open System Architecture
COBIT	:	Control Objectives for Information and Related Technology
CRD	:	Centre for Reviews of Dissemination
DODAF	:	Department of Defence Architecture Framework
DARE	:	Database of Abstracts Reviews of Effects
E2AF	:	Extended Enterprise Architecture Frameworks
EA	:	Enterprise Architecture
EABOK	:	Enterprise Architecture Body of Knowledge
EAL	:	Evaluation Assurance Level
EAP	:	Spewak's Enterprise Architecture Planning
EIF	:	European Interoperability Framework
EISA	:	Enterprise Information Security Architecture
ES	:	Enterprise Security
ESA	:	Enterprise Security Architecture
ESAF	:	Enterprise Security Architecture Framework
FEAF	:	Federal Enterprise Architecture Framework
FEAFRM	:	Federal Enterprise Architecture Reference Model
FESF	:	Fujitsu Enterprise Security Architecture
FGISBS	:	Framework for Governance of Information Security in Banking System
FSPAT	:	Framework for Security and Privacy in Automotive Telematics
GEA	:	Government Enterprise Architecture
GEAF	:	Gartner Enterprise Architecture Framework
GERAM	:	Generalised Enterprise Reference Architecture and Methodology
GRAI	:	Graphs with Results and Actions Inter-related
GIM	:	GRAI Integrated Methodology
JTA	:	Joint Technical Architecture
IAF	:	Integrated Architecture Framework
IBF	:	Internet Banking Framework
IDEAS	:	International Defence Enterprise Architecture Specification
IPS	:	Intrusion Prevention Systems
ISM	:	Information Security Framework

ITSAF	:	Insider Threat Security Architecture Framework
DNDAF	:	Department of National Defence and the Canadian Forces Architecture Framework
MODAF	:	UK Ministry of Defence Architecture Framework
MCMC	:	Malaysian Communications and Multimedia Commission
NATOAF	:	NATO Architecture Framework
NIHEAF	:	NIH Enterprise Architecture Framework
NISTEA	:	NIST Enterprise Architecture
OBASHI	:	OBASHI Business & IT Methodology and Framework
OBSFC	:	Online Banking Security Framework for Cross-cultural
OSA	:	Open Security Architecture
PCI-DSS	:	Payment Card Industry Data Security Standard
PERA	:	Purdue Enterprise Reference Architecture
PEEEAMB	:	Performance Evaluation on End-to-End Security Architecture for Mobile Banking System
PFIRIES	:	Policy Framework for Information Security
PKIMBSF	:	Public Key Infrastructure for Mobile Banking Security Framework
RM-ODP	:	Reference Model of Open Distributed Processing
SABSA	:	Sherwood Applied Business Security Architecture
SAGA	:	Standard and Architectures for eGovenment Application
SAML	:	Security Assertion Mark-up Language
SFMB	:	Security Framework for Mobile Banking
SIEMF	:	Security Information and Event Management Framework
SLR	:	Systematic Literature Review
SMDAF	:	Security Management Development Architecture Framework
SMEs	:	Subject Method Experts
SOA-EAF	:	Service Oriented Architecture Enterprise Architecture Framework
SQIBUCF	:	Service Quality in Internet e-banking User-based Core Framework
SSL	:	Secure Sockets Layer
TAFIM	:	Technical Architecture Framework for Information Management
TEAF	:	Treasury Enterprise Architecture Framework
TISAF	:	Treasury Information System Architecture Framework
TLS	:	Transport Layer Security
TRM	:	Technical Reference Model
TOGAFTM	:	The Open Group Architecture Framework
USEUBIEF	:	Usability and Security in EU E-Banking Systems Towards an Integrated Evaluation Framework
VPN	:	Virtual Private Network
WS-security	:	Web Service Security
ZEAF	:	Zachman Enterprise Architecture Framework

LIST OF APPENDICES

Appendix A: SLR (Data Source)	165
Appendix B: Characteristic and Analysis of Frameworks	176
Appendix C: Enterprise Security Practice Publication by Year	184
Appendix D: Security Attributes by Publication by Year	185
Appendix E: Assessment of Frameworks Against ES Practices	186
Appendix F: Scores of Frameworks in Relation to ES Practices	187
Appendix G: Assessment of Frameworks Against ESA Attributes	188
Appendix H: Scores of Frameworks in Relation to ESA Attributes	189
Appendix I: Fishbone Diagram	190
Appendix J: Consent Form	191
Appendix K: ESAF Components and Artefacts	192
Appendix L: Interviewees' Responses	212
Appendix M: Evaluation Template (Assessment Two)	216

CHAPTER 1: INTRODUCTION

1.1 Overview

This chapter details a comprehensive discussion of the overview of the enterprise security architecture, background of the study, which includes challenges faced by practitioners and banking users. Furthermore, it elaborates the purpose, motivation, objective, and scope of this research. Lastly, it concludes with research impediments and layout of the thesis.

1.2 Background

Presently in the banking industry, banks depend highly on financial systems for their day to day operations. Basically, financial systems are all embracing with a wide range of financial suites, with coverage of complete core and retail banking processes such as managing customers' accounts, core processing systems, financial accounting, lending and compliance, collateral management, loan and payment service, and risk analysis and management. Nevertheless, these financial suites send back and forth the most vital financial and personal data such as bank account details, personal identification numbers and details, social security numbers, credit card payment numbers, high-value confidential information between businesses and individuals. Furthermore, these information exchanges allow banks to deliver high level services and give an opportunity to penetrate emerging markets. However, it has also created vulnerabilities including security breaks and data outflows and leakages. Ultimately, bankers have to accept the high risk of data leakages on daily operations. These major drawbacks can occur while transmitting data to customers, merchants, government bodies, retailers and other third party institutions, while it is being processed (Tahajod, Iranmehr, & Darajeh, 2009). Biswas, Taleb, & Shinwary (2011) stated that the banking environment is obviously doubtful that many things could fail with one customer.

According to Randazzo, Keeney, Kowalski, Cappelli, & Moore (2005), poor security of enterprise architecture (EA) design combined with unscrupulous system implementation of the financial system has obstructed the entire financial system. The financial institution's reputation is thus jeopardised, and they have to bear serious liquid damage. It is important for financial institutions to have an enterprise security architecture framework (ESAF) to overcome these security challenges.

With the proliferation of information technology being pervasive, enterprise security architecture is playing a pivotal role in existing enterprise architecture perimeters. This is even obvious in complex business scenarios and operations and mission critical applications such as banks and financial institutions, where multiple business lines and operations are to be managed and integrated that was uncommon in the past decades. Information security is at the centre-stage to technology-related challenges. It has various aspects; nevertheless the fundamental goal is to sustain the confidentiality, integrity, and availability of an institution's information and digital assets. Any integrity issues facing these factors can critically expose an institution to both legal and reputational risk (Murphy, Boren, & Schlarman, 2000).

1.2.1 Enterprise Architecture Framework (EAF)

An enterprise architecture framework (EAF) maps all of the software development processes within the enterprise and how they relate and interact to fulfil the enterprise's mission. It provides organizations with the ability to understand and analyse weaknesses or inconsistencies to be identified and addressed. There are a number of already established EAF in use today; some of these frameworks were developed for very specific areas, whereas others have broader functionality (Urbaczewski & Mrdalj, 2006).

1.2.2 Security Architecture Framework (SAF)

A security architecture framework is a framework that allows enforcement of coexisting application and environment specific security policies by applying security mechanisms in a consistent manner (Hartig et al., 1993).

1.2.3 Business Security Framework (BSF)

BSF concentrates on presenting a security framework for Internet banking based on discovering and defining security requirements for Internet banking such that the transactions being conducted are secured within their respective environments (Hutchinson et al., 2003).

In this research, the researcher seeks to define enterprise security architecture (ESA) covering its various facets that encompasses the underlying IT technical components in a highly cohesive structure. Once such a structure is in place, it enables the organisation to find its business, IT and compliance components that must be present to attain the key objectives and goals, and provide key stakeholders with the opportunity to plan and prioritise strategic IT security investments important to technological implementations, process enhancements and user awareness initiatives (Tahajod, Iranmehr, & Darajeh, 2009).

1.3 Current Challenges on ESA in the Banking Environment

The current security challenges in the context of banking industry are highlighted in Figure 1.1.

Security Model	Business Process & Requirement	Security Fundamental	Enterprise Secure Architecture Core	Governance
Less coverage on complex issues	Rapid change of environment and technology	Security principles not established and not officially acknowledge	Lack of a global approach	Need for security infrastructure governance
No holistic view	Organizations' growing dependence on IT security risks increasingly contribute to operational and reputational risk			Standards and security compliances are complex and hard to understand
Cater few deployment scenarios	Architecture language is not adapted to provide support for security analysis			It's not explained how to successfully implement each security control
Add too much details				

Figure 1.1: Current Challengers on ESA

Nagaratnam et al. (2002), provides a detailed security architecture to integrate security models, mechanisms, protocols, and platforms to operate securely. As claimed by Demchenko, De Laat, Koeroo, & Groep (2008), security models have limited scope, applicability and coverage. Furthermore, they are only catered for a few deployment scenarios. They fail to harness pertinent issues like community organisation, site access integration and resistance with operating platforms, proper provisioning cross-domain resources, or covering over the community. There is no holistic “security view” from the existing EAFs. Moreover, they are unable to detect architectural restrictions in resolving identity management control and governing policy and enforcement scenarios.

Oda, Fu, & Zhu (2009) claimed that in order to improve the existing security architecture, it is recommended that the key stakeholders should participate in the development and that the important players should work in tandem to analyse both the information and system security requirements. Shariati, Bahmani, & Shams (2011) have concluded that none of the existing ESAFs, even the ones that have taken a holistic

or a practical approach, have explored interoperability in ESA clearly. They recommended that the requirements which are generic to both interoperability and security ought to be pulled out and ESAFs must capture those requirements.

Along with Fitzgerald (1994), during the reviewing of informational security, it is found that often times the organisation may not have the basic foundation of principles of information tenure and custodianship. Often, these principles were not officially acknowledged to proprietors, or to the user departments. As a result of this, the service providers interpret differently on the security needs. Gutierrez, Fernandez-Medina, & Piattini (2005) highlighted that the lack of a global approach still exists in constructing security architectures for Web Service based systems.

Based on Murphy et al. (2000), ESA defines information security strategy as a layered architecture that comprises policy, standards with the interlinking of procedures. They have further stressed that ESA is imperative to an effective information security program, in the absence of which governance of the infrastructure and security would be a herculean task to achieve. As highlighted by Tahajod et al. (2009), the security architecture blueprint is a tool to plan the organisation's future security. Typically, it gives a mechanism to map to the organisation's objective for secure logical view. It includes security policies and concepts, architecture, and security domains and risk management. According to Kim & Cha (2012), however, industry standards and existing security models are very complicated and it is difficult to comprehend and implement them. In addition, they are unable to provide adequate guidelines to implementing the standard in real situation.

1.4 Problem Statement

Currently, the IT industry is littered with many EA frameworks but their approach and level of coverage are different. Some frameworks are designed for specific industries while others are created for the general audience. The researcher has found several gaps in the existing EA frameworks that are currently used by the industry. For example, TOGAF and Zachman frameworks are the two most comprehensive frameworks being implemented in the industry. However, they can still be improved upon in terms of the security aspects. Although most of the frameworks provide different panoramic viewpoints, they are still lacking in proper security coverage. Furthermore, certain frameworks do not visibly map the objectives with the viewpoints and deliverables, while others are lacking of coverage on the ESA modules.

The architectural frameworks that the researcher has examined can be classified into three categories: EAF, SAF, and BSF. The generic enterprise architecture frameworks (EAF) are lack of guidance for security implementation. They mainly focus on EA fundamentals rather than security and not specifically targeted at the banking domain. On the other hand, existing security architecture frameworks (SAF) support security implementation in the organisations but are still not comprehensive enough to cover all the enterprise security (ES) practices and enterprise security architecture (ESA) attributes. They do not address the banking domain too. Existing banking security frameworks (BSF) although focus on the banking domain, but there is no single BSF which is comprehensive enough to support the banking domain at the organisational level like a SAF does. Therefore, a comprehensive framework that is effective enough to address security requirements of the banking domain, acts as a single reference model for security implementation of an organisation, and robust enough against security attacks and threats in the banking domain, is in need.

1.5 Research Objectives

The purpose of this study is to establish and enable an ESAF for banking industry. This would help banking practitioners to adapt the ESAF and implement systems based on industry needs. This would also satisfy the requirements of the banking governing body and those who seek for a comprehensive ESAF. Overall, the ESAF would benefit the industry practitioners and the banking industry as a whole. In order to provide a comprehensive ESAF, the researcher must have some conception of what are aspects to focus on while building the ESAF. Therefore, the study aims to realise the following objectives:

- To identify the ESA attributes and ES practices to be incorporated into a comprehensive and effective ESAF that is easy to use by the practitioners.
- To develop an ESAF that incorporates the defined ESA attributes and ES practices.
- To evaluate the comprehensiveness, effectiveness and ease of use of the proposed ESAF for the banking environment.

1.6 Research Questions

In order to meet the purpose and objectives of the study, the following research questions were used to frame this study.

- RQ1: What are the requirements of a comprehensive and effective ESAF?
(Refer to Section 2.3)
- RQ2: What are the existing frameworks, particularly the security frameworks for banking environments? (Refer to Section 2.4)

- RQ3: What is the solution to fill the gap between existing frameworks and ESA attributes and ES practices? (Refer to Chapter 4)

The answers to the above questions would be very beneficial to banking software developers, vendors and the bankers who are responsible for enabling security in enterprise architecture in banking environment.

1.7 Research Scope

The research scope is focused on the banking domain and ESAF.

- This research is determined to minimise the top ten data breaches in banking industry as explained in Section 2.2.
- The proposed layered architecture covers key areas of ESAF such as ESA fundamental, ESA requirements, enterprise architecture core, enterprise security assets, security integration and security governance.
- The proposed ESAF is designed for small and medium bankers who intend to develop e-Banking solutions.

1.8 Thesis Layout

Chapter 1- In this chapter, the researcher presents an overview of the research, which includes the importance of the research and its background, problem statement and motivation of the study. Moreover, it further elaborates the research scope, and objectives, and concludes with the thesis layout.

Chapter 2- In this chapter, the researcher presents a systematic literature review which identifies the ES practices and ESA attributes. The researcher has carried out a comprehensive review of the existing frameworks. After identifying the ES practices,

ESA attributes and existing frameworks, the researcher examines the coverage of the ES practices and ESA attributes in the frameworks. Finally, the researcher discusses the identified gaps in the existing frameworks and potential improvements.

Chapter 3- In this chapter the researcher presents the research methodology for carrying out the research work. It is a three-phase approach which elaborates the early stage of the study, design and implementation, and evaluation of the outcome. The methodology systematically elaborates the enterprise security requirements gathering, requirement validation, ESA design, and evaluation. Besides that, it discusses the reliability and validity, and ethical consideration of the study.

Chapter 4- In this chapter, the researcher presents the design details of the proposed ESAF for the banking environment, which include the major actors and components for enterprise architecture security in the banking environment.

Chapter 5- This chapter provides the detailed implementation of the proposed ESAF for the banking environment.

Chapter 6- In this chapter, the researcher describes the evaluation criteria that were used for evaluating the proposed ESAF for the banking environment.

Chapter 7- In this chapter, the researcher describes the research findings and gaps, and contributions of the study. The researcher further discusses the limitations of the study and future research areas.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter provides the detailed review and critical analysis of the literature related works on ESA. It is essential to gather related work in the past, comprehend and critically analyse the current problems and challenges in the ESA domain before one can suggest an ESAF. There are three parts in this chapter, which include identification of top ten security attacks and threats, a systematic literature review (SLR) and a review of existing frameworks, including of EA, SAF, banking security framework BSF and ESAF. The SLR was used to identify all the ES practices and ESA attributes. It presents all the ESA concepts including definitions, ESA models, reference models, essential characteristics, actors and drivers for ESA adoption. Finally, the researcher compares the SLR finding on ES practices and ESA attributes with the existing frameworks.

2.2 Taxonomy of Attacks and Cases

Many potential threats lurk in the dark abysses of the information superhighway of the internet such as viruses, worms, Trojans and botnets. A botnet is a malicious software program which is programmed in such a way that it creates a cluster of infected machines and transmits user activities to its controller. If not rectified in time, it sometimes results into a Distributed Denial of Service (DDOS) attacks such as credential theft, click fraud, spamming and bank account thefts (Soltani, Seno, Nezhadkamali, & Budiarto, 2014). In 2014, cybercriminals continued to steal private information on an epic scale, by direct attack on institutions such as banks. According to Wood et al. (2014), the exposure of financial information grew from 17.8% to 35.5% in 2014, the largest increase within the top 10 list of information types exposed. Likewise, a recent CIGIIPSOS poll surveying over 23,000 respondents in 24 countries found that 64% of respondents were more worried about their online privacy compared to one year

ago, and 78% of respondents were concerned about criminal hackers stealing their banking information (Jardine, 2015).

The number of breaches increased by 23% and attackers were responsible for the majority of these breaches. At 49%, the majority of breaches were caused by attackers, up from 34% in 2013. Finance was the fourth targeted sector of 2014, with 13% of targeted attacks designed for this sector (Wood et al., 2014). According to Sullivan (2014), merchants suffered serious data security breaches in years 2008 to year 2013. Out of these data breaches, there were 1,489 publicly disclosed breaches, 13 were mega breaches that exposed at least 862 million records. During the same period, Depository Financial Institutions (DFI) suffered 207 publicly disclosed breaches that exposed 6 million records. This incidence rate that is calculated as the number of data breaches divided by the number of merchants or the DFIs is only 0.02% for the merchants (Sullivan, 2014). In Table 2.1, the researcher provides an exploratory descriptive analysis of various banking attacks and their cases.

Table 2.1: Various Banking Attacks and Reported Cases

Type of Attack	Reported Financial Attacks
<p>1. Malware Attack</p> <p>Computer systems that can be breached without the consent using any malicious software are categorized as malware attacks. Malware includes computer-viruses, worms, Trojan horses and spyware (Malin, Casey, & Aquilina, 2008).</p> <p>a) Trojan Horse</p> <p>Unwanted applications that can grant access of the computer system to the hackers are categorized as Trojan horse. They come as a part of legitimate software</p>	<p>In 2013, malware contributed to about 6.2% encountered financial attacks. It is a 1.3 % increase in comparison with 2012. In a similar manner, cyber-attacks involving malware to hijack financial data has increased in number by 27.6% thus reaching 28,400,000 and the number of users affected by malware tops 3,800,000 in total, resulting an 18.6% increase year on year. Out of all the finance-related malware, tools that demonstrated the most dynamic development are associated with Bitcoin and Zeus a malware dominates them all (Etaher, Weir, & Alazab 2015).</p> <p>Gartner have estimated the losses, just</p>

bundles and enter the system seamlessly (Szor, 2005).

b) Virus

Viruses are computer programs that have the capability to replicate itself and spread throughout the systems. Although initially they seem to be harmless to the users, their negative impact may vary from reducing the computer's processing speed to corrupting the RAM and hard disk. E-mails and file-sharing have become the main sources for the spreading of viruses (Szor, 2005).

c) Virus Hoax E-mail

Hoaxes are e-mail warning about viruses, designed for the purpose of disrupting businesses and to cause concern. Caution should be taken before avoiding them completely, as they may be legitimate at time (Jakobsson & Myers, 2006, Hinde, 2002). Intruders use this strategy in such a way that the user is misled to update their PayPal financial details on their hoax websites (Dhinakaran, Nagamalai, & Lee, 2011).

d) Worm

Worms are mainly created to consume the host system's resources such as processing time, storage and networked appliances. Unlike viruses, these malicious applications replicate themselves until they have consumed all the storage capacity of the computer including the networked systems and result in crashing the web server and interrupting the internet access in the network (Nazario, 2004).

e) Spyware

A spyware is a computer program code which once installed on the operating system transmits the user information to the spyware creator (Giri & Singh, 2014).

While a virus program causes operating system to malfunction, a spyware is more lethal in nature. It transmits user activity

in the US, were over USD\$7.5 Billion in the three years to September 2008 because of phishing attacks (Petty & Stevens 2009). Internet bank phishing began in 2003. The first Internet bank to be attacked was the Commonwealth Bank of Australia in March 2003 (McCombie & Pieprzyk, 2010).

Recent attacks on banking websites by the torpig virus that steals financial details such as bank account details and credit card data by emulating the users keystrokes. The hackers then manage to steal user credentials (Soltani et al., 2014).

In between year 2009-2010, the worm sabotaged 100 thousand hosts in several countries, 60% of them were in Iran (Rid, 2012).

<p>like keystroke actions on websites (that could be banking or social) to its perpetrators (Khattak et al., 2014).</p> <p>f) Keystroke Capturing / Logging</p> <p>A computer keyboard's keystrokes can be captured by using specialized software. This method is called keystroke logging. It is used by people with malicious intent to capture sensitive user information (Jesudoss & Subramaniam, 2014).</p>	
<p>2. Distributed Denial of Service Attacks</p> <p>Distributed Denial of Service Attacks (DDoS) are attempts to interrupt computer machines or network infrastructure to make them inaccessible or unreachable within a specific time frame to their users (Seo, Lee, & Perrig, 2013).</p>	<p>In a DDoS attack on credit card companies such as Master Card, Visa and Post Finance in year 2010 bringing down the operations. In the year 2012, nine major United States (Bank of America, HSBC, Citi, Fargo, Bancorp, PNC, CapitalOne, Fifth Third & BB&T) banks were affected because of DDoS attacks (Zargar, Joshi, & Tipper, 2013).</p>
<p>3. Injection Flows (SQL, OS and LDAP)</p> <p>It takes place when untrusted data is sent along with command or query to an interpreter. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data (Atashzar, Torkaman, Bahrololum, & Tadayon, 2011).</p>	<p>The SQL injection attacks on Dexia Bank Belgium (2008 to 2009) ended up with \$1.7 million in loss due to a malware on network that helped to rob many of card numbers. The Global Payment Systems attack (2011 to 2012) has resulted a theft of more than 950,000 card numbers and losses of approximately \$92.7 million (Reedy & Buzzeo, 2013).</p>
<p>4. Social Engineering</p> <p>It allows illicit access to a system to achieve explicit objective. Following lists social engineering attacks:</p> <p>a. Lottery Fraud</p> <p>The intruders approach the consumers through email and advise them of a lottery prize and in exchange their personal/banking details are requested along with a processing fee. Thus it leads to further fraud with the obtained data (Overton, 2007).</p>	<p>A majority of the lottery scams are perpetuated by Nigerians for 419 Advance Fee fraud (AFF). A 2007 statistic indicates that user reaction on scam emails is 2.5% (Ampratwum, 2009; Tive, 2006).</p> <p>Advance Fee fraud, \$12.7 billion of losses were reported in 2013 and over \$82 billion to date (Ampratwum, 2009).</p> <p>The Australian Crime Commission report, Organized Crime in Australia 2011, estimates that millions of dollars have been lost in Australia to such scams. According to AUSTRAC's 2010 typologies and case studies report, Australian victims lost AUD21.5 million</p>

<p>b. Advance Fee Fraud</p> <p>In this scenario, emails are spawned offering the end user a generous offer to help move a large amount in US dollars. This amount is said to be corporate profits, unspent government funds, or unclaimed money to a deceased person. A small advance fee will be requested for the transaction, which causes a loss.</p> <p>c. Boiler Room Attack</p> <p>Bogus or illegitimate sellers attempt to sell the share or stocks to targeted users. In case, the victim has accepted the offer, the fraudster ask them to pay the money and compensation is not allowed (Stevenson, 1998).</p> <p>d. Pharming</p> <p>A technique adopted by fraudsters to gather personal data from users through a fake website which is similar to the original website. These fake websites are created with a hope that the consumers may visit by mistake or make typos in website address. In extreme cases the hacker may also redirect from the genuine website to sham site (Friedrichs, 2008).</p>	<p>on this scam (Delrue, 2014).</p> <p>Phaming attack reported, attackers spotted the defects in internet wireless routers of networking companies like Asus, D-Link, Cisco, Linksys, Micronet, Netgear, Tenda, TP-Link and launched a pharming attack on SOHO that attacked over three hundred thousand devices (Heffner & Yap, 2009).</p>
<p>5. Network Eavesdropping</p> <p>Attackers are targeting the network layer while data transmission is in progress and they use sophisticated techniques like sniffing to trap the data packets travelling in the network tunnel (Wu, Chen, Wu, & Cardei, 2007).</p>	
<p>6. Data Disruption Attacks</p> <p>The intruders attempt to disrupt targeted operational systems and create mass destruction to the daily business operations. A moral behind the attempt is to make sure within a time frame, data utilization back is dropped to (Zero Geers,</p>	<p>2013 reported a massive disruption attacks from South Korea which series of malware attacks against several of the country's banks (Shinhan Bank, Nonghyup Bank and Jeju Bank) and it had disrupted user access, and interrupted banking transactions and wiped PCs (Casey, 2006; Sherstobitoff & Itai Liba,</p>

2010).	2013).The Estonian banking operation was disrupted for one and a half hours in year 2007 due to data disruption attack (Rid, 2012).
<p>7. Identity Theft</p> <p>In an identity theft, a fraudster impersonates as someone else from whom critical information is obtained. This information is then illegally used to apply credit or gain rights toward banking accounts (Camp & Johnson, 2012).</p>	<p>According to statistics, in identity theft victims, 37% are credit card account holders, 40% is misused information and 85% is the misuse of credit card and bank account data. Also as per the report of the department of equity, cases of identity theft lost \$24.7 billion in revenue in the year 2012 (Sullivan, 2014).</p>
<p>8. Broken Authentication & Session Management and Cross-Site Scripting (XSS)</p> <p>One of the critical aspects of security measure is ‘Authentication’. It includes major aspects of user active sessions and authentication modules. However, even the most fool-proof authentication systems can be breached either by DDoS attacks or by “walk by” attacks. One of the ways to avoid such attacks should be the user must be required to authenticate themselves at regular intervals of time during their sessions (Bailey, Okolica, & Peterson, 2014). The XSS attacks allow intruders to steal victims’ sessions or redirect them to malicious sites. This occurs when the application functions which are associated with authentication and session management are not properly implanted in the system. It does allow hackers to reveal users’ personal data such as passwords and session tokens (Fogie, Grossman, Hansen, Rager, & Petkov, 2011).</p>	<p>Based on statistical reports, FBI/CSI confirmed that 92 percent of victims reported more than 10 broken authentications in banking websites. In another statistical study conducted by the Gartner group showed that 75 percent of the attacks were on internet based web applications. An Acunetix audit result verbally expresses “on average 70% of websites are at earnest and immediate risk of being hacked and 91% of these websites contained some form of website susceptibility, ranging from the more solemn ones such as SQL Injection and Cross Site Scripting (XSS”. These assailment fundamentally capitalize on infelicitous applications (Jose Fonseca, Vieira, & Madeira, 2007).</p>
<p>9 Security Misconfiguration</p> <p>Most of the web applications are not properly configured according to the standards or best practices. Moreover, these sensitive data, including credit card details, banking information, and user</p>	<p>2013 reported, malicious code called as WIN 32/Caphaw attacked that target the major European banks. The attackers were using webinjects to take control over the banking user’s web browser session.</p>

authentication credentials require extra protection to avoid modification on the fly (Seo, Kim, Cho, & Cha, 2004)	Hsbc.co.uk, barclays.co.uk, santander.co.uk, bankofscotland.co.uk, natwest.co.uk, rbs.co.uk, poste.it, uncredit.it, cedacri.it, and fineco.it are some of the banking domains from United Kingdom and Italy which were attacked.
<p>10 Phishing</p> <p>Phishing starts with an e-mail that claims to be from a valid banking or online retail organization, Usually the content of the email will request the consumers to update or verify their personal information and e-banking details. Sometimes the e-mail will also contain a link to a fake website to spoof the user. By clicking the link the user may accidentally install spyware to their computer which will log the users' future internet usage Baker, (Tedesco, & Baker, 2008).</p>	<p>According to statistics, the number of phishing attacks has steadily grown from 7,197 as reported in December, 2005 to a whopping 28,531 in December 2006. As per the Gartner report (Ludl, McAllister, Kirda, & Kruegel, 2007) financial losses have escalated to \$2.8 billion in year 2007, and year 2013 reported that global loss of over \$1.6 billion (Konradt, Schilling, & Werners, 2016).</p>

2.2.1 Identify ES Practices and ESA Attributes

A systematic literature review (SLR) based on the guidelines proposed by Kitchenham et al. (2009) and Da Silva et al. (2011) was carried out to identify major ES practices and ESA attributes. There are three consecutive stages in a SLR process: planning, execution, and result analysis, with a fourth stage to store the results at the end of each stage, i.e. packaging. The execution of the entire literature review process is verified by two checkpoints.

2.2.2 Review Design

This section describes the foundation of this review by defining SLR research questions and search keywords.

2.2.2.1 SLR Research Questions

The ESAF consists of two key requirements that are ES practice and ESA attributes. The ES practices are a list of best practices that protect the enterprise security. Likewise, ESA attributes are a list of security quality attributes of an ESA that adds value to secure solutions. This SLR was intended to identify the ES practices and ESA attributes that affect the comprehensiveness and effectiveness of an ESAF. The SLR research questions that the researcher intended to answer in this research are as follows:

RQ 1.1: What are the effective ES practices recommended for use in an ESAF?

RQ 1.2: What are the effective ESA attributes that affect the effectiveness of an ESAF?

The researcher derived the two SLR research questions based on RQ1 stated on Page 7, i.e. what are the requirements of a comprehensive and effective ESAF?.

2.2.2.2 Search Process

The databases used to perform this SLR were ACM Digital Library, IEEE Xplore, Science Direct, Springer Link, Emerald, and Google Scholar. The researcher has chosen these databases as the main sources since they predominantly address the ESA domain compared with other databases and sources. Besides, an additional reference mechanism was added to ensure that all the relevant literature was properly analysed. These search results were checked for relevance in the journals' titles, specific keywords and abstracts. The search was conducted between August and September 2015. The researcher used a set of simple search strings and aggregated the outcome from each of the searches from the sources:

- a) "Enterprise security architecture".

- b) “Enterprise security architecture” AND “framework”
- c) “Enterprise security architecture” AND “practice”.
- d) “Enterprise security architecture” AND “model”.
- e) “Enterprise security architecture” AND “development”.
- f) “Enterprise security architecture” AND “process”
- g) “Enterprise security architecture” AND “best practices”
- h) “Enterprise security architecture” AND “attributes”
- i) “Enterprise security architecture” AND “management”.
- j) “Enterprise security architecture” AND “risk”.
- k) “Enterprise security architecture” AND “roles”.
- l) “Enterprise security architecture” AND “governance”.
- m) “Enterprise security architecture” AND “integration”.
- n) “Enterprise security architecture” AND “requirement”.
- o) “Enterprise security architecture” AND “reference model”.
- p) “Enterprise security architecture” AND “guidelines”.
- q) “Enterprise security architecture” AND “baseline”.
- r) “Enterprise security architecture” AND “principles”.
- s) “Enterprise security architecture” AND “domain”.
- t) “Enterprise security architecture” AND “design”.
- u) “Enterprise security architecture” AND “standard”.
- v) “Enterprise security architecture” AND “compliance”.
- w) “Enterprise security architecture” AND “design”.
- x) “Enterprise security architecture” AND “implementation”.

2.2.3 Review Conducted

The section defines the review protocol for conducting the SLR. The SLR review protocol refers to structure and rules of conducting the review.

2.2.3.1 Inclusion and Exclusion Criteria

The inclusion criteria for literature were conference proceedings, journal papers, chapters from books and e-books found by the search terms. Only studies that focused on ESA frameworks and model, security frameworks and security practices, model related to EASF, and security attributes were included.

The exclusion criteria for literature were studies not written in English, studies with no relevance to the research questions, duplicated articles (by title or content) and short papers (e.g., brochures)

2.2.3.2 Range of Research Papers

The literature review performed covers published research from year 1993 (initial publication of security architecture was found in 1993) to year 2015 (when the search was done).

Those identified papers were prudently categorised by author names, year of publication and journal/proceeding titles, proposed security attributes, proposed security practices, type of security concerns, and type of ESA addressed.

2.2.3.3 Study Selection Procedure

The planned selection process for this study was divided into two: initial selection of published literature that could sufficiently meet the search strings or selection criteria based on its title, abstract, and keywords. This is followed by selecting from the initial selection of published literature by reading the complete text of the paper. The primary

reviewer would conduct the selection process. Nevertheless, a re-evaluation of the selected studies is conducted by randomly selecting the primary sources so that any biases can be avoided or mitigated. The selection of studies was performed through the following processes:

- Search in database to identify relevant studies using search keywords
- Exclude studies based on the exclusion criteria
- Exclude irrelevant based on title and abstract
- Exclude irrelevant based full text
- Evaluation by supervisor
- Re-evaluation in random

2.2.3.4 Quality Assessment

In order to evaluate the quality of the selected papers, the researcher followed the Centre for Reviews and Dissemination (CRD) of Database of Abstracts of Reviews of Effects (DARE) criteria elucidated by Keele (2007). DARE focuses mainly on systematic reviews that evaluate the effects of healthcare interventions and the delivery and organization of health services. It elaborated the following criteria such as inclusion and exclusion, search adequate, synthesised process etc. The researcher then designed the following questions (Table 2.2) for quality assessment.

Table 2.2: Quality Assessment Questions

QA	Quality Assessment Questions
QA1	Does the research focus on ESAs?
QA2	Does the research focus on Security?
QA3	Is the research area(s) clearly addressed?
QA4	Is the proposed security solution clearly addressed?

In order to measure the quality impact of journal papers, the following criteria were used when evaluating the quality assessment questions: True = 1; Partial = 0.5; False = 0. Scores were assigned to quantifiably rank the identified practices and attributes. Table 2.3 depicts the quality assessment scoring criteria of the questions. These questions assist in checking biases, the external validation and the internal validation of selected research papers.

Table 2.3: Quality Assessment Questions Categorisation

QA	True (T)	Partial (P)	False (F)
QA1	The research clearly emphasises ESA	The research incompletely addresses ESA	The research does not emphasis ESA.
QA2	The research clearly emphasises on security practices	The research incompletely addresses security practices	The research does not emphasise security practices
QA3	The research problem was concisely explained	The research problem was stated but unclear	The research problem was not stated
QA4	The research concisely explains the proposed solution	The proposed solution was incomplete	The proposed solution was not clearly addressed

2.2.3.5 Data Extraction Form

The data extraction allows for the organisation of information needed from the different studies selected for answering the SLR research questions. Table 2.4 indicates the data extraction form that was employed for all selected papers in order to conduct an in-depth analysis.

Table 2.4: Data Extraction Form

No.	Extracted data	Description	Type
1	Identity of study	Unique identity for the study	General
2	Bibliographic references	Authors, year of publication, title and source of publication	General
3	Type of studies	Book, journal paper, conference paper, patents, white paper.	General
4	The practices employed	Description of ES practices used in developing ESA	RQ1
5	The attributes considered	Description of ESA attributes used in developing ESA	RQ2
6	Finding/Contribution	Indicating finding and contribution of study	General

2.2.3.6 Synthesis

Table 2.5 illustrates the number of papers found per source based on the keywords search in the selected databases. The second column (papers found) indicates the results of an initial screening of paper found in each source. The third column (primary) indicates number of papers after elimination by applying the exclusion criteria. The last column (final selection) indicates the number of papers from each source after examining full text of the selected papers and evaluation by the external reviewer (supervisor).

The significant gap between number of papers found and primary selection raises from Google Scholar, IEEE Xplore and ACM Digital Library, where most of the found papers were duplicated, short paper, or irrelevant. Figure 2.1 illustrates the number of studies identified after each step along the process.

Table 2.5: Data Source

Data Source	Papers Found	Primary	Final Selection
IEEE Xplore	154	35	25
ACM Digital Library	132	14	10
Science Direct	37	12	9
Taylor & Francis	6	6	4
Emerald	12	7	4
Springer	35	15	10
Google Scholar	353	38	26
Total	729	127	88

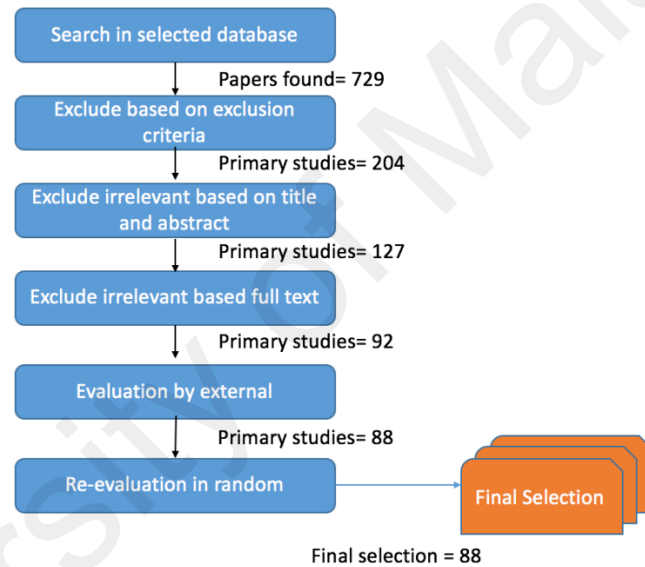
**Figure 2.1: Study Selection Procedure**

Table 2.6 represents the numbers of selected studies categorised by source type. It also shows that the majority of studies were of conference proceeding (41%) and journal papers (39%).

Table 2.6: Study Categories by Source Type

Study	Count	Percentage
Journal Paper	34	39%
Conferences	36	41%
Google Patent	2	2%
White Papers	2	2%
DTIC Document	4	5%
Book Chapter	10	11%
	88	100%

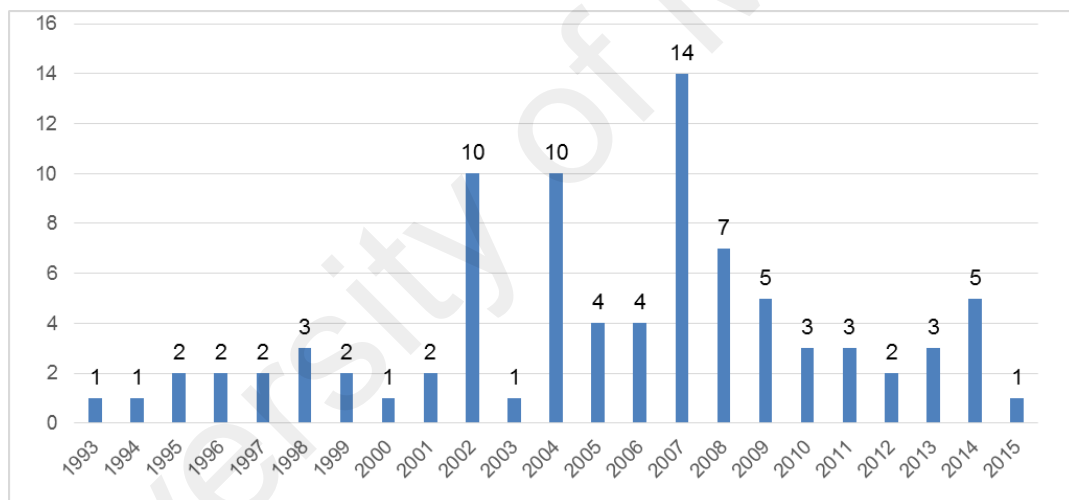
**Figure 2.2: A Number of Studies by Year**

Figure 2.2 shows the distribution of the studies by the year they were published. Out of the 88 studies, 72 papers were published after 2002, while 16 were published between 1993 and 2001. According to the statistics, the most number of papers (43), were published in the period of 2002-2007, then gradually decreasing in 2008 – 2013, before picking up again in 2014. This trend is probably due to the increasing of data breaches in web applications during the time.

Appendix A shows the 88 selected studies. The Appendix provides intricate details of the papers such as authors, year of publication, and for the sake of brevity, the researcher has uniquely labelled individual studies from R01 to R88.

2.3 SLR Results

This section provides the answers of SLR RQs (RQ1.1-1.2) based on the 88 selected primary studies.

2.3.1 Overall Quality Assessment Results

In line with quality assessment questions to be addressed (Table 2.2), the researcher has conducted the assessment and evaluated the primary studies accordingly. The rated score is given based on each QA (QA1-QA4) presented in Table 2.3. As shown in Table 2.7, thirteen (13) papers, which include R4, R9, R12, R15, R18, R34, R35, R47, R52, R61, R62, R73, and R88 have the highest score of 4 (100%). Figure 2.3 shows the papers with the least scores are R7, R23, R54, R58, and R85, with a minimum score of 3 (75%). Based on the assessment, the researcher concluded that the overall quality of the research study is good as all the papers score 75% or above.

Table 2.7: Qualitative Assessment Results

PID	QA1	QA2	QA3	QA4	Total Score	% by Max S
R1	P	T	T	T	3.5	87.5
R2	P	T	T	T	3.5	87.5
R3	P	T	T	T	3.5	87.5
R4	T	T	T	T	4	100
R5	P	T	T	T	3.5	87.5
R6	P	T	T	T	3.5	87.5
R7	P	P	T	T	3	75
R8	P	T	T	T	3.5	87.5
R9	T	T	T	T	4	100
R10	P	T	T	T	3.5	87.5
R11	P	T	T	T	3.5	87.5
R12	T	T	T	T	4	100
R13	P	T	T	T	3.5	87.5
R14	P	T	T	T	3.5	87.5
R15	T	T	T	T	4	100
R16	P	T	T	T	3.5	87.5

R17	P	T	T	T	3.5	87.5
R18	T	T	T	T	4	100
R19	P	T	T	T	3.5	87.5
R20	P	T	T	T	3.5	87.5
R21	P	T	T	T	3.5	87.5
R22	P	T	T	T	3.5	87.5
R23	P	P	T	T	3	75
R24	P	T	T	T	3.5	87.5
R25	P	T	T	T	3.5	87.5
R26	P	T	T	T	3.5	87.5
R27	P	T	T	T	3.5	87.5
R28	P	T	T	T	3.5	87.5
R29	P	T	T	T	3.5	87.5
R30	P	T	T	T	3.5	87.5
R31	P	T	T	T	3.5	87.5
R32	P	T	T	T	3.5	87.5
R33	P	T	T	T	3.5	87.5
R34	T	T	T	T	4	100
R35	T	T	T	T	4	100
R36	P	T	T	T	3.5	87.5
R37	P	T	T	T	3.5	87.5
R38	P	T	T	T	3.5	87.5
R39	P	T	T	T	3.5	87.5
R40	P	T	T	T	3.5	87.5
R41	P	T	T	T	3.5	87.5
R42	P	T	T	T	3.5	87.5
R43	P	T	T	T	3.5	87.5
R44	P	T	T	T	3.5	87.5
R45	P	T	T	T	3.5	87.5
R46	P	T	T	T	3.5	87.5
R47	T	T	T	T	4	100
R48	P	T	T	T	3.5	87.5
R49	P	T	T	T	3.5	87.5
R50	P	T	T	T	3.5	87.5
R51	P	T	T	T	3.5	87.5
R52	T	T	T	T	4	100
R53	P	T	T	T	3.5	87.5
R54	P	P	T	T	3	75
R55	P	T	T	T	3.5	87.5
R56	P	T	T	T	3.5	87.5
R57	P	T	T	T	3.5	87.5
R58	P	T	T	P	3	75
R59	P	T	T	T	3.5	87.5
R60	P	T	T	T	3.5	87.5
R61	T	T	T	T	4	100
R62	T	T	T	T	4	100
R63	P	T	T	T	3.5	87.5
R64	P	T	T	T	3.5	87.5
R65	P	T	T	T	3.5	87.5
R66	P	T	T	T	3.5	87.5
R67	P	T	T	T	3.5	87.5
R68	P	T	T	T	3.5	87.5
R69	P	T	T	T	3.5	87.5
R70	P	T	T	T	3.5	87.5
R71	P	T	T	T	3.5	87.5
R72	P	T	T	T	3.5	87.5
R73	T	T	T	T	4	100
R74	P	T	T	T	3.5	87.5

R75	P	T	T	T	3.5	87.5
R76	P	T	T	T	3.5	87.5
R77	P	T	T	T	3.5	87.5
R78	P	T	T	T	3.5	87.5
R79	P	T	T	T	3.5	87.5
R80	P	T	T	T	3.5	87.5
R81	P	T	T	T	3.5	87.5
R82	P	T	T	T	3.5	87.5
R83	P	T	T	T	3.5	87.5
R84	P	T	T	T	3.5	87.5
R85	P	T	P	T	3	75
R86	P	T	T	T	3.5	87.5
R87	P	T	T	T	3.5	87.5
R88	T	T	T	T	4	100
Total	49	87	87.5	87.5	312	
By max QA	55.6%	98.8%	99.4%	99.4%	88.6%	

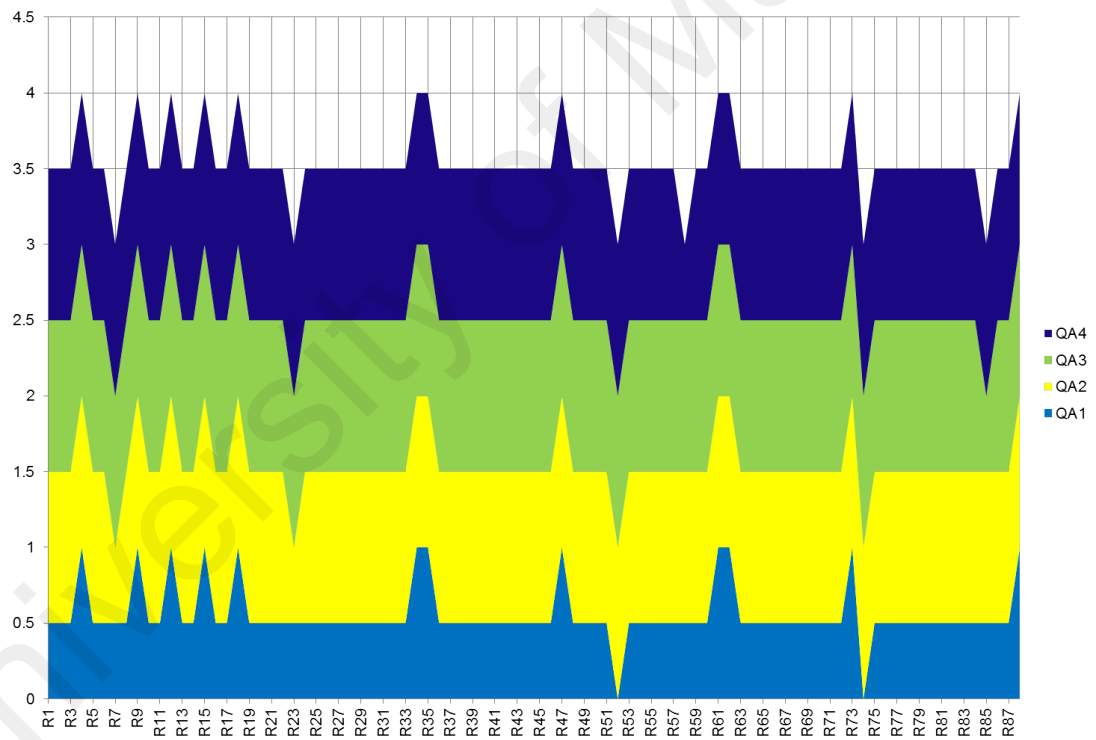


Figure 2.3: Qualitative Assessment Score

2.3.2 Discussion and Highlights on RQ1.1 What are the Effective ES Practices recommended for use in ESAF?

According to Arconati (2002), fundamentals of an enterprise security architecture consists of policy, security domains, trust levels, and tiered networks. Along with Bruce et al. (2000), the four main criteria that supported the information security management (ISM) include the commitment of top management, strategies related to security and vision, ISM structure, and training and security awareness programs.

According to Joshi et al. (2001), the RBAC models offer the most practical framework to addressing a wide range of security requirements for large enterprises. As claimed by Pulkkinen et al. (2007), the business strategies must be paired with partnering enterprises to alleviate trust and privacy such that it collectively complies with accommodating the mission, the alliance strategy, corporate vision and the security policies of the business network. This raises the need for a strategic adjustment and collaboration in creating identity access management provisioning across the business structure. Onwubiko (2009) highlighted that current modern business practices are based on a business area, in order for the organisation to prepare the security policy and the practices cover regulatory standards, legal compliance, and accreditation.

In line with Kim & Cha (2012), there are several international standards recommended for security processes and management, security controls, security requirements engineering and management. There are SSE-CMM, ISO/IEC 15408, ISO/IEC 27002, and OCTAVE. In addition, there are forty-one primary studies (R2, R7, R11, R12, R15, R19, R21, R25, R28, R30, R33, R34, R35, R36, R42, R45, R46, R48, R49, R51, R56, R57, R58, R59, R60, R61, R63, R65, R66, R67, R68, R69, R70, R73, R75, R76, R81, R82, R83, R86, R88) that support this point.

Table 2.8 represents the identified ES practices. The ES practices cover major areas of security countermeasures in management aspect and in the degree of resistance to protect the valuable or vulnerable assets. 40 ES practices have been identified based on the data. Then, the researcher applied the filter (eliminate the ESA implementation and generic practices) to remove 12 irrelevant ES practices. As shown in Table 2.8, 28 ES practices have been identified.

Table 2.8: Security Practices

Reference	ES Practices
Murphy et al. (2000)	Security Model: comprises assessing risk, information classification methodologies as the core elements. The security model is an essential security feature to be facilitated by a system. It should include in depth specifications which allow and forbid relationships between subjects and objects.
Nagaratnam et al. (2002)	Secure Integration: establishes the trusted connection in between internal and third-parties. This is very important component, when organisations are deal with multiple systems. This is described in three major areas: secure integration, security technologies and secure protocol and binding. These integration components are secure the connection with third party components.
Kim and Seong (2005) , Barateiro et al. (2011)	Risk Assessment; analyses the predicted risk for the assets and its projection. The aim of risk assessment is to assess the risk related situation and identify the threat. The quantitative risk assessment calculates the risk of the potential loss and the probability of the loss. The method of risk assessment diverges and it depends on the industry. The risk analysis is intended to separate explicit and typical events that affect an organisation.
Sherwood (1996)	Gap Analysis: to find out the necessary missing security components such that they can be acquired. The gap analysis identifies information security gaps that may happen within an organisation. It investigates the current information security standpoint to industry best practices or standards and regulations. It can frequently identify capabilities that already exist within an organisation, offer the ability to promote these capabilities rather than adopt new ones. Gap analysis can help find and mitigate problems and provide recommendations and the solution on how to fix them.
Sherwood (1996)	Security Strategy: to develop the security services so as to meet the requirements. Security strategies are changing according to a trend of threats. It also becomes very complicated, multi-layered and fragmented, and thus assists the organisation to minimise the risks.
Kim and Seong	Security Roles: who is responsible for managing and

(2005)	maintaining the information systems in the organisation.
Kim and Seong (2005)	Security Mechanism: it is executed to alleviate or reduce the risk and also it consists of safeguards and countermeasures. Security controls are the safeguard to the organisation to prevent and diminish the loss. It also provides the counter measurements for specific vulnerabilities. Security control is equipped with wide range of disciplines which are administrative and preventive measurements, technical detection and correction and detective controls.
Joshi et al. (2001)	Security Requirement: is a non-functional requirement that secure the systems. It is related to all the security attributes such as system confidentiality, integrity, and availability. Overtly declaring security requirements throughout a project's initial stage is the impeccable complement to security testing
Mellado et al. (2010)	Reference Models: it is an abstraction of framework or explicit domain ontology. It is an abstract framework or domain-specific ontology comprising of an intertwined set of noticeably outline concepts created by an expert in order to boost clear communication. It characterises the complete set of system components and business function.
Tahajod et al. (2009)	Security Baseline: understand mandatory minimum standards and practices for the organisation. It defines a set of elementary security objectives which are compulsory to apply by any specified services or systems. The goals are set to be sensible and comprehensive, and do not levy technical matters.
Talukder & Chaitanya (2008)	Application Security: helps identify, fix and prevent security vulnerabilities in the software. Application security is the general practice of adding features or functionality to software to prevent a range of different threats. These include DDOS attacks and other cyber-attacks.
Onwubiko (2009)	Security Framework: to understand and establish security policy and practice. The security framework consists of people, technology, and process to achieve an organisation's business objectives and secure environment. It also makes sure that policy definition, enforcement, measurement, monitoring, and reporting are in place.
Foster et al. (1998)	Security Policy: is defined as a group of security subjects and object and interrelationships. This is the most important document that gives in writing on how an organisation plans to protect the company's physical and information technology (IT) assets. It is often considered to be a "living document", which infers that it will be continuously updated to cope with the upcoming threats and their removal.
Moriconi et al. (1997)	Standard and Compliance: encompasses efforts to ensure that organisations are abiding by both the industry best practices, regulations and government legislation. The security standards enable organisations to practice safe security techniques to stop security attacks. These guidelines provide general outlines as well as specific techniques for implementing security
Sherwood et al. (1995)	Security Metrics: it a dashboard that monitors and measures organisation security measurements. A metric is a system of similar measures to enable quantification of some characteristic. A measure is a dimension compared against a standard. Thus, security metric is a system of related dimensions (compared against a standard) enabling

	quantification of the degree of freedom from the possibility of suffering damage or loss from malicious attack.
Ramadan and Hefnawi (2007)	Network Security: details the conceptual design of the security infrastructure pertaining to the networks, and any related security mechanisms, policies and procedures. The network security is the process of compelling physical and conducting software preventative assessment to defend the fundamental of networking infrastructure. It prevents from unauthorised user access, misuse of authentication, malfunction, modification of data, system destruction, or improper data and packet disclosure. It helps to create a secure platform for users and programs in a secure environment.
Gasmi et al. (2008)	Security Concepts: addressed on a trust model which encompass the components of the system, and security goals. Security concepts associate with different fields of security such as countermeasures, assurance, risk, threat, vulnerability, exploit and defence in depth.
Covington, Fogla, Zhan, & Ahamad (2002)	Security Technology: it's a tool that facilitates enterprise security leaders to accomplish their security goals. Security technology provides essential tools for safe communication and protection of data. It is the process of measurement implementation to secure and protect data breaches. These technologies include a combination of computer hardware and software resources.
Kolter et al. (2007)	Access Control: Access control is about granting access to the authorised personnel and preventing an unauthorised user to access.
Tahajod et al. (2009)	Security Threats/Model: is the central system that provides vulnerability assessments of all information technological assets. The security model is an essential security feature to be facilitated by a system. It should include in depth specifications which allow and forbid relationships between subjects and objects. It outlines the necessary logic and rules to be implemented. It also addresses the high-low level grant criteria for the users.
Murphy et al. (2000)	Security Guidelines: associated with IT security to provide references and guidance.
Talukder & Chaitanya (2008)	Data Security: refers to protective digital privacy measures that are applied to prevent unauthorized access to system. The data security gives an outlook of the architectural underpinning of the exclusive platform. It is a wide-ranging resolution that aims at mitigating the attack surface of sensitive data. It is abiding by the data compliance requirements.
Caralli, Stevens, Willke, & Wilson (2004)	Security Principles: integral to managing the enterprise security.
Talukder & Chaitanya (2008)	Infrastructure Security: is the area of concern surrounding the protection of systems, hardware, network equipment and assets. Infrastructure security architecture consists of banking IT infrastructure, network traffic and communication systems. It prepares a security policy, processes, procedures, and implements secure infrastructure plan, obtains approval process form the senior management, implement security policies and plans, maintain a standardised documentation of the entire IT infrastructure, periodically tests and audits.
Tahajod et al. (2009)	Security Incident Management: provides and maintains the enterprise managed security events efficiently and resourcefully. It is intended to provide the computer systems

	for monitoring and detecting security events, unauthorised access, security breaches, and incidents related to the security standards, compliance and practices. These incidents are reported and documented for investigation and further studies. These incidents are vital to management to prepare for future threats and vulnerabilities of the systems.
Tahajod et al. (2009)	Security Awareness: facilitates the organisation in having a concise understanding of its risk posture. The security awareness programmes provide the knowledge to organisation members and cover the physical and informational assets of the organisation. Organisation need to carry out awareness programmes periodically to ensure that all staff are aware of security controls and measurements
Moral-Garcia, Moral-Rubio, Femandez, & Femandez-Medina (2014)	Security Pattern: recurring problems related to information systems security, promoting the reusability of designs when developing enterprise security architectures. Security patterns are built for the different purposes to achieve information security goal. The patterns are generally equipped with security attributes such as confidentiality, integrity, and availability. According to the need of security, the requirement has to select the suitable security pattern.
Foster et al. (1998)	Secure Protocol/Binding: defined as an abstract security operation. A security protocol is a concrete protocol that performs a security-related function and applies cryptographic methods. The protocol includes details about data structures and representations. It is also used to implement multiple, and compatible and interoperable versions of a program.

Table 2.9: Number of Studies by ES Practices

#	Security Practices	Papers	Study Identifiers
1	Security Models	40	R1,R7,R8,R4,R6,R12,R14,R16,R18R19,R22,R24,R32,R33,R37,R38,R40,R41,R42,R44,R46,R48,R49,R50,R51,R52,R53,R56,R57,R64,R66,R69,R73,R75,R76,R78,R80,R84,R85,R87
2	Secure Integration	16	R4,R19,R21,R32,R38,R42,R45,R47,R48,R49,R50,R60,R67,R69,R70,R82
3	Risk Analysis and Assessment	32	R2,R3,R4,R12,R18,R27,R28,R33,R35,R36,R37,R42,R46,R51,R55,R56,R57,R60,R61,R62,R64,R66,R68,R69,R70,R73,R78,R81,R82,R84,R85,R86
4	Gap Analysis	5	R6,R56,R65,R81,R88
5	Security Strategy	9	R6,R12,R27,R30,R62,R68,R81,R82,R88
6	Security Roles	14	R4,R12,R17,R27,R35,R36,R42,R49,R62,R72,R74,R82,R83,R87
7	Security Mechanism	28	R1,R2,R8,R9,R11,R19,R25,R28,R30,R34,R35,R37,R38,R39,R44,R46,R52,R63,R65,R69,R73,R74,R75,R78,R82,R84,R85,R87
8	Security Requirement	35	R2,R3,R6,R10,R14,R19,R23,R24,R25,R28,R29,R30,R34,R36,R38,R42,R49,R50,R51,R53,R54,R59,R61,R64,R65,R73,R74,R76,R78,R80,R81,R83,R85,R86,R87
9	Reference Models	4	R35,R46,R49,R86
10	Security Baseline	4	R33,R39,R62,R80
11	Application Security	21	R1,R2,R4,R5,R6,R7,R8,R9,R10,R11,R14,R16,R18,R19,R20,R28,R34,R40,R59,R67,R73
12	Security Frameworks	11	R4,R12,R25,R38,R44,R49,R51,R55,R81,R83,R88
13	Security Policy	59	R1,R2,R3,R5,R7,R8,R9,R10,R12,R14,R15,R18,R19,R20,R22,R23,R25,R27,R29,R32,R34,R35,R36,R37,R38,R40,R42,R44,R45,R46,R50,R51,R52,R53,R54,R55,R56,R57,R58,R59,R61,R62,R63,R64,R67,R69,R70,R72,R73,R74,R75,R76,R80,R82,R83,R84,R85,R87,R88
14	Standard & Compliance	41	R2,R7,R11,R12,R15,R19,R21,R25,R28,R30,R33,R34,R35,R36,R42,R45,R46,R48,R49,R51,R56,R57,R58,R59,R60,R61,R63,R65,R66,R67,R68,R69,R70,R73,R75,R76,R81,R82,R83,R86,R88
15	Security Metrics	2	R4,R78
16	Network Security	8	R3,R11,R45,R56,R57,R70,R74,R82
17	Security Concepts	2	R53,R80
18	Security Technology	19	R2,R3,R6,R10,R19,R20,R30,R31,R32,R33,R40,R46,R59,R63,R67,R70,R75,R80,R82
19	Access Control	58	R2,R3,R7,R8,R9,R10,R14,R16,R17,R19,R20,R22,R25,R29,R32,R33,R34,R35,R36,R37,R38,R39,R40,R41,R44,R45,R46,R48,R49,R50,R51,R52,R53,R54,R55,R56,R57,R59,R61,R62,R63,R64,R65,R66,R67,R68,R69,R70,R72,R73,R74,R75,R76,R78,R80,R81,R82,R87
20	Security Threats/Model	9	R24,R48,R57,R60,R62,R66,R69,R73,R76
21	Security Guidelines	7	R12,R18,R52,R56,R61,R70,R81
22	Data Security	21	R1,R4,R5,R6,R7,R8,R9,R10,R11,R12,R15,R18,R34,R35,R36,R37,R40,R59,R69,R80,R86
23	Security Principles	10	R2,R9,R19,R27,R28,R29,R39,R54,R57,R70
24	Infrastructure Security	9	R4,R8,R11,R12,R15,R18,R19,R46,R68
25	Security Incident Management	2	R69,R88
26	Security Awareness	5	R2,R12,R25,R62,R82
27	Security Patterns	2	R34,R52
28	Secure Protocol and Binding	2	R10,R19

Table 2.9 illustrates the number of studies based on the identified ES practices. Among all the practices, security policy is the most addressed practice (59 papers) followed by access control (58 papers). On the other hand, security metrics, security concepts, security incident management, security pattern, secure protocol/binding are the least addressed practices (2 papers each).

There are 18 papers (R2, R12, R13, R19, R34, R35, R45, R46, R51, R56, R62, R69, R70, R73, R74, R81, R82, R88) that have addressed more than 10 practices. R19 addresses the most practices (15) as compared to the others, while there are 13 papers (R5, R7, R11, R14, R15, R16, R17, R22, R23, R24, R29, R31, and R58) that addressed below 5 practices. R5 has the least addressed practices (2 practices).

Appendix C illustrates the number of significant studies by year of publication (1993-2015). The years 2007, 2008 and 2009 have the most publications (77, 39, and 43, respectively). On the other hand, the years 1995-2001 have the least number of publications and the least number of practices were indicated. The researcher noticed that the number of publications gradually declined between 2010-2015. In the past three years, the trend of research has been changed, where more priority is given to security model, secure integration, security management, security implementation, security policy, security compliance and risk assessment and management.

2.3.3 Discussion and Highlights on RQ1.2 What are the Effective ESA Attributes that Affect the Effectiveness of ESAF?

This section details the research finding related to RQ1.2. The researcher highlighted all the significant attributes of primary studies that are pertinent for ESAF.

Based on the fact, the attributes that affect the comprehensiveness of ESAF can provide a full coverage of security in a coarse-grained, full-fledged and static fashion. According to Barateiro et al. (2011), the information security is well-defined as the protection of confidentiality, integrity and, availability of information. Moreover, it further encompasses other security characteristics, including authenticity, accountability, non-repudiation, and reliability. In accordance with Allen (2005), customers are demanding ESA policies to be accommodated as concern about the secrecy of personal data and identity theft cases upsurge. It is also permitting transactions to transpire with superior integrity and privacy. Thus, it also contributed to guaranteeing business throughput, customer satisfaction, and buoyancy, which are able to craft the customer loyalty. Besides, they stated that forming and retaining customers' confidence in an institute's security and privacy stance increases the prospect that clients will refer to the other products and services offered by the organisation. Kolter et al. (2007) also stressed that a basic requirement of the end users is privacy, effectively when the system is dealing with sensitive personal data. According to Blackwell (2010), it is important to be more concerned about the secure quality factors confidentiality, integrity, and availability. If organisations are unable to implement those ESA attributes, it will ultimately affect the organisation's goodwill. As stated by Enose (2014), the objective of a malicious hacker is not only to challenge the control system's resilience but also to annihilate it. Therefore, the need to build a secure foundation of automation and control system layer that can withstand the fluctuations forced on its structure, design and control parameters. In the context of cyber security, it means the ability of the system to quickly and effectively reconstitute the control under attacks. In relation to RQ 1.2, the researcher examined the data and Table 2.10 shows the definition of the identified ESA attributes. 15 ESA attributes were selected based on the extracted data.

Table 2.10: Security Attributes

Reference	ESA Attributes
Barateiro et al. (2011)	Reliability: it defines as the property of trustworthiness. Reliability is the property of leading to consistent intended behaviour and results. For instance: banking user data are often considered reliable when they are exact and precise, and when they can be reproduced. By adapting high reliability in operations, bankers be able to reduce operation cost, reduced risk of environment issues, reduced overheads and better process stability.
Kim & Seong (2005)	Availability: Data must be made accessible when users or systems require it. Characteristics of resource that is committable, operable, or usable upon demand to perform its designated or required function.
Li, Luo, & Liu (2010)	Encryption: is applied to protect messages by encoding and allows only authorised parties to read.
Pulkkinen et al. (2007)	Audit: to ensure that compliance is in place with policy and procedures. Furthermore, regularly review and examine the audit log files to ensure security compliance.
Pulkkinen et al. (2007)	Authorisation: This is to ensure that permitted and authorised person or system to process grant access.
Pulkkinen et al. (2007)	Authentication: to validate the credentials of access systems. Authentication is an access control technique or combination of techniques that verify the identity of an individual who is attempting to gain admittance into an information system. As a example, data of plural biometric characteristics are able to combined to increase overall confidence in the authentication.
Kim & Seong (2005)	Confidentiality: is a set of rules that limits access or places restrictions on certain types of information.
Shin, Jung, Kim, & Lee (2014)(2014)(2014)	Privacy: The data can only be accessed by the people who have authorization to view and use it.
Shariati et al. (2011)	Interoperability: is the ability of different information technology systems and software applications to communicate, exchange data, and use information that has been exchanged.
Mohammadi et al. (2014)	Trust: This is to committed or entrusted to one to be used or cared for in the interest of another.
Atoum et al. (2014)	Resilience: the capable of recover quickly from attacks. It also intent to handle quickly adapting of modifications in technology.
Leitold, Hollosi, & Posch (2002)	Non-Repudiation: provision against false denial of having carried out a transaction
Kim & Seong (2005), Barateiro et al. (2011)	Integrity: characterised by maintaining stringent protocols that thwart any unauthorised attempts to breach the integrity of the resources.
Mukkamala, Chekuri, Moharrum, & Palley (2004)	Anonymity: anonymity is applied to any interaction of a user identity from being shared with another user or with a third party.
Joshi et al. (2001)	Accountability: Accountability is the property that ensure that the action of an entity can be traced solely to entity. Accountability guarantees that all operations carried out by individuals, systems or processes can be identified and that the trace to the author and the operation is kept (traceability).

Table 2.11: Number of Studies by ESA Attributes

#	Attributes	Papers	Study Identifiers
1	Reliability	8	R3,R4,R27,R36,R42,R68,R75,R86
2	Availability	34	R2,R3,R4,R6,R8,R9,R12,R24,R27,R28,R30,R32,R37,R42,R43,R45,R46,R47,R49,R52,R55,R58,R59,R61,R64,R66,R68,R69,R70,R71,R73,R76,R82,R88
3	Encryption	32	R1,R2,R3,R9,R11,R14, R15,R20,R29,R31, R32, R33,R34,R35,R39, R41, R44,R45, R46, R47,R48,R52,R53,R57,R59,R61,R63,R72,R75,R80,R84,R87
4	Audit	29	R2,R3,R4,R6,R8, R9,R17,R19,R25,R27,R28, R35,R37,R41,R43,R45, R46,R47, R52, R57,R58, R61, R64, R67,R69,R70,R71,R81,R82
5	Authorization	49	R2,R4,R8,R10,R11,R15,R16,R17,R19, R20, R21, R22, R24,R28, R29,R31,R32,R34, R35, R37,R39, R41,R42,R43,R46, R47,R52,R53,R54, R56,R57,R61, R63,R65, R66,R67,R68, R69, R70,R72,R74, R75,R76,R78,R80,R82,R85,R87,R88
6	Authentication	51	R1,R2,R3,R4,R6,R7,R8,R9,R10,R11,R15,R17,R19,R20,R21,R22,R24,R25,R28,R29, R32, R33,R34,R35, R36,R37,R39,R41, R43,R44, R46,R47, R53,R54, R55, R57,R58, R61,R63, R65,R66,R67,R68, R69,R72,R73,R75,R78,R80,R84,R87
7	Confidentiality	46	R2,R4,R6,R9,R12,R15,R17,R19,R21,R24,R27,R28,R33, R34,R37,R41,R42, R43,R44,R46, R47, R49, R52, R53,R55,R56,R59,R60,R61,R63,R64,R66,R67,R68, R69,R70, R71, R72, R73, R74,R76,R80, R82, R85,R87,R88
8	Privacy	21	R2,R10,R19,R24,R27,R29,R31,R32,R36,R37,R41,R42,R46, R47,R49,R51, R64,R71,R72, R83,R84
9	Interoperability	7	R4,R6,R10,R19,R51,R53,R83
10	Trust	20	R1,R2,R11,R15,R19,R20,R22,R25,R31,R34,R36,R39,R53, R57,R72,R74,R75,R80, R81, R84
11	Resilience	6	R27,R28,R36, R68,R69,R81
12	Non-Repudiation	15	R8,R10,R14,R19,R21,R24,R29,R32,R33,R41,R46,R55,R73,R80,R86
13	Integrity	55	R2,R3,R4,R6,R8,R9,R10,R11,R12,R14, R19,R21,R24,R25,R27, R28,R29, R31,R32,R33, R34, R36, R37, R39, R41,R42,R43,R45, R46,R47,R49,R52, R53,R56, R58, R59, R60,R61,R63, R64,R66,R67,R68, R69,R70,R71,R72,R74,R76,R80,R82,R84,R86,R87,R88
14	Anonymity	5	R11, R16, R19,R43,75
15	Accountability	19	R2,R4,R6,R13,R14,R18,R25,R28,R35,R36,R43,R49,R56,R57,R59,R66,R67,R69,R86

As shown in Table 2.11, integrity is the most addressed practice (55 papers). On the other hand, anonymity (5), resilience (6), interoperability (7), reliability (8) attributes are the least addressed security attributes. Each publication addresses at least two attributes except for R5 (None), R7 (1), R23 (1), and (R48 (1 each). R4 and R46 address the most attributes (10).

Appendix D illustrates the number of studies by years of publication between 1993 and 2015. The years 2002, 2004, 2007, 2008, and 2010 have the most publications. The majority of publications were found between the years 2002 to 2015. On the contrary, the years 1995-2001 have the least number of publications and the least number of attributes were indicated. The analysis shows that the number of publications gradually rose between 2013-2014, where more priority is given to authorisation, authentication, confidentiality, availability, and integrity.

2.4 Existing Frameworks

This section is intended to identify existing frameworks, in particular the security frameworks for banking environment. It will address RQ2 (What are the existing frameworks, particularly the security frameworks for banking environments?).

2.4.1 Type of Enterprise and Security Architecture Frameworks

This research is based mainly on three types of frameworks which are generic enterprise architecture framework, security architecture framework (SAF) and banking security framework (BSF). Existing enterprise and security architecture frameworks were identified from the industrial practices and scientific databases. The industrial practices used the enterprise architecture body of knowledge (EABOK), information systems audit and control association (ISACA), Gartner and Open group. The databases used to identify enterprise and security frameworks were ACM Digital Library, IEEE Xplore, Science Direct, Springer Link, Emerald, and Google Scholar. The researcher has chosen these databases as the main sources since they predominantly address the ESA domain compared with other databases and sources. Besides, an additional reference mechanism was added to ensure that all the relevant literature was properly analysed.

In order to analyse the existing frameworks, they are further classified into sub categories (Figure 2.4).

- Generic- generic architecture focuses on fundamental of EA.
- SAF- mainly focuses on security attributes and practices.
- BSF- specifically addresses the banking domain and implementation of security in banking industry.

Generic				SAF		BSF	
TOGAF	GERAM	RM-ODP	EABOK	SABSA	FESF	AERA	SQIBUCF
IAF	ZEAF	ARIS	OBASHI	COBIT	NIST SP	IBF	PKIMBSF
C4ISR	DODAF	NATO AF	TAFIM	PFIRES	OSA	SFMB	BBSF
JTA	MODAF	DNDAF	AGATE	SIEMF	ITSA	OBSFC	PEEAMB
IDEAS	FEAF	GEA	TEAF	SMDAF	EISA	USEUBIEF	FGISBS
EIF	NISTEA	TISAF	SAGA	AFUCIFS	FSPAT		
NIHEAF	PERA	GEAF	GRAI GIM				
CIMOSA	E2AF	EAP	4+1 MODEL				
SOA-EAF							

Figure 2.4: Types and Categorisation of EAF

The characteristics and analysis of framework is included in **Appendix B**.

2.4.2 Overall Analysis and Discussion

Generic enterprise architecture frameworks are further classified into seven categories, which include enterprise developed framework, commercial framework, defence framework, government framework, healthcare framework, manufacturing industry framework and other framework.

SAFs are classified into eight categories, which include enterprise security architecture framework, security architecture framework, information and management framework, threat security architecture framework, security management framework, enterprise information security framework, information flow security framework, and security and privacy framework.

BSFs are classified into eight categories, which include general banking framework, Internet banking framework, banking mobile framework, banking biometric framework, cross cultural framework, banking product performance framework, banking system usability framework, and banking governance framework.

According to the analysis, the researcher has found that BSFs focus on only one or a few elements of the framework rather than a holistic view of the entire security. The framework's strength is capable of handling a specific security area (for instance: e-banking). Therefore, the framework security coverage is less and may need to use multiple frameworks to cover other security aspects. Furthermore, it has the lowest coverage of security compared with SAFs.

2.5 Framework Assessment

The framework assessment is intended to identify the gaps between existing frameworks and ESA attributes and ES practices. It will address RQ3 (RQ 3: What is the gap between existing frameworks and ESA attributes and ES practices?).

55 frameworks have been identified from the literature which consist of 33 generic EAF, 12 SAF and 10 BSF. The researcher then compared the frameworks with the identified ES practices and ESA attributes identified in the SLR and the results will be discussed in the next section.

2.5.1 Criteria for Framework Assessment in Relation to ES Practices

To measure the quality impact of a framework in addressing ES practices, the researcher used the following scoring procedure: Yes = 1; Partial = 0.5; No = 0 (Kitchenham et al., 2009). Table 2.12 illustrates the quality assessment scoring of the chosen frameworks in addressing ES practices.

Table 2.12: Quality Assessment Questions

	Yes (Y)	Partial (P)	No (N)
Quality Assessment Questions	The framework clearly emphasises ES practice	The framework incompletely addresses ES practices	The framework does not emphasise ES practices

2.5.2 Assessment of Generic EAF, SAF and BSF against ES Practices

In general, security practices in the organisation become the de facto standard. Nevertheless, there are certain organisations that are taking initiatives on security awareness, prioritising the industrial standards, and assuring the future platforms are fully secured (Talukder & Chaitanya, 2008). The rated score is given based on each QA question presented in Table 2.12. The total score indicated the marks of the selected frameworks are in accordance with the QA questions. In addition to that, the highest possible score for a framework is 28, i.e. 1 score for a “Yes” for each ES practice, with a total of 28 practices. As shown in Appendices E and F, the generic frameworks with the highest scores are NIST EA and MODAF, which score 48.15% and 42.59%, respectively. The frameworks with the lowest scores are Zachman and 4+1 Model, which account for 0%. Overall, the average score of the frameworks are slightly above 40%.

Access control and security policy are the most adopted ES practices (31) among the frameworks. Nevertheless, there are seven practices, i.e. security awareness, security incident management, security guidance, reference models, security patterns, security metrics, and security model, not addressed by any of the frameworks.

Among the SAFs, COBIT scores the highest marks of 57.41%. Six of other frameworks, which include SABSA, PFIREs, ITSAF, SMDAF, FESA, and EISA score between 40% and 50%. Based on the assessment, the researcher concludes that the overall quality of the frameworks studied have not sufficiently addressed the security needs of banking industry as all the frameworks score below 60%.

Among all the SAFs, security framework, security mechanism, standard and compliance, security requirement, risk analysis, security principles and security policy are the most addressed ES practice. Likewise, there are three practices, i.e. security patterns, reference model and security metrics are not addressed by any of the SAFs. On the other hand, security strategy, gap analysis, security roles, security infrastructure, security binding, are the least addressed practices.

Among the BSFs, IBF and PKIMBSF score the maximum score of above 30% (35.19% and 37.04%, respectively). Other frameworks score below 30%. Based on the assessment, the researcher concludes that the overall security practices of the BSF, are not sufficient as of all the frameworks score below 40%.

Among all the BSFs, security framework, security mechanism, standard and compliance, security requirement, security principles and security policy are the most addressed ES practice by the BSFs. Likewise, there are three practices, security patterns, reference model and security metrics are not addressed by any of the frameworks. On the other hand, security strategy, gap analysis, security roles, security infrastructure, security binding, are the minimum addressed practices.

For all the frameworks, the findings have been alarming in the context of readiness to security practices. The least addressed practices are security awareness, security incident management, reference models, security models, security patterns, security metrics and security threat model.

2.5.3 Criteria for Framework Assessment in Relation to ES Attributes

To measure the quality impact of the frameworks, the researcher used the following scoring procedure: Yes = 1; Partial = 0.5; No = 0 (Kitchenham et al., 2009). Table 2.13 illustrates the quality assessment scoring of the chosen frameworks.

Table 2.13: Quality Assessment Questions

	Yes (Y)	Partial (P)	No (N)
Quality Assessment Questions	The framework clearly emphasises on enterprise security architecture attributes	The framework incompletely addresses enterprise security architecture attributes	Framework does not emphasise on enterprise security architecture attributes

2.5.4 Assessment of Generic EAF, SAF and BSF against ESA Attributes

The maximum score is 15, i.e. 1 score for a “Yes” for each ESA attribute, with a total of 15 attributes. As shown in Appendices G and H, SABSA and COBIT get the maximum score of above 50% (53.13% and 56.25%, respectively). The frameworks ZACHMAN and 4+1 MODEL recorded the lowest score (0%).

Availability, authentication, authorisation, confidentiality and integrity are the most addressed attributes (31) among the generic frameworks. There are two attributes, i.e. anonymity and resilience, not addressed by any of the frameworks.

Among the SAFs, COBIT gets the highest score of 56.25% and SABSA scores 53.13%. The SAFs with lowest scores reported are SIEM, SMDAF, FESA, and AFUCIFS, all with a score of 31.25%. Among all the SAFs, availability, authentication, authorisation and confidentiality are the most addressed ESA attributes (10). Anonymity is not addressed by any of the SAFs. In general, other attributes are not addressed significantly.

Among the BSF, PKIMBSF gets the highest score of 50.00% and IBF scores 46.88%. The most addressed ESA attributes are authentication, authorisation, availability, confidentiality and integrity. Attributes such as resilience, anonymity, accountability and interoperability are neglected by the BSFs.

2.6 Summary

This chapter has provided a detailed review of the ESA. It has addressed effectiveness ES practices and ESA attributes that affect the effectiveness of ESAF. Furthermore, it has detailed out the existing frameworks. It has also explained the assessment of frameworks against ES practices and attributes.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter addresses the detailed methodology that is relevant to the research. As Table 3.1 illustrates, this research was accomplished by a number of steps ranging from an initial stage to requirements elicitation and validation stage, design and implementation stage, and then lastly evaluation stage. It begins with the early stage of the problem identification and formulating the main research questions. This is followed by a research on associated work in literature, and carrying out several brainstorming sessions with industrial experts and studying to articulate the problem statement and define research objectives. During the design and implementation stage, the conceptual framework and detailed ESAF for the banking industry are presented. This includes layers of the ESAF and its components. Finally, the evaluation of the ESAF is presented. Figure 3.1 illustrates the step-by-step research methodology.

Table 3.1: Research Methodology

Stage		Activities
Stage 1	Initial Phase	<ul style="list-style-type: none">• Problem identification• Formulate main research questions
Stage 2	Requirements Elicitation and Validation	<ul style="list-style-type: none">• Literature review (Taxonomy of attacks /Identification of ES practices and ESA attributes/ Review of existing frameworks)• Requirements validation by stakeholders• ESAF assessment• ESAF baseline• Refinement of problem statement• Defined objectives and sub research questions

Stage 3	Design and Implementation	<ul style="list-style-type: none"> Formulate conceptual ESAF Design detailed ESAF Implementation of ESAF
Stage 4	Evaluation	<ul style="list-style-type: none"> Validate the conceptual ESAF

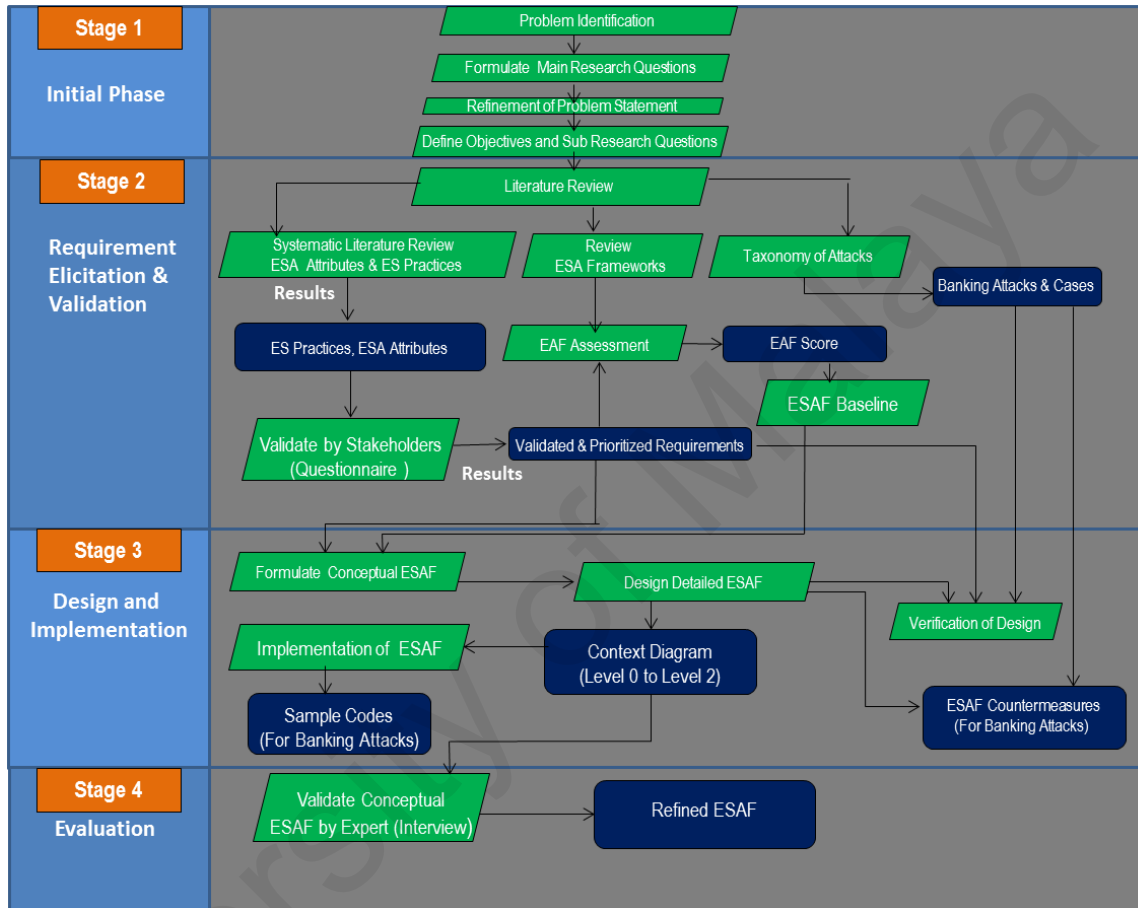


Figure 3.1: Research Methodology

3.2 Problem Identification

The researcher used the Ishikawa or fishbone diagrams (Refer to **Appendix I**) to define the banking enterprise security problems. In the beginning stage, the researcher has conducted several brainstorm sessions with stakeholders including CEO, CIO, HOD, project and product managers, business analysis and engineers to identify the possible causes. The researcher has also identified the boundaries and finalised the

scope of the research. After the literature review, the researcher redefined the problem statement accordingly and prioritise the research scope.

3.3 Literature Review

The literature review is presented in Chapter 2. The literature review consists of three parts: taxonomy of attacks, a SLR to identify essential ES practices and ESA attributes, and a review of existing EA frameworks. In the taxonomy of attacks, the researcher provided an exploratory descriptive analysis of various banking attacks and their cases. The researcher has identified top ten attack types and reported financial attacks through literature.

The SLR on ES practices and ESA attributes followed the guidelines introduced by Keele (2007) and Kitchenham et al. (2009). According to them, there are three consecutive stages in a review process: planning, execution, and result analysis, with a fourth stage, i.e packaging, to store the results at the end of each stage. The SLR systematically explored fundamentals of ESAF, i.e. ES practices and ESA attributes. Six databases, i.e. ACM Digital Library, IEEE Xplore, Science Direct, Springer Link, Emerald, and Google Scholar were used in the SLR.

The review of existing frameworks, on the other hand, revealed a better understanding of the current issues and implementation of ESAFs, especially in the banking environments. A number of frameworks in the literature have been examined. The researcher evaluated their strengths and weaknesses in fulfilling the ESA attributes and ES practices. This finding also provides a clear direction for this research and helps to refine the problem statement and research objectives.

3.4 Validate ES Practices and ESA Attributes

The researcher put forward some strategies to mitigate threats in SLRs. The researcher established the protocol for the study during the planning phase, which was reviewed by an external reviewer (the supervisor). The well-defined inclusion and exclusion criteria were helpful to reduce the identification error of primary studies. All decisions and results were double-checked by at least one person. In addition, the researcher used multiple databases that execute the queries on the different sources to reduce human errors during the search phase. The researcher checked those papers twice to detect and remove duplicated papers.

The researcher carried out the requirements validation activities to validate the baseline ES practices and ESA attributes by the industry practitioners and banking stakeholders. The researcher used questionnaire to validate the data. After validation of ES practices and ESA attributes, the researcher used a scoring system to quantifiably prioritise the requirements.

3.4.1 Questionnaire

Questionnaire is suitable for quantitative research and exploratory research paradigms. The researcher used questionnaire as the data collection method to gather the data from banking stakeholders. 188 questionnaires were distributed to stakeholders of banking systems development, including chief technical officers (CTO), senior vice presidents (SVP), project management office heads (PMO), project managers (PM), business analysts (BA), and software architects and engineers. The questionnaire was based on the finding of SLR on ES practices and ESA attributes.

Stratified sampling and expert sampling were used as the major sampling method. Stratified sampling involves the use of “stratum”, a subset of the target population

wherein the members possess one or more common attributes. Expert sampling is based on persons with recognised or demonstrable knowledge, skills, and expertise in the selected areas (Kothari, 2004). The selected subject method experts include CTOs, BAs, SVPs, software consultants, system architects, software architects, security architects, security subject method experts, project directors and project managers who have expertise in the banking domain. The survey consisted of mainly close-ended questions. The researcher then applied the scoring approach to transform the data collected in order to prioritise the ES practise and ESA attributes.

3.5 Frameworks Assessment

A comprehensive ESAF for banking environments is lacking both in literature and practice. Chapter 2 describes in detail the various frameworks and challenges of security for the banking domain. In order to achieve the first research objective (to identify the ESA attributes and ES practices to be incorporated into a comprehensive, and effective ESAF that is easy to use by the practitioners.), it is imperative to identify and classify the core security requirements for banking environments. The researcher used the scoring method (Yes = 1; Partial = 0.5; No = 0) to measure the quality impact of a framework in addressing ES Practices and ESA attributes.

3.6 ESAF Baseline

After ESAF assessment, the researcher selected frameworks with the highest scores as a baseline. The proposed ESAF was then designed based on the baseline frameworks, i.e. SABSA, COBIT and NIST, with the scores shown in Table 3.2.

Table 3.2 ESAF Baseline Frameworks

Framework	SABSA	COBIT	NIST
ES Practices	46.30%	57.41%	46.30%
ESA Attributes	53.13%	56.25%	56.30%

3.6.1 SABSA

The SABSA framework is extensively used by the industry and it provides a unified information security solution to organisations. It consists of a six-layer model that covers all components of the IT lifecycle such as strategy, design, implementation and management and operations (Burkett, 2012; Sherwood et al., 1995; Sherwood, 2005; Sherwood, 1996).

3.6.2 COBIT

The COBIT is a framework introduced by ISACA to manage IT and IT governing body. It consists of four domains, which include plan and organise, acquire and implement, deliver and support, and monitor and evaluate. It is equipped with 34 processes. Besides, it has been aligned with ITIL, BASEL, ISO27000, CMMI, TOGAF and PMBOK (Bernroider & Ivanov, 2011; De Haes, Van Grembergen, & Debreceeny, 2013; Von Solms, 2005).

3.6.3 NIST

NIST is a five-layer model for enterprise architecture, and designed for organising, planning, and building an integrated set of information and information technology architectures. The five layers are business, information, information system, data, and data delivery architecture (Framework, 2010; Fong & Goldfine, 1989; Council, 1999)

3.7 ESAF Design

To ascertain security between banking systems and the security requirements, there is an urgent need for a comprehensive ESAF. The second research question is to address the design of the ESAF. In order to achieve that, the researcher has created the level 0 to level 2 conceptual diagrams. In the design stage, the actors and security components as well as their interactions were further elaborated.

3.8 ESAF Implementation

Once the security framework design stage was completed, to accomplish the second research objective, the proposed framework was modelled into a workable environment to enable evaluation of its effectiveness in banking environments at the next stage. For implementation, each layer of the ESAF must deliver the artefacts to accomplish the specific tasks at the layer. 21 templates were designed to support the application of the proposed ESAF.

3.9 ESAF Evaluation

To accomplish the third objective after completing the implementation stage, the important components of the proposed framework were evaluated to ascertain that the security requirements are met. As Figure 3.2 illustrates, this ESAF evaluation was accomplished in a number of steps: setting up prerequisite criteria, select the interviewees (by banking domain, technical knowledge and years of experience), invite interviewees, send an evaluation copy of ESAF, template and scenarios to interviewees, brief interviewees on the ESAF and discuss the identified scenarios, conducting the first assessment based on three criteria (comprehensiveness, effectiveness and ease of use), conducting the second assessment based on the given scenarios, getting suggestions and recommendations, and incorporate recommendations to the proposed ESAF .

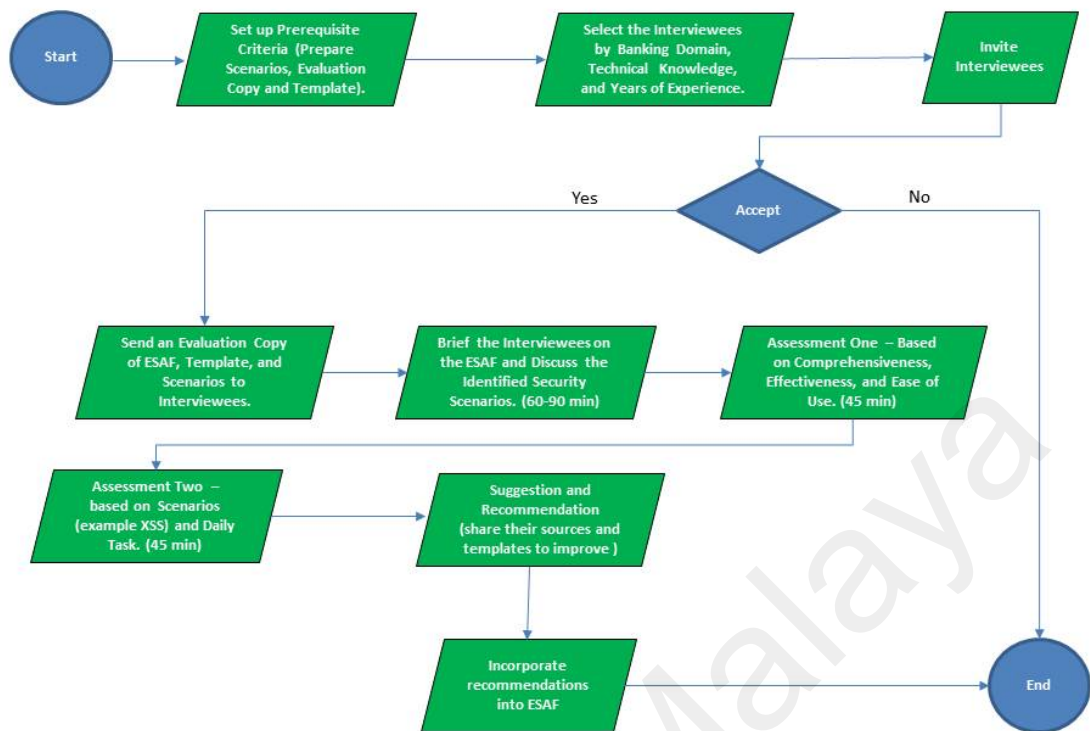


Figure 3.2: Evaluation Flow

3.9.1 Interview

Bell & Bryman (2007) highlighted that the use of interviews is a controlled way to obtain information from interviewees. With an interview, it is easy to respond and elaborate subject areas clearly. The interviewer has the opportunity to drill down on the subject thoroughly. Interviews were carried out with 24 industrial practitioners who are from the banking domain to evaluate the proposed ESAF.

The interviews were carried out with banking stakeholders and industry practitioners who have vast experience in banking information systems, EA, EA frameworks and security domain. The purpose of the interview was to validate the proposed framework by the experts of the subject matter, who have at least 3 years of experience in developing banking information systems, and were well versed with the security domain.

3.9.2 Interview Strategy

The researcher has selected the semi-structured interview strategy (Berg, Lune, & Lune, 2004). According to Kvale & Brinkmann (2009), the strategy is suitable if the interviewer is well experienced and familiar with the domain because that would facilitate a conversation rather than a dialogue. Such a conversation helps in finding out the subtle grains of information that is invisible in a questionnaire. The interview also allowed the researcher to ascertain information captured through the questionnaire.

3.9.3 Interview Guidelines

Table 3.3 illustrates the questions that guided the interview.

Table 3.3: Interview Guidelines

No.	Main Interview Question	Sub Interview Questions
Q1	What are the advantages of the proposed ESAF in relation to tasks that need to be carried out? What are the suggestions to improve the ESAF?	<ol style="list-style-type: none">1. What is the effectiveness of the ESAF in relation to the tasks (day-to-day IT project task)?2. What is the comprehensiveness of the ESAF in relation to the tasks?3. What is the ease of use level of the ESAF in relation to the tasks?
Q2	How can the ESAF support enterprises to develop ESA?	<ol style="list-style-type: none">4. How does the ESAF assist in ESA development?5. Which layers or components of the ESAF are more imperative to support ESA development? Why?6. What are the impacts of the ESAF on ESA development and implementation?7. What are the advantages and drawbacks of the proposed ESAF templates and guidelines?

3.9.4 Selection of Interviewees

In-depth interviews were conducted with security and architectural experts who have academic and industrial experience in security, and ESA development and implementation.

3.9.5 Conducting and Transcribing Interviews

The researcher began by emailing the interviewees so that they were informed in advance of research questions and goals. The researcher has also given the ESAF overview document, template and guidelines for them to prepare for the interview. With those who acknowledged, the researcher set up a physical appointment. Those who could not be available physically helped the researcher to provide an audience using virtual communication tools such as WebEx, WhatsApp, Skype, and telephone. Each interview lasted at least half an hour to one hour.

3.10 Ethical Considerations

Throughout the research, the researcher has ensured the participants' privacy and confidentiality. Furthermore, the participants' demographic details such as name, title, bank name, and location were not captured, and also their responses are not accessible by any third party. This is to comply with the Personal Data Protection Act and banking industry practices in relation to confidentiality. The participants also signed a consent form, which informs about their rights in participating in the survey, and how the data that they provided will be handled in compliance with privacy and confidentiality (Refer to **Appendix J**).

3.10.1 Reliability and Validity

In a scientific study, the reliability of the study is of prime importance. In this study, the researcher tried to elucidate the aims and processes of the research systematically.

For instance, with the SLR, the researcher had deliberately described the literature selection process so that any researcher is able to replicate the review and get the same results. In order to validate the research findings, the researcher has conducted questionnaires and interviews with the industry experts.

3.10.2 Bias

A pure scientific study goal is to eliminate bias as much as possible so that prejudices and preconceptions cannot alter the course of the research (Schmidt & Hunter, 2014). To eliminate bias, the interviews were carried out like natural conversations wherein the researcher did not direct the course of the interview and were fully autonomous to the interviewees so that they had ample time to elaborate on their answers.

3.11 Summary

This chapter has explained the research methodology to carry out the research. It has also justified the reason for selecting the research method, and addressed the design and implementation steps of the proposed ESAF. Furthermore, it has detailed out the evaluation technique that was used for validating the proposed ESAF. The next chapter presents the proposed ESAF.

CHAPTER 4: DESIGN OF ENTERPRISE SECURITY ARCHITECTURE FRAMEWORK

4.1 Introduction

This chapter emphasises the design of the enterprise security architecture in banking environments in detail. At an abstract level, the framework defines the key components, their interactions and the underlying components. It also describes the requirements validation of the ESAF by stakeholders.

4.2 Prioritisation of ES Practices and ESA Attributes

ES practices and ESA attributes have been identified and presented in Chapter 2, but not prioritised based on the perceived importance in the banking industry yet. The researcher conducted a questionnaire survey to prioritise the ES practices and ESA attributes.

4.2.1 Validation by Stakeholders

4.2.1.1 Survey Respondents' Demographics

An online questionnaire was prepared using Google docs and the URL was emailed to several departmental heads including chief executive officer (CEO) / chief technology officer (CTO), vice president (VP) / senior vice president (SVP), subject method expert (SME), project manager (PM)/ project management office (PMO) etc. Table 4.1 shows the distribution of respondents, which indicates that representatives from all relevant stakeholders have been covered in the survey.

Figures 4.2 to 4.4 show the demographic details of the survey respondents.

Table 4.1: Summary of the Survey Respondents

Position/Role	Distributed	Responded	(%) to total respondents
CIO/CTO/CA	20	7	7%
VP/SVP	27	12	12%
ESA/ SA/Application Architect/TA	35	21	21%
SME	21	13	13%
PM/PMO	15	8	8%
Technical lead	25	16	16%
BA	19	14	14%
Senior Engineers	26	8	8%
	188	99	

4.2.1.2 Age Group**Table 4.2:** Age Group of the Survey Respondents

Position/Role	30-35	35-40	40-45	45-50	50-60
CIO/CTO/CA			1	4	2
VP/SVP			3	7	2
ESA/ SA/Application Architect/TA	1	12	5	3	
SME		8	4	1	
PM/PMO		4	3	1	
Technical lead	3	11	2		
BA	5	7	2		
Senior Engineers	6	2			
Total	15	44	20	16	4
Percentage %	15.2%	44.4%	20.2%	16.2%	4%

4.2.1.3 Work Experience**Table 4.3:** Work Experience of the Survey Respondents

Position/Role	5-10Y	10-15y	15-20Y	20+
CIO/CTO/CA		1		6
VP/SVP		3	3	6
ESA/ SA/Application Architect/TA	1	4	4	12
SME		6	4	3
PM/PMO	3	4	1	
Technical lead	3	9	4	
BA	4	8	2	
Senior Engineers	5	2	1	
Total	16	37	19	27
Percentage %	16.2%	37.4%	19.2%	27.2%

More than 83% of the respondents have at least 10 years of work experience, 27% have more than 20% years of work experience.

4.2.1.4 Education Background

Table 4.4: Educational Background of the Survey Respondents

Position/Role	Diploma holder	Degree holder	Post Graduate holder
CIO/CTO/CA		1	6
VP/SVP		4	8
ESA/ SA/Application Architect/TA		7	14
SME		3	10
PM/PMO		2	6
Technical lead		11	5
BA		8	6
Senior Engineers	3	4	1
Total	3	40	56
Percentage%	3%	40%	57%

Nearly 97% of the respondents hold a bachelor or a postgraduate degree.

4.2.2 Validated and Prioritised Requirements

Predicated on literature review, the researcher has selected 15 security attributes as ESA attributes and 28 security practices as ES practices without prioritising them. In order to explicate the priority of the attributes and practices, the researcher utilised the industry expertise to feedback on the priorities the attributes and practices. The researcher has used a scoring system to categorise the ESA attributes and ES practices as follows:

1. For each attribute or practice, E, there are 6 possible responses (r_1 to r_6) and each response (r_i) is assigned a corresponding score S_i (where $1 \leq i \leq 6$) as depicted in Table 4.5.

2. For each attribute or practice, E, the researcher computed the fraction of each of its responses chosen by the respondents, denoted as $F(E_{r_i})$, where (where $1 \leq i \leq 6$)
3. The score for each response, $S(E_{r_i})$ is computed using the following equation:

$$S(E_{r_i}) = F(E_{r_i}) \times S_i$$

4. The researcher then computed the total score for each attribute or practice, E denoted as $T(E)$ using the following equation:

$$T(E) = \frac{\sum_{i=1}^6 S(E_{r_i})}{6} \times 100\%$$

5. Based on the total score, $T(E)$ for each attribute or practice, E, the researcher categorised the importance of each E into one out of four possible levels as shown in Table 4.6.
6. Finally, the researcher ranked the attributes and practices based on their total scores, as shown in Tables 4.7 and 4.8.

First Step – survey responses were converted into scores. Table 4.5 shows the scoring system.

Table 4.5: Mapping of Responses to Scores

Response (r)	1	2	3	4	5	6
	SA	A	SWA	SWD	D	SD
Score (s)	6	5	4	3	2	1

SA- Strongly Agree, A-Agree, SWA-Somewhat Agree, SWD-Somewhat Disagree,
D-Disagree, SD- Strongly Disagree.

Second step -Applied the formula below to get the totality.

$$\text{Total Score} = (S6+S5+S4+S3+S2+S1)/6*100$$

Third step –Ranking on Results

Table 4.6: Total Level of Importance

75%-100%	H
50%-74%	M
25%-49%	L
0-24%	N/A

H-High, M-Medium, L-Low, N/A-Not applicable.

Table 4.7: Ranking of ESA Attributes

ESA Attributes	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Authentication	0.60	3.58	0.05	0.26	0.11	0.44	0.14	0.42	0.10	0.20	0.00	0.00	81.67	H
Authorization	0.59	3.52	0.06	0.31	0.11	0.44	0.14	0.42	0.10	0.20	0.00	0.00	81.50	H
Confidentiality	0.55	3.27	0.10	0.51	0.10	0.40	0.15	0.46	0.10	0.20	0.00	0.00	80.62	H
Privacy	0.33	2.00	0.31	1.57	0.09	0.36	0.16	0.49	0.10	0.20	0.00	0.00	76.92	H
Availability	0.35	2.12	0.28	1.42	0.12	0.48	0.11	0.33	0.12	0.24	0.01	0.01	76.80	H
Integrity	0.36	2.18	0.26	1.32	0.09	0.36	0.16	0.49	0.12	0.24	0.00	0.00	76.52	H
Reliability	0.27	1.64	0.36	1.82	0.11	0.44	0.13	0.39	0.11	0.22	0.01	0.01	75.45	H
Trust	0.26	1.53	0.40	1.99	0.08	0.33	0.16	0.49	0.10	0.20	0.00	0.00	75.63	H
Audit	0.20	1.21	0.43	2.17	0.11	0.44	0.15	0.46	0.10	0.20	0.00	0.00	74.73	M
Resilience	0.22	1.33	0.41	2.07	0.10	0.40	0.15	0.46	0.11	0.22	0.00	0.00	74.73	M
Non-Repudiation	0.23	1.39	0.36	1.82	0.13	0.52	0.15	0.46	0.12	0.24	0.00	0.00	73.90	M
Anonymity	0.18	1.09	0.43	2.17	0.09	0.36	0.17	0.52	0.12	0.24	0.00	0.00	73.07	M
Accountability	0.20	1.21	0.41	2.07	0.07	0.28	0.19	0.58	0.12	0.24	0.00	0.00	73.07	M
Encryption	0.11	0.67	0.50	2.48	0.08	0.32	0.19	0.58	0.12	0.24	0.00	0.00	71.43	M
Interoperability	0.07	0.43	0.38	1.92	0.22	0.89	0.19	0.58	0.13	0.26	0.00	0.00	67.87	M
Agent Based	0.05	0.31	0.33	1.67	0.28	1.13	0.18	0.55	0.15	0.30	0.00	0.00	65.88	M

All the attributes were prioritised to have high or medium level of importance.

Table 4.8: Ranking of ES Practices

ES Practices	Strongly Agree	Score=6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	Score=2	Strongly Disagree	Score=1	Total	Rank
Security Mechanism	0.27	1.64	0.37	1.87	0.11	0.44	0.18	0.55	0.10	0.20	0.00	0.00	78.33	H
Security Policy	0.41	2.45	0.25	1.23	0.07	0.28	0.17	0.52	0.10	0.20	0.00	0.00	78.00	H
Secure Integration	0.27	1.64	0.38	1.92	0.10	0.40	0.18	0.54	0.06	0.12	0.00	0.00	77.12	H
Risk Analysis	0.34	2.04	0.30	1.52	0.08	0.32	0.17	0.52	0.11	0.22	0.00	0.00	76.93	H
Application Security	0.33	2.00	0.31	1.57	0.09	0.36	0.16	0.49	0.10	0.20	0.00	0.00	76.92	H
Data Security	0.32	1.94	0.32	1.62	0.09	0.36	0.15	0.46	0.11	0.22	0.00	0.00	76.58	H
Security Guidelines	0.28	1.70	0.36	1.82	0.08	0.32	0.19	0.58	0.08	0.16	0.00	0.00	76.33	H
Network Security	0.33	2.00	0.30	1.52	0.08	0.32	0.17	0.52	0.11	0.22	0.00	0.00	76.25	H
Standard / Compliance	0.26	1.58	0.37	1.87	0.07	0.28	0.24	0.73	0.05	0.10	0.00	0.00	76.00	H
Security Principles	0.29	1.76	0.34	1.72	0.07	0.28	0.21	0.64	0.08	0.16	0.00	0.00	75.92	H
Security Framework	0.27	1.59	0.39	1.94	0.08	0.33	0.16	0.49	0.10	0.20	0.00	0.00	75.85	H
Security Technologies	0.18	1.09	0.48	2.38	0.09	0.36	0.21	0.64	0.04	0.08	0.00	0.00	75.78	H
Access Control	0.22	1.34	0.44	2.20	0.07	0.28	0.18	0.55	0.08	0.16	0.00	0.00	75.62	H
Infrastructure	0.27	1.64	0.35	1.77	0.09	0.36	0.18	0.55	0.10	0.20	0.00	0.00	75.33	H
Security Req. Mgt	0.22	1.33	0.42	2.12	0.07	0.28	0.19	0.58	0.09	0.18	0.00	0.00	74.90	M
Security Strategy	0.22	1.33	0.41	2.07	0.08	0.32	0.18	0.55	0.10	0.20	0.00	0.00	74.60	M
Security Awareness	0.12	0.73	0.49	2.46	0.11	0.44	0.19	0.58	0.12	0.24	0.00	0.00	74.05	M
Security Threat/Model	0.16	0.97	0.47	2.33	0.08	0.32	0.19	0.58	0.10	0.20	0.00	0.00	73.35	M
Secure protocol	0.13	0.79	0.53	2.63	0.09	0.36	0.15	0.46	0.10	0.20	0.00	0.00	73.88	M
Security Roles	0.18	1.09	0.44	2.22	0.08	0.32	0.19	0.58	0.10	0.20	0.00	0.00	73.57	M
Security Analysis	0.21	1.27	0.42	2.12	0.08	0.32	0.16	0.49	0.10	0.20	0.00	0.00	73.37	M
Security Model	0.10	0.61	0.53	2.66	0.10	0.41	0.16	0.49	0.10	0.20	0.00	0.00	72.80	M
Security Metrics	0.16	0.98	0.47	2.35	0.09	0.37	0.12	0.37	0.15	0.30	0.00	0.00	72.73	M
Gap Analysis	0.12	0.73	0.50	2.48	0.11	0.44	0.17	0.52	0.10	0.20	0.00	0.00	72.72	M
Security pattern	0.12	0.73	0.52	2.60	0.08	0.33	0.16	0.49	0.10	0.20	0.01	0.01	72.72	M
Security Incident Mgt	0.14	0.85	0.48	2.38	0.08	0.32	0.20	0.61	0.10	0.20	0.00	0.00	72.55	M
Security baseline	0.13	0.79	0.48	2.38	0.10	0.40	0.17	0.52	0.12	0.24	0.00	0.00	72.05	M
Security Concepts	0.09	0.55	0.48	2.38	0.18	0.73	0.16	0.49	0.09	0.18	0.00	0.00	71.95	M

All the practices were prioritised to have high or medium level of importance.

Based on the level of priority, the researcher designed the proposed framework.

4.3 Overview of the Proposed ESAF

Figure 4.1 presents an overview of the enterprise security architecture for banking environment. The conceptual diagram illustrates the holistic view of the ESAF and it consists of six layers, which include ESA fundamentals, ESA requirements, ES core, ES assets, security integration and security governance. The framework is designed based on SABSA, COBIT and NIST.

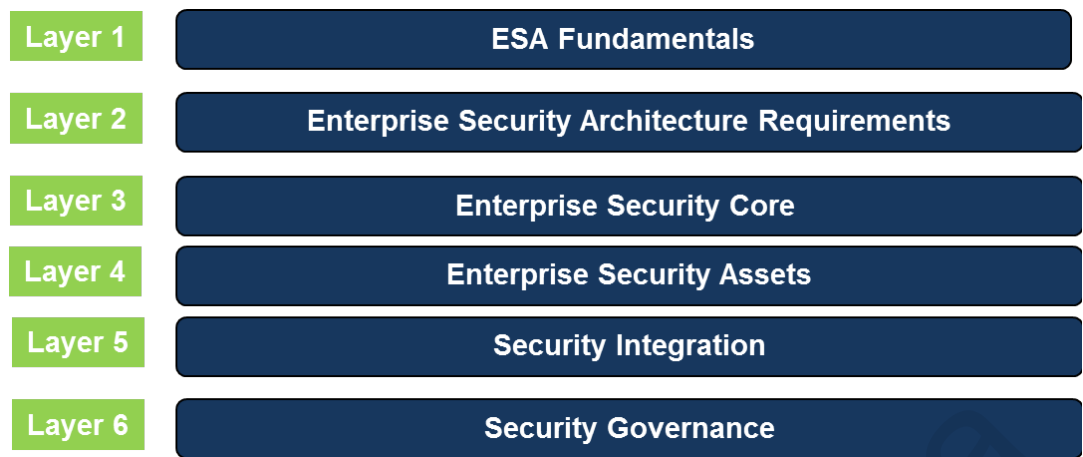


Figure 4.1: High Level ESA Framework

4.4 Detailed EASF

Figure 4.2 illustrates the major components of the ESAF for banking environment, which describes the major players, their interaction and parts. A key principle in designing the proposed ESAF is that it is mandatory to cover ES practices and ESA attributes prioritised to have high level of importance while coverage of attributes and practices with medium importance is highly recommended. Coverage of attributes and practices with low importance is optional.

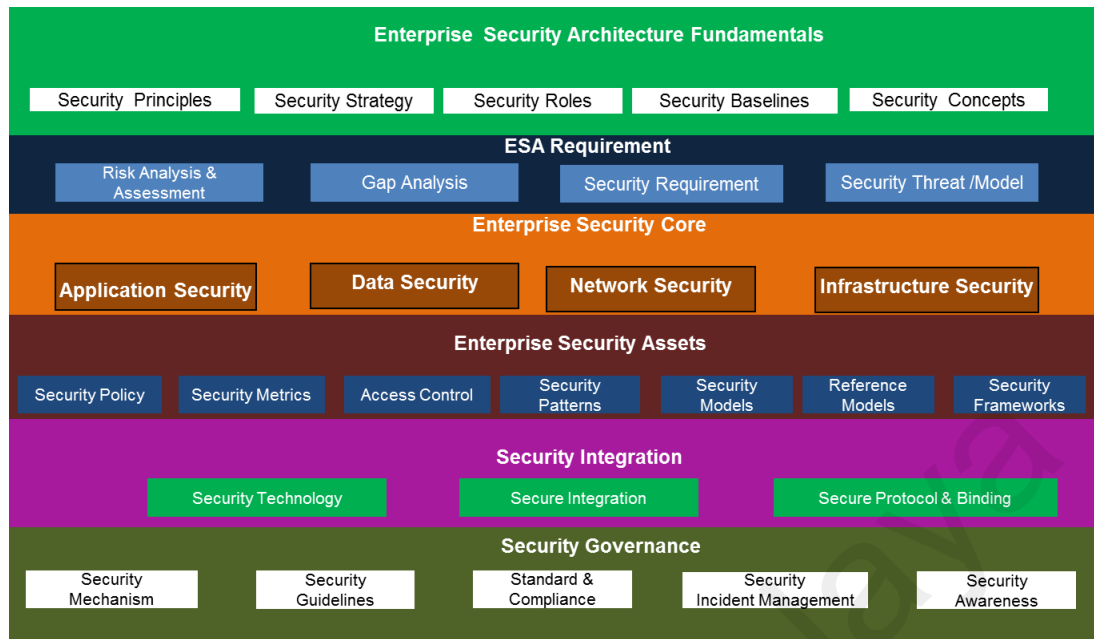


Figure 4.2: Components of ESAF

Table 4.9 shows the mapping between layers of the proposed ESAF and the 15 ESA attributes with high or medium importance. All the attributes are covered by at least 5 out of the 6 layers.

Table 4.9: Mapping between ESAF Layers and ESA Attributes

	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Layer 6
Availability	X	X	X	X	X	X
Authentication	X	X	X	X	X	X
Authorization	X	X	X	X	X	X
Confidentiality	X	X	X	X	X	X
Privacy	X	X	X	X	X	X
Integrity	X	X	X	X	X	X
Reliability	X		X	X	X	X
Trust	X	X	X	X	X	X
Audit	X		X	X	X	X
Resilience	X	X	X	X	X	X
Non-Repudiation	X	X	X	X	X	X
Anonymity	X	X	X	X	X	X
Accountability	X	X	X	X	X	X
Cryptology	X	X	X	X	X	X
Interoperability		X	X	X	X	X

Table 4.10: Mapping between ESAF Layers and ES Practices

ES Practices	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Layer 6
Security Principles	x					
Data Security			x			
Application Security			x			
Network Security			x			
Infra security			x			
Security Policy				x		
Access Control				x		
Security Framework				x		
Secure Integration					x	
Security Technologies					x	
Security Mechanism						x
Security Guidelines						x
Standard / Compliance						x
Security Strategy	x					
Security Roles	x					
Security Baseline	x					
Security Concepts	x					
Gap Analysis		x				
Security Req. Mgt		x				
Risk Analysis		x				
Security Threat/Model		x				
Security Metrics				x		
Security Pattern				x		
Reference Model				x		
Security Model				x		
Secure Protocol					x	
Security Incident Mgt						x
Security Awareness						x

Table 4.10 shows the mapping between layers of the proposed ESAF and the 28 ES practices.

4.5 Components in the Enterprise Security Architecture Framework for Banking Environment

As shown in Figure 4.2, the proposed ESAF for banking environments defines six major layers: ESA fundamental, ESA requirements, enterprise security core, enterprise security assets, security integration and security governance. Each layer takes part and accomplishes tasks in the framework.

4.5.1 ESA Fundamentals

The ESA fundamentals provide a foundation of the enterprise security architecture. An ESA fundamental is further broken down into the security principles, strategy, baselines, and concepts. Its major responsibility is to manage and control the EA stakeholders.

4.5.2 Enterprise Security Architecture Fundamental

Figure 4.3 shows the components of the enterprise architecture fundamentals cluster.



Figure 4.3: ESA Fundamentals

4.5.2.1 Security Principles

(a) *Secure weakest link*

The level of security is determined by its weakest link which the intruders are likely to attack. This weakest link should be identified and strengthened. Viega & McGraw (2001) mentioned that users including system administrator are also a major vulnerability to the system.

(b) Defence in depth

If there are multiple levels of safeguard in a security system then the gravity of security is not entirely governed by the feeble part of the system. In this situation, Viega & McGraw (2001) recommended to deploy several security layers to defend against the attacks.

(c) Fail securely

Often the system flaws contribute to the security failures. These failures should overtly be evaded in critical systems. Based on Viega & McGraw (2001), it is imperative to point out the system vulnerability and not to get compromised by a social engineering threat.

(d) Least privilege

According to Wassermann & Cheng (2003), providing the concepts that each working entity in a system must allow only the least set of authorisations that are required for it to execute its tasks. In a complex system, there are many privileged users, there tend to be a misuse of rights. Viega & McGraw (2001) recommended that it is rational to apply this security principle to eradicate the security breaches.

(e) Compartmentalise

This principle aims to achieve the same goal as the least privilege principle. It intends to reduce the destruction an attack can affect. According to Viega & McGraw (2001), a system should be divided into a number of independent cohesive components such that any breach in one does not affect the other components.

(f) *Keep it simple.*

As highlighted by Viega & McGraw (2001), to avoid complexity it is recommended to keep the security robust and as simple as possible. Wassermann & Cheng (2003) named this principle economy of mechanism. Viega & McGraw (2001) show that usability is the fundamental part of a system design.

(g) *Promote privacy.*

Privacy comprises dual objectives. The information that is planned to be collected from the users ought to be reduced to maintain the privacy (Viega & McGraw, 2001).

(h) *Hiding secrets is hard.*

In the system environment, all the time hiding the most important value component. In case intruders manage to find the private keys, they are able to expose the secret algorithms. Security can easily be compromised. Therefore, care should be taken to protect these valuable assets (Viega & McGraw, 2001).

(i) *Be reluctant to trust.*

Most security violations are possible because system developers extend trust unnecessarily. Most of the violations occur due to software engineers are unreasonably encompass the trust on their work or some of the third party components or resources. Viega & McGraw (2001) recommended that engineers to mistrust each other when designing the systems.

(j) *Using community resources*

The open design principles emphasised that community resources are secure to use when designing the systems (Wassermann & Cheng, 2003). Furthermore, Wassermann

& Cheng (2003) showed that one way of protecting algorithms is to decouple the public and private keys for their protection mechanisms thus improving their overall capability.

4.5.2.2 Security Strategy

It is a roadmap for the organisation to adapt to future security challenges. Security strategies are changing according to a trend of threats. It also becomes very complicated, multi-layered and fragmented, and thus assists the organisation to minimise the risks. In order to formulate the long-term security strategy, the organisation may need to assess their existing security status and evaluate their goals in conjunction with long-term road mapping.

4.5.2.3 Security Roles

The ESA team attends to various security services to organisations which are different from sizes, cultures, and industries. The way organisations practice ESA may be different and the strategic imperatives of their businesses are different (Lapkin, 2005). Table 4.11 displays the major stakeholders and their responsibilities.

Table 4.11: Security Roles and Responsibilities

Role	Responsibility
Business Analyst (BA)	<p>A business analyst is responsible for analysing business domain, business requirements and documenting its processes or systems, assessing the business model and conducting business impact analysis for changes in the requirements. BA describes the role as “a liaison among stakeholders in order to understand the structure, policies, and operations of an organisation, and to recommend solutions that enable the organisation to achieve its goals.” Typical responsibilities of a BA include:</p> <ul style="list-style-type: none"> • Capture security requirements • Assist on abuse use case
Technical Lead	<p>A technical lead is responsible for the fundamental of architecture for the software system, besides managing software developers and the work load of the project. A technical lead is normally a mentor</p>

	<p>for the development team. Typical responsibilities of a technical lead include:</p> <ul style="list-style-type: none"> • Conduct architecture risk analysis • Promote security oriented design • Ensure secure code practices and give orientation to developers • Train the developers for secure coding practices and SOP
Security Architect	<p>A security architect is responsible for maintaining the security of a company's systems. He evaluates all the access points of the systems and identifies the loopholes of the systems. Similarly, he recommends the best practices to secure the systems. He introduces security policies and best protocols that fit into the enterprise. Typical responsibilities of a security architect include:</p> <ul style="list-style-type: none"> • Review architecture risk analysis • Lead design secure oriented design • Introduce new security practices • Continue improvement of the system security design
CTO/CEO	<p>A CTO is an administrative level designation in a bank and he manages technological issues in the organisation. An administrative role of the CTO would often ascend of the process of automating existing activities. A CTO is the key decision maker of the ESAF implementation and also a key owner of the security program blueprint.</p> <p>A CEO is in command of managing profit in the organisation. In the security aspect, the CEO is the key decision maker for emerging security technologies and security adaptability of the systems.</p>
Project Director	<p>He is accountable for managing a project at the strategic level. He is normally the project's focal point, managing resources and finances to determine that the project progresses on time and on a budget. In the security aspect, he must ascertain that all the security standards and best practices are being followed and complied to.</p>
Software Engineers	<p>He is a person who mainly involve with the phase of the development in the systems development life cycle (SDLC) process and may participate in the design or software project management. The aspects of security responsibilities include the secure design; apply the secure coding standards and the genuine secure implementation.</p>

4.5.2.4 Security Baselines

It defines a set of elementary security objectives which are compulsory to apply by any specified services or systems. The goals are set to be sensible and comprehensive,

and do not levy technical matters. All systems or services ought to be implemented and deployed in compliance with specific security baselines.

4.5.2.5 Security Concepts

Generally, it is addressed on a trust model which encompasses the components of the system, and security goals (Gasmi et al., 2008). Security concepts associate with different fields of security such as countermeasures, assurance, risk, threat, vulnerability, exploit and defence in depth.

4.5.3 ESA Requirements

It is the key component of controls and manages the ESA requirements. In the ESAF for banking environment, activities of ESA requirement providers can be described in four major areas. As shown in Figure 4.4, an ESAF for banking environment consists of risk assessment, gap analysis, security requirement and security threat model.



Figure 4.4: ESA Requirements

4.5.3.1 Risk Analysis and Assessment

The ISO-17799:2005 presents guidelines and best practices for organisations to use when conducting risk assessments. The aim of risk assessment is to assess the risk related situation and identify the threat. The quantitative risk assessment calculates the risk of the potential loss and the probability of the loss. The method of risk assessment diverges and it depends on the industry. The risk analysis is intended to separate explicit and typical events that affect an organisation. By evaluating and monitoring risk nature, business activities are able to classify the security risks.

4.5.3.2 Gap Analysis

The gap analysis identifies information security gaps that may happen within an organisation. It investigates the current information security standpoint to industry best practices or standards and regulations. It can frequently identify capabilities that already exist within an organisation, offer the ability to promote these capabilities rather than adopt new ones. Gap analysis can help find and mitigate problems and provide recommendations and the solution on how to fix them. Since it enables long-term planning by setting goals and outlining changes and practices. The ultimate goal of a gap analysis is to gain a list of prioritised activities that an organisation can complete to move closer to its vision.

4.5.3.3 Security Requirements

The security requirements fall into the category of non-functional requirements. It is related to all the security attributes such as system confidentiality, integrity, and availability. Overtly declaring security requirements throughout a project's initial stage is the impeccable complement to security testing. Visibly charting impending security requirements at the beginning of the project allows development teams to make compromises about the cost of adding security into a project. It can also be expressed on different notion levels. Security requirements can be categorised as follows:

Secure Functional Requirements- these security requirements are identified and documented in the functional requirements specification. Generally, the misuse cases capture and elucidate these requirements.

Secure Development Requirements- these requirements state that software development should be carried out by rigorously tighten the development cycle and close all the vulnerabilities.

4.5.3.4 Security Threat Models

(a) *Threat Modelling*

Threat modelling was introduced by Ford Motor company to support between IT security and control and its business users' analysed threat, to better understand the risks. It helps to understand the possible threats and vulnerabilities of the system environment and assets. In this process, analysts will be able to quantify the risks and be able to make a decision on which assets need utmost and least protection and allocate the organisation resources accordingly (Ingalsbe, Shoemaker, Mead, & Drommi, 2008). There are four types of threat modelling available: systematic or not systematic, scenario based, mathematical, and automated. Furthermore, there are two threat modelling introduced by Microsoft: the systemic methodology which focuses on data flow and system trust boundaries; and Threat Analysis and Modelling (TAM) methodology which is based on application usage scenarios (Myagmar, Lee, & Yurcik, 2005).

(b) *STRIDE*

The STRIDE is a methodology for detecting possible threats. This methodology is generally utilised by Microsoft for threat modelling of their systems. The STRIDE acronym is composed of the first letter of each of the following categories, which include spoofing, tampering, repudiation, information disclosure, DoS and elevation (Talukder & Chaitanya, 2008). Table 4.12 further elaborates the possible threats and countermeasures.

Table 4.12: Threats and Countermeasures

Threat	Countermeasures
Spoofing user identity	<ul style="list-style-type: none"> • Facilitate multi step authentication process. • Avoid saving passwords in notepad or files. • Avoid transfer user credentials in plain text format over electronic communication. • Bulwark authentication cookies with SSL.
Tampering with data	<ul style="list-style-type: none"> • Apply data security practices like hashing and digital signatures • Apply secure protocols on electronic communication especially message integrity checks.
Repudiation	<ul style="list-style-type: none"> • Use and apply secure audits and maintain the audit trails by using digital signatures
Information disclosure	<ul style="list-style-type: none"> • Use multi-step encryption and authorisation process. • Ensure secured communication protocol usage • Use and apply strong hashed passwords policies.
Denial of service	<ul style="list-style-type: none"> • Use and apply network throttling mechanisms that can validate and filter the network usage.
Elevation of privilege	<ul style="list-style-type: none"> • Use and apply the lowest privileged services accounts to execute user processes and resource accessibility.

(c) DREAD

The DREAD methodology infers to Damage, Reproducibility, Exploitability, Affected users, and Discoverability. It is used to define impending threats and their impact on the business with subsequent risk mitigation (Talukder & Chaitanya, 2008).

(d) Attack Tree

An attack tree is the system security tool that evaluates the system threats. It identifies all the potential vulnerabilities which may destruct the assets. By using an attack tree, users are able to emulate and foresee the various events of attacks (Moore, Ellison, & Linger, 2001).

(e) *Attack Surface*

Fundamentally, the attack surface is a combination of protocols, services, and interfaces. In a secure design, it is used to analyse the expanse of the attack and its subsequent assessment. It achieves this by identifying the vulnerabilities in the system design and patching them up by reducing unnecessary code (Talukder & Chaitanya, 2008).

4.5.4 Enterprise Security Core

The enterprise security core is the heart of the Enterprise architecture security framework for banking environments. As EA security grows, the managing of EA security can be too complex for the banking environment. An enterprise security core is an entity that manages and implements modules of banking systems. As shown in Figure 4.5, the enterprise security core consists of four components:

Application Security: Application security modules and components enhance a provided service by refining some explicit competence and given value added services to banking users. The improvements include governing and controlling access to components and application modules setting, identity management, performance reporting, and enriched security.

Network Security: The network security modules and components combine and integrate multiple services into the system. The network security provides secure data transmission protocols and confirms the protected data communication and movement between the banking users and third party financial service providers.

Data Security: The data security provides comprehension of the ESA requirements of data security platform, which is a detailed coverage of data-centric security

architecture, for diminishing the attack surface of confidential data and its compliance requirements.

Infrastructure Security: Infrastructure components and devices that enrich a provided service by refining some explicit competence and giving value added services to banking users. The improvements include managing access to infrastructure and its devices, which include servers, switches, routers, hosting services, data centre facilities, etc.

The enterprise security core consists of four components, which include application security, data security, network security, and infrastructure security.



Figure 4.5: Enterprise Security Core

4.5.4.1 Application Security

Firstly, a security policy is put in place to begin with information security which is then applied to the application security. Since applications are to be treated as resources, this has more risks than any other levels. There are two major components to be accomplished: application security life cycle (ASDLC) and secure interoperable infrastructure components. The security vulnerabilities at the application level can be improved by cohesive coding and secure architectural design.

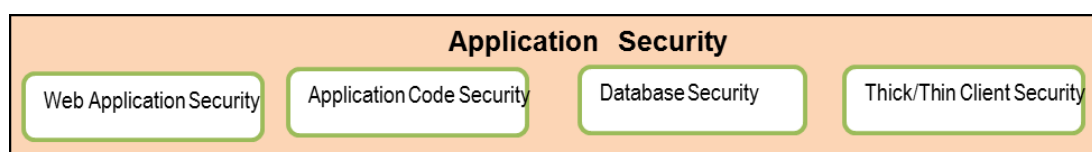


Figure 4.6: Application Security

As shown in Figure 4.6, the application security consists of four components, which include web application security, application code security, data security, and thick/thin client security.

(a) ***Web application security***

Security team has to carry out a multiple levels of assessment to govern security requirements to identify the impacted application, data or network domain. Vulnerability assessment techniques are needed to carry out tasks such as web application assessment. These assessments encompass evaluating web or application security vulnerabilities and accommodate the proactive assessable recommendations.

(b) ***Application code security***

Technical lead has to prepare the secure code standards suited for their banking environment. They have to refer to industry best practices and governing bodies that recommend secure code standards such as OWASP etc. Similarly, they have to perform the programming code review to identify the poor code standards and vulnerabilities such as the back door of the systems. Generally, application code review is to validate the secure application design and implementation. It aids to mitigate the risks at the early stage of the development and consistency in design throughout the development.

(c) ***Database security***

Security team has to implement the assessment of the security configuration of a database identity, the known drawback of the database account settings, and privileges such that not to allow unauthorised user access to the data. The secure database testing process embraces with secure database configuration, protection, and assessments of databases attacks, secure passwords, third party software vulnerabilities in databases.

(d) ***Thick and thin client security***

Thick client assessment has to examine and review the sever side controls and data transmission path between client and server and secure tunnel. It is necessary to review critical path of the data communication between the server and clients, data exposure and encryption vulnerabilities. Moreover, this process has to review and examine handling of memory, files, and registry of the sensitive data disclosure. Thick and thin client assessment have to contain bypass authentication and authorisation controls, network components or permissions.

4.5.4.2 Data Security

The data security gives an outlook of the architectural underpinning of the exclusive platform. It is a wide-ranging resolution that aims at mitigating the attack surface of sensitive data. It is abiding by the data compliance requirements. In order to work effectively, it makes use of other components like firewall, data encryption, access controls and security intelligence appliances.

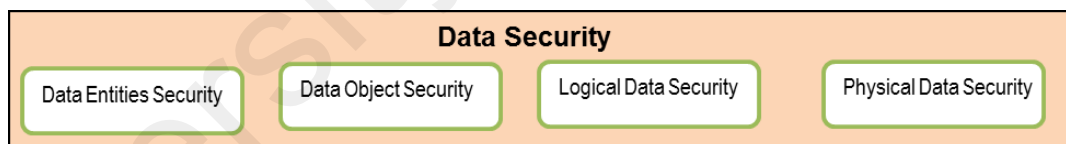


Figure 4.7: Data Security

As shown in Figure 4.7, the data security consists of four components, which include data entities security, data object security, logical data security, and physical data security.

(a) ***Data Entities Security***

It signifies a data subject from the common data model that is used in the logical data model. It also defines the components outlined in a logical security data model. A logical data model is a mirror of the entire organisation's data which are systematically

structured in terms of data administration technology. Logical security data model should sternly follow the structures recognised and defined in the conceptual data model as it defines the semantics of a business.

(b) ***Data Object Security***

Data object security provides access to dimensional objects. Data architect must set object security before other users can access them. Data object security is implemented using SQL GRANT and REVOKE.

(c) ***Logical Data Security***

This element focuses on the logical structure of the database design. It fully depends on security attributes such as authorisation, authentication, encryption, and passwords.

(d) ***Physical Data Security***

It is an essential part of any organisation's entire data security strategy. These strategies include guards, video surveillance, tracking and monitoring facilities and storage technology. These controls come along with physical access control technologies, authentication, and monitoring which consist of card key or biometrics scanning systems to access the organisation's sensitive data.

4.5.4.3 Network Security

The network security is the process of compelling physical and conducting software preventative assessment to defend the fundamental of networking infrastructure. It prevents from unauthorised user access, misuse of authentication, malfunction, modification of data, system destruction, or improper data and packet disclosure. It helps to create a secure platform for users and programs in a secure environment. It is particularly based on any activities intended to safeguard the organisation's network.

These actions safeguard the usability, reliability, integrity, and safety of the banker's data transmitted over the network. A network security system usually consists of many components. It is a piece of component consists of anti-virus and anti-spyware, Firewall, IPS, and VPNs as depicted in Figure 4.8.

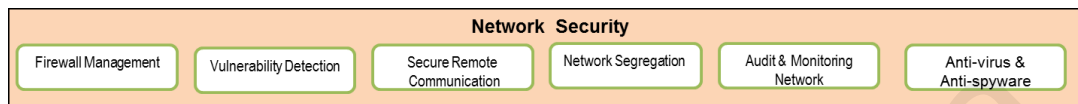


Figure 4.8: Network Security

(a) ***Firewall management***

This is a resource intensive task and requires a high level of expertise to prevent unauthorised access. The firewall management systems permit to provision, deployment, upgrade and patch to keep the organisation up with the latest threats. It offers 24x7 firewall administration, log monitoring, and device health check. Moreover, it should strengthen policies and analysis of firewall logs periodically.

(b) ***Vulnerability detection***

Vulnerability detection facilitates automated vulnerability scans daily or periodically or on the ad-hoc basis. It records down entire results and produces vulnerability trends patterns for all the WAN, LAN or a single IP address.

(c) ***Secure remote communication***

It implements an SSL VPN to help meet the remote access needs of banking staff. This secure communication helps to preserve data confidentiality and integrity when transmitted across the Internet. The protocol allows banking users to connect to the banking network via a VPN client software or web browser capable of using SSL encryption. The SSL VPN allows access to banking systems and computing resources with an Internet connection in a safe and secure manner.

(d) ***Network segregation***

It splits a whole network into sub networks. Gains of such splitting are predominantly boosting the security and also “zoning” to provide effective controls to limit further movement across the network. Segregation is achieved by a combination of firewalls and VLANs (Virtual Local Area Networks). Software-Defined Networking (SDN) allows the creation and management of micro-segmented networks. VLAN is important to their application servers because of the confidential nature of the information they process and store. Banking users can be segregated by departments, their roles and operations such as server administrators, security administration, managers, and executives. The Payment Card Industry Data Security Standard (PCI-DSS), and similar standards provide guidance on creating a clear separation of data within the network.

(e) ***Audit and monitoring network***

Network auditing is a vital task in a banking environment. By doing audit, security auditors are able to identify vulnerabilities and threats, and send a formal audit report to network administrators. Networks are dynamic entities, which grow, shrink, change and split themselves continuously. Likewise, network administrator and security teams perform regular network auditing and monitoring of any changes to the pre-set baseline. It is necessary to support and control all the network security layers.

(f) ***Anti-virus & Anti-spyware***

Perhaps one of the most irritating and disturbing attacks on cyber security is the virus attack. In order to keep the banking system secure, specialised software called anti-virus software is used. It is software that usually prevents, detects and removes the malicious software. These virulent software codes come in a variety of formats like malicious

BHOs, browser hijackers, ransomware, keyloggers, backdoors, rootkits, Trojan horses, worms, malicious LSPs, diallers, fraud tools, adware, and spyware. The anti-virus software has effective heuristic mechanisms in place to combat against these.

4.5.4.4 Infrastructure Security

Infrastructure security architecture consists of banking IT infrastructure, network traffic and communication systems. It prepares a security policy, processes, procedures, and implements secure infrastructure plan, obtains approval process from the senior management, implement security policies and plans, maintain a standardised documentation of the entire IT infrastructure, periodically tests and audits the entire banking network security (The Internet, Intranet, and Extranet), update the network regularly, and maintain an audit trail of all changes, and create security awareness among users.

Secure Infrastructure component consists of four secure elements:

- **Infrastructure security boundary defence**

It includes setting up and maintaining internet service provider (ISP), firewalls, routers and proxy servers and DMZ zone

- **Operating systems and servers protection**

This holds server hardening, which includes updating filters and patches / service packs / hotfixes on a regular basis.

- **Host infra protection**

Internal workstation set up and connection to banking backbone.

- **Infrastructure data transmission protection**

This element includes end user access device security and data encryption covers

4.5.5 Enterprise Security Assets

An EA assets component controls and manages the EA assets. In the enterprise security architecture framework for banking environment, activities of the enterprise architecture asset security providers can be described in seven major areas: security policy, security metrics, access control, security patterns, security model, reference model, and security framework as depicted in Figure 4.9.



Figure 4.9: Enterprise Security Assets

4.5.5.1 Security Policy

This is the most important document that gives in writing on how an organisation plans to protect the company's physical and information technology (IT) assets. It is often considered to be a “living document”, which infers that it will be continuously updated to cope with the upcoming threats and their removal. This document also includes a comprehensive treatment of employee education towards cyber security threats and correction mechanisms in place.

4.5.5.2 Security Metrics

A metric is a system of similar measures to enable quantification of some characteristic. A measure is a dimension compared against a standard. Thus, security metric is a system of related dimensions (compared against a standard) enabling quantification of the degree of freedom from the possibility of suffering damage or loss from malicious attack. Security metric can be measured by TCSEC (Orange book), ITSEC (Europe's Orange book), CTCPEC (Canada's Orange book), Common Criteria, SSE-CMM, NIST FIPS-140 series, and NIST SP 800-55.

4.5.5.3 Access Controls

Access control is about granting access to the authorised personnel and preventing an unauthorised user to access. Access to accounts can be enforced through many types of controls (Joshi et al., 2001). Table 4.13 shows selected access control models.

Table 4.13: Type of Access Control

Approach	Characteristics
DAC	<ul style="list-style-type: none">• It is based on ownership and most widely used approach. Major drawback is that low assurance and doesn't provide a high security.• In contrast with the RBAC, it is able to deliver dynamic alteration and task oriented controls• It is compulsory to use classification levels
MAC	<ul style="list-style-type: none">• It is completely based on administration• It deliberately uses the control rules.• It is difficult to make adjustment but it gives intensive assurance and security.
RBAC	<ul style="list-style-type: none">• It is easy to make change and give more flexibility• It complies with principle of least privilege and managing perspective.• It is highly reliable with new technologies and also supports multi domains
Access control task and workflow	<ul style="list-style-type: none">• Task based security authorisation model• RBAC immensely useful for WFMS• The most vital element of transaction oriented
Hypertext based authorisation	<ul style="list-style-type: none">• It is rely on hypertext model• It is copiously provide security for Web objects
Certificate based	<ul style="list-style-type: none">• It is use of current PKI facility• It is matched with host access control• It can facilitate the trusty Web
Agents	<ul style="list-style-type: none">• It provides flexibility of adaptation and mobility• Itinerant agents managed to find new security disputes• It provides a complementary system development approach• It is beneficial for multi domain settings

4.5.5.4 Security Patterns

Design patterns are built for the different purposes to achieve information security goal. The patterns are generally equipped with security attributes such as confidentiality, integrity, and availability. According to the need of security, the requirement has to select the suitable security pattern. Otherwise, it will become an anti-pattern. The security patterns assist to construct end-to-end security into multi-tier enterprise applications, XML-based Web services, and allow identity management in Web applications. It helps to implement single sign-on authentication, multi-factor authentication and enable identity provisioning in web-based applications (Steel, Nagappan, & Lai, 2005).

4.5.5.5 Security Models

The security model is an essential security feature to be facilitated by a system. It should include in depth specifications which allow and forbid relationships between subjects and objects. It outlines the necessary logic and rules to be implemented. It also addresses the high-low level grant criteria for the users. It provides comprehensive guidance to implement the security policy in the system (Fultz & Grossklags, 2009; Joshi et al., 2001).

4.5.5.6 Reference Models

It is an abstract framework or domain-specific ontology comprising of an intertwined set of noticeably outline concepts created by an expert in order to boost clear communication. It characterises the complete set of system components and business functions. It also helps to communicate thoughts evidently between associates of the same community (Bass & Mabry, 2004).

4.5.5.7 Security Frameworks

The security framework consists of people, technology, and process to achieve an organisation's business objectives and secure environment. It also makes sure that policy definition, enforcement, measurement, monitoring, and reporting are in place. Moreover, it must include security attributes such as confidentiality, integrity and availability (Kark, Stamp, Koetzle, & Mulligan, 2007).

4.5.6 Security Integration

The security integration component controls communication with third party systems. In the ESAF for banking environment, activities for security integration provider can be described in three major areas: secure integration, security technologies and secure protocol and binding as depicted in Figure 4.10.



Figure 4.10: Security Integration

WSDL: The web service description language is a contract language used to declare web service interfaces and access methods using specific description templates (Vernadat, 2007). The webservice security standards include WS-policy, WS-security, WS-trust, WS secure conversation, WS reliable messaging, and WS atomic transaction (Meier et al., 2003).

(a) *Web Server SSL/TLS Encryption*

Encryption techniques vastly facilitate the data privacy and secrecy. The most widely utilised protocols are SSL and TLS. Generally, it implements the data encryption at the web server level to protect external or third party system connection.

(b) Web Service Security (WS-Security)

WS-security can be implemented at the gateway to protect the inbound and outbound messages through the third party. It also implements WS-Security using username tokens or Security Assertion Mark-up Language (SAML) tokens.

(c) WS-Security using Username Token Profile

The WS-Security Username Token Profile defines a standard way of identifying the requested users with their username and password to authenticate the system. In this practice, inbound and outbound messages exchange the tokens through the secure gateway.

(d) Web Service Security using SAML Token Profile

The SAML Token Profile uses assertions to define a standard way to associate common information such as issuer ID, assertion ID, subject and so on.

4.5.6.1 Security Technology

Security technology provides essential tools for safe communication and protection of data. It is the process of measurement implementation to secure and protect data breaches. These technologies include a combination of computer hardware and software resources. Besides, there is an XML security standard which falls under the software net and provides a practical and feasible solution.

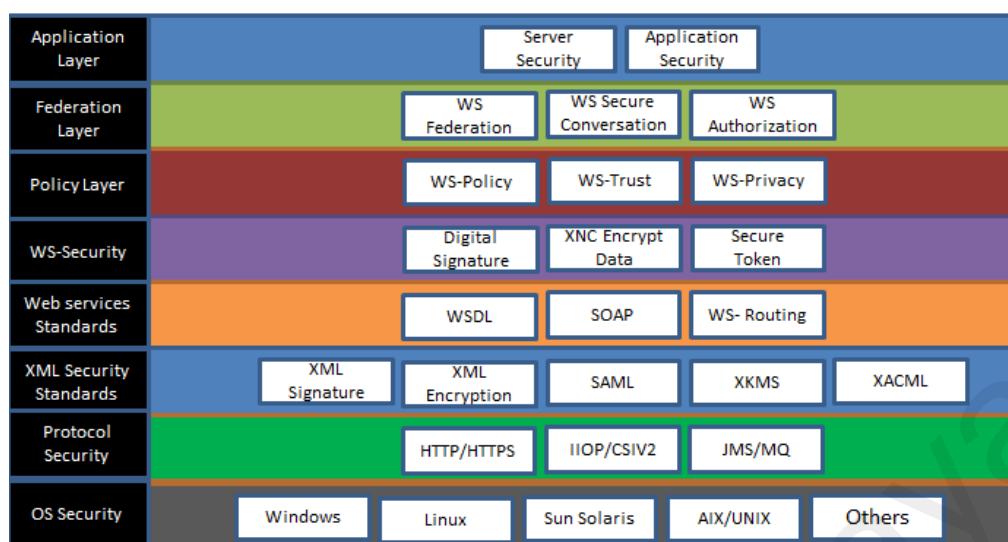


Figure 4.11: Security Technology Stack

Figure 4.11 illustrates the layering of security technology and standards that exist today and how they fit into the security model.

Security is an integral part of a network. A network has many layers. The security provided at each layer is as follows: at network layer these are IPsec, SSL [SSL] or TLS: At the binding layer, it is HTTPS, in the case of IIOP, it can be provided by CSIV2. At the messaging layer, it is provided by a message provider. In using XML as a security component it is given by XML Digital Signature, XML Encryption, XML Key Management Service (XKMS), and assertion languages (e.g., SAML). In the case of SOAP payloads, security is based on WS-Security.

4.5.6.2 Secure Integration

Secure integration establishes the trusted connection between internal and third-party systems. Secure integration brings enterprise systems together. Enterprise is able to design, construct and maintain stand-alone and integrated security systems and communication networks with third party systems in a secure manner (Norman, 2014).

4.5.6.3 Security Protocol and Binding

A security protocol is a concrete protocol that performs a security-related function and applies cryptographic methods. The protocol includes details about data structures and representations. It is also used to implement multiple, and compatible and interoperable versions of a program. The security protocol is extensively used for secure application development and data transportation. The cryptographic protocol commonly integrates with security attributes.

4.5.7 Security Governance

The security governance, in a nutshell, involves policies and process that make it possible to use information efficiently and effectively. The ultimate goal of security governance is to help a business or any type of organisation achieve its objectives.

In addition to addressing legal and regulatory requirements, effective information security governance is simply good business and provides a series of significant benefits, including:

- Addressing the increasing potential for legal liability of the organization and senior management as a result of information inaccuracy
- Providing assurance of policy compliance
- Increasing predictability and reducing uncertainty of business operations by lowering risk to definable and acceptable levels
- Providing the structure and framework to optimize allocations of limited security resources
- Providing a level of assurance that critical decisions are not based on faulty information

- Providing a firm foundation for efficient and effective risk management, process improvement, rapid incident response and continuity management
- Providing greater confidence in interactions with trading partners
- Improving trust in customer relationships
- Protecting the organization's reputation

The security governance components govern the compliance and regulation. In the ESAF for banking environment, activities of security governance providers can be described in five major areas: security controls, security guidelines, standard and compliance, security incident management and security awareness as depicted in Figure 4.12.



Figure 4.12: Security Governance

4.5.7.1 Security Mechanism (Control)

Security controls are the safeguard to the organisation to prevent and diminish the loss. It also provides the counter measurements for specific vulnerabilities. Security control is equipped with wide range of disciplines which are administrative and preventive measurements, technical detection and correction and detective controls. As reported by the government accountability office (GAO) (Dacey, 2010), the control environment sets up the platform for an organisation, implies the control awareness of their people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment strictly manages the integrity and ethical values and maintains assigned authority of people.

4.5.7.2 Security Standards, Guidelines and Best Practices

The security standards enable organisations to practice safe security techniques to stop security attacks. These guidelines provide general outlines as well as specific techniques for implementing security. Following are some of these standards: (Talukder & Chaitanya, 2008)

(a) *Common Methodology for IT Security Evaluation (CEM)*

It delivers solid direction to assessors to apply and understand content and presentation. The target group of evaluators are sponsors, developers, and other parties (Tipton & Krause, 2003).

(b) *Common International Standard (ISO/IEC 15408)*

The ISO/IEC 15408 assures confidence against security functionality of IT products by providing a communal set of requests to be seen in those products during the security evaluation. These guidelines are also followed during building, examination and/or releasing the product for the function of security. Any product with this ISO/IEC 15408 standard fulfils three types of security attributes: confidentiality, integrity and availability, by providing assets protection from unauthorised disclosure, modification or loss of use. ISO/IEC 15408 considers risks from both human and non-human activities (Baggen, Correia, Schill, & Visser, 2012).

(c) *Basel III*

Basel III is a comprehensive framework for banking sector to measure and strengthen the regulations to properly govern the banking system (Chabanel, 2011). Basel III introduces measurements to mitigate the risks and improve the risk governance. Furthermore, it governs the regulations which helps to improve the banking resilience for a period of time (Harle et al., 2010).

(d) **COBIT 5**

The COBIT 5 is a business framework for the governance and management of enterprise IT. It incorporates the up-to-date enterprise governance and management techniques, principles, best practices, analytical tools and models to increase the trust and awareness of the information systems. The usage of COBIT 5 helps in all types of enterprises to sustain and achieve business strategic goals and to eliminate the high risk (De Haes et al., 2013).

(e) **ISO 21188:2006**

ISO 21188:2006 provides two important functions. Firstly it defines a requirement framework that will help to manage a public key infrastructure (PKI) based on certificate policies. Secondly, it enables the usage of PKI certificate in any financial service industry. It is planned to support implementers to outline the PKI practices. It also enables a number of certificate policies, which include the usage of the digital signature, remote authentication, and data encryption (Dimitriadis, 2007).

(f) **FISCAM**

This standard is typically used in financial planning and audit performance and attestation engagements as in the US Government Auditing Standards. It consists of the top-down, risk based approaches that consider the significance and effectiveness of audit procedures and their influence on audit risks, evaluation of general controls and their pervasive impacts on business process application controls, as well as security management at all levels (Dacey, 2010).

(g) **National Institute of Standard and Technology (NIST)**

NIST (US) is tied up with different security standards (Linstrom & Mallard, 2003). NIST works with PKI, advanced authentication systems, biometrics, public key

cryptographic techniques, cryptographic protocols and interfaces, public key certificate management, smart tokens, cryptographic key escrowing, and security architectures (Talukder & Chaitanya, 2008).

(h) ***CERT***

CERT assists software developers and consultants to eliminate the vulnerabilities of the programming coding. It gives a set of wide-ranging guidelines on the coding error and security standards, and best practices to implement the secure programming (Davis, Humphrey, Redwine, Zibulski, & McGraw, 2004). CERT also supports the built-in British Standard Association (BSI) software assurance, which includes the best security practice, tools, and principles. CERT also provides a guidance to build the secure software in each of the software development life cycle (Talukder & Chaitanya, 2008).

(i) ***ISO 17799***

ISO 17799 security standard provides a model and process to efficaciously manage information security. This standard defines the requisites for establishment, implementation, operation, monitor, review and maintenance (Von Solms, 2005). The ISO 17799 is structured into 10 major sections, covering areas like personnel and organisational security, security policy, asset classification including communications and operations management and system development and others (Talukder & Chaitanya, 2008).

(j) ***Public-key Cryptographic Standard***

PKI is a widely used standard in the banking industry which comprises mechanisms to securely distribute security keys. The standard supports advanced encryption standard and transport layer security (Cramer & Shoup, 1998). The symmetric-key and public-

key techniques are applied in most security protocols such as SSL and S/MIME (Elgamal, Treuhaff, & Chen, 1996).

(k) *Open Web Application Security Project (OWASP)*

The OWASP is introduced by Open Community to improve the secure application development. OWASP also forms a set of standards to define baseline approaches and establish a security assessment for the application development (Talukder & Chaitanya, 2008). The objective of OWASP is to help the stakeholders on the dangers attached to websites with security threats. OWASP gives a platform for industry expertise and academicians to collaborate and work together to build a conducive and cohesive environment.

(l) *Organisation for the Advancement of Structured Information Standards (OASIS)*

This standard helps in building up the software development cycle, providing with the convergence and adoption of standards that are open source thus helping for the global information society. The implementation of OASIS helps establish secure web standards for e-business in both public and application level hubs (Talukder & Chaitanya, 2008).

(m) *System Security Engineering Capability Maturity Model (SSE-CMM)*

This standard was developed with the objective of advancing security engineering as a defined, mature and measurable discipline. The implementation of this framework helps in mitigating any security loopholes and establishes a trusted product life cycle throughout from its installation to maintenance and subsequent decommissioning (von Wangenheim, Hauck, Salviano, & von Wangenheim, 2010).

(n) ***EALs***

EALs provides the numerical grade for information technology products and systems. This assurance level reflects the assurance requisite which ought to be fulfilled to achieve Prevalent Criteria certification. Although the EAL level does not quantify the security of the system itself, it only quantifies the security system readiness to this assurance level (Falcioni, Ippoliti, Marcantoni, & Re, 2013). The EALs involve stringent documentation, analysis, and testing processes (Joshi, Yesha, Finin, & Yesha, 2013). It is worth noting that a banking product with a greater EAL cannot be considered “more secure” in a specific application than one with a lower EAL, because of varied functional features in their Security Targets (Smith, 2007).

4.5.7.3 Law & Regulations

(a) ***1986 Computer Fraud and Abuse Act (CFAA)***

This act safeguards the interests of the government and financial institutions of the US. It is due to this act that accessibility to any protected computer without authorisation is deemed a federal crime. It has been used proactively to prosecute hackers to help safeguard trade secrets and other proprietary information (Field, 2009).

(b) ***Data Protection Act (UK)***

The Data Protection Act 1998 outlines UK law on the processing of data on classifiable living people. It governs the safeguard of personal data in the UK. In practice it provides a way for individuals to control information about themselves (Beyleveld, 2007).

4.5.7.4 U.S Laws Pertaining to Hacking

(a) *1973 U.S. Code of fair information practices*

This code of practice addresses the automated data systems. It fully governs the computerised personal data systems, records, computers, and the privileges of citizens (Garfinkel, 2002).

4.5.7.5 Regulatory Laws

(a) *2000 Graham-Leach-Bliley Act (GLBA)*

In order to maintain the safeguarding of such private user financial data the GLBA provides inhibited privacy protections against the sale of users' private financial information (Fay, 2007).

(b) *2001 USA Patriot Act*

This act is widely known as "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001". It has a clause that allows wide ranging jurisdiction abilities to law enforcement agencies to examine the telephone and e-mail communications, medical, financial, and other records; relieved restrictions on overseas intelligence collected within the United States (Sinnar, 2003).

(c) *2002 Federal Information Security Management Act (FISMA)*

The FISMA outlines an all-inclusive framework to shield the government information, operations, and assets against natural or man-made threats. It entrusts responsibilities for numerous agencies to safeguard the confidence of data in the federal government (Kim & Solomon, 2013).

(d) ***2003 Sarbanes-Oxley Act (SOX)***

SOX is protects the stakeholders of the organisation and the public for any of wrong doing activities such as fraud. It also improves the accuracy of the records and its disclosure. SOX addresses the methods of storing financial and IT records. It is states that which records are stored and duration of the storage. SOX acknowledged that all electronic records must be kept for at least five years (Tarantino, 2008).

4.5.7.6 Non-U.S. Laws Pertaining to Hacking

The United States is not the only country to have computer crime laws. Those at the forefront of prosecuting computer crime are Australia, Canada, France, Germany, Iran, Japan, North and South Korea, and the United Kingdom.

(a) ***UK Computer Misuse Act of 1990***

The act makes certain activities illegal, such as hacking into other people's systems, misusing software, or helping a person to gain access to protected files in someone else computer. Its goal was to discourage behaviour on hacking in the future (Welch, 1999).

4.5.7.7 Cyber Laws of Malaysia

(a) ***Computer Crime Act 1997***

The Act intends to offer for offenses connecting to the abuse of computers. Besides, it provides lodgings with unauthorised entrance to computer material, determined to commit other offenses and alteration of electronic contents (Librero & Arinto, 2007).

(b) ***Malaysian Communications and Multimedia Commission Act 1998***

The MCMC is the regulatory body for communication and multimedia industry. The role of this act is to enforce the national policy for communication and multimedia

sector. In addition, the MCMC is accountable for internet activities (Brown, Hossain, & Nguyen, 2005).

(c) *Digital Signature Act 1997*

This act aims at promoting all the electronic transactions to use digital signature. It also enables the law for ecommerce by giving an opportunity for online secure transaction through the practise of digital signature. It also offers a framework for the authorities, and to identify the digital signatures (Mazziotti, 2008).

(d) *Copyright Act (Amendment) 1997*

The act states that transmission of copyright works over the Internet is a breach of copyright. It is also an infringement of copyright to circumvent any effective technological measures aimed at restricting access to copyright works. It safeguards the intellectual property rights for companies taking part in content creation in the ICT environment (Mazziotti, 2008).

(e) *Optical Disc Act 2000*

The act is to oversee the running of optical discs operation, which was identified as the main source of privacy. The role of optical disc legislation is to supervise and monitor legitimate replication operations through the giving out of licences and conducting routine inspections to ensure compliance (Campbell & Campbell, 2009).

(f) *Electronic Transactions Act 2006*

This act protects the electronic commerce regulation for the private and public sector (Mason, 2012).

4.5.7.8 Security Incident Management

It is intended to provide the computer systems for monitoring and detecting security events, unauthorised access, security breaches, and incidents related to the security standards, compliance and practices. These incidents are reported and documented for investigation and further studies. These incidents are vital to management to prepare for future threats and vulnerabilities of the systems. It also helps to review the existing systems and practice to continue improvement. Some cases are escalated to the top management for review and attention (Anderson, Compton, & Mason, 2004; Standardization & Commission, 2005).

4.5.7.9 Security Awareness

The security awareness programmes provide the knowledge to organisation members and cover the physical and informational assets of the organisation. Organisations need to carry out awareness programmes periodically to ensure that all staff are aware of security controls and measurements. It is also an appropriate communication tool to assess the participant's understanding of the security controls and practices (D'Arcy, Hovav, & Galletta, 2009).

4.6 Relationships between Components in the ESAF for Banking Environments

In the ESAF for banking environment, users request services from the enterprise security core and security integration. The other four layers including the ESA fundamentals, ESA requirements, enterprise security assets, security governance are embedded in the framework. By this architecture, the actual ESA components are invisible to the banking users and all the stakeholders. Therefore, they are interacting directly with the enterprise security core and security integration (Figure 4.13).

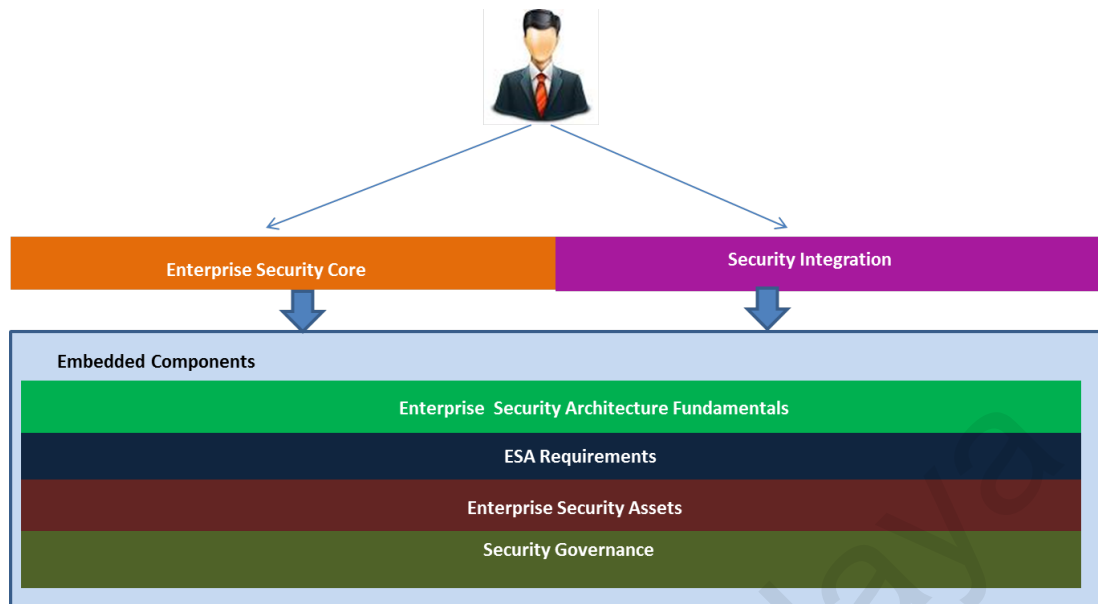


Figure 4.13: Relationships between Components in the Enterprise Security Architecture Framework for Banking Environments

4.7 Banking Top Issues and Countermeasures from ESAF

Table 4.14 shows how the proposed ESAF is able to address top 10 issues to verify that banking attacks through its layers and components.

Table 4.14: Mapping between ESAF Layers and Banking Attacks

Issue	ESAF Layers and Component	Countermeasure
1. Malware Attack a. Trojan Horse b. Virus c. Virus Hoax E-mail d. Worm e. Spyware f. Keystroke Capturing /	Layer 1 -Security Roles, Security Baselines, Layer 2 - Gap Analysis, Security Requirements, Risk Analysis, Treat Model Layers 3 -Application Security, Network Security components- (Anti-virus and Anti –Spyware Module, Firewall Management, Vulnerability detection, Audit & Monitoring Network) Layer 4 -Security Policy, Access Control, Security Framework Layer 5 -Security Technology, Layer 6 -Security Mechanism , Security Guidelines, Security Compliance, Security Incident	<ul style="list-style-type: none"> Software patches for operating systems and antivirus software's must be regularly updated. The network administrator must block all unused ports, must disable all unused protocols & services and must maintain a secure firewall around the network (Demme et al., 2013). The key-logger attack can be eliminated by using a virtual keyboard (Nyang, Mohaisen, Kwon, Kang,

Logging	management, Security Awareness	& Stavrou, 2011).
2. Distributed Denial of Service Attacks	<p>Layer 1- Security Principles, Security Baselines Layer 2- Gap Analysis, Security Requirements, Risk Analysis, Security Threat Model Layers 3-Infra Security, Network security components-IPS is handling it.</p> <ul style="list-style-type: none"> • Anti-virus and anti –spyware module • Firewall management • Vulnerability detection <p>Audit & monitoring network Layer 4-Security Policy module address the account lockout policies Layer 5 –Security Technology Layer 6 –Security Incident Management, Security Awareness, Security Mechanism, Security Standard, Guidelines and Best practices-ISO 27001 address the Server and TCP/IP Tunnel hardening</p>	<ul style="list-style-type: none"> • Use the SOP for configuration such as applications and etc. • Regularly update the software patches • Hardening the TCP/IP tunnel • Keep account lockout policies in place • Allow high volume traffic and threshold • Review and maintain failback • Use Intrusion Detection Systems to detect the potential threats (Back, 2002; Zargar et al., 2013).
3. Injection Flows (SQL, OS and LDAP)	<p>Layer 1-Security Principles, Security Strategy, Security Baselines, Security Concept. Layer 2- Gap Analysis, Security Requirements, Risk Analysis, Threat Modelling help to eliminate the SQL injection. Layer 3- Application Security Layer 4- Security Policy, Security Framework, Security Patterns, Security Metrics, Security Model Layer 5- Security Technology Layer 6-Security mechanism, Security Guidelines-OWASP address the implementation. Security Standard, Security Incident Management, Security Awareness</p>	<ul style="list-style-type: none"> • Regular updates on software and operating system patches (Fonseca, Vieira, & Madeira, 2009).
<p>4. Social Engineering a. Lottery Fraud b. Advance Fee Fraud c. Boiler Room</p>	<p>Layer 1- Security Baselines Layer 2-Gap Analysis, Security Requirement, Risk Analysis, Threat Model Layer 6 – Security Incident Management, Security Awareness- Security Standard,</p>	<ul style="list-style-type: none"> • To establish a trustworthy relationship with the employees • Proper identification of data in such a way that sensitive information is protected from social engineering attacks or security system

<p>Attack</p> <p>d. Pharming</p>	<p>Guidelines and Best Practices.</p>	<p>malfunctions</p> <ul style="list-style-type: none"> • To establish and maintain policies related to security, proper implementation of security protocols and processes • To provide employee engagement to security practices • To perform regular security audits and perform scheduled security inspections • To apply regulated waste paper management service in security firms (Kee, 2008).
<p>5. Network Eavesdropping</p>	<p>Layer 1-Security Baseline Layer 2-Gap analysis, Security requirement management, Threat Model Layer 3- Network security Layer 4- Access control Layer 5- Security Technologies Layer 6- Security Compliance, Security Incident Management and Security awareness</p>	<p>Message encryption techniques help in thwarting network eavesdropping. Security cipher protocols like AES 128 bit or RC4 stream cipher are commonly used in the industry to counter this problem (Mousa & Hamad, 2006).</p>
<p>6. Data Disruption Attacks</p>	<p>Layer 1-Security Baseline, Security Strategy, Security Roles, Security Concepts Layer 2-Gap Analysis, Security Requirement Management, Threat Model Layer 3- Network Security, Infra Security Layer 4- Security Policy, Security Framework, Access Control, Sec Layer 5- Secure Integration, Security Technologies, Security Protocol Layer 6- Security Mechanism, Security Guidelines, Security Standard, Security Awareness, Security Incident Management</p>	<ul style="list-style-type: none"> • To configure routers so that it restricts unwarranted network access. • To configure the operating systems on banking servers by disabling unauthorized access to ports and protocols and to put network mechanisms in place that can filter network traffic data by using encrypted session handshakes over the communication channel. • To apply regular security updates to servers (Meier et al., 2003).
<p>7. Identity Theft</p>	<p>Layer 1-Security Principle, Security Baseline, Security Concepts Layer 2-Gap analysis, Security</p>	<ul style="list-style-type: none"> • To enforce strong password guidelines and to ensure that strong passwords are a

	<p>requirement management, Threat Model, Risk Analysis</p> <p>Layer 3- Data Security, Application Security</p> <p>Layer 4- Security Policy, Access control, Security Framework, Security Metrics, Security Patterns, Reference Model, Security Model, Security Protocol</p> <p>Layer 5- Security Technologies</p> <p>Layer 6- Security Mechanism, Security Guidelines, Security Standards, Security Incident, Management, Security Awareness</p>	<p>combination of alphanumeric and symbolic characters.</p> <ul style="list-style-type: none"> • To place network mechanism in place that can lockout a user account post a certain number of unsuccessful login attempts • To enforce proper browser protocols like emptying the cache after use, ensuring passwords are not stored (Meier et al., 2003).
<p>8. Broken Authentication & Session Management and Cross-Site Scripting (XSS)</p>	<p>Layer 1- Security Principles, Security Baseline, Security Strategy, Security Roles, Security baselines, Security Concepts</p> <p>Layer 2- Gap analysis, Security requirement, Threat Model, Risk Assessment</p> <p>Layer 3- Data Security, Application Security, Network Security</p> <p>Layer 4- Security policy, Access Control, Security Framework, Security Patterns, Security Models</p> <p>Layer 5- Security Technologies, Secure Integration, Secure Protocol and Binding</p> <p>Layer 6- Security Mechanism, Security Guidelines, Standard & compliance, Security Incident management, Security Awareness</p>	<ul style="list-style-type: none"> • To enforce network protocol like SSL that augments a secure communication channel over the traditional HTTPS connection • To implement automatic time based user logout mechanism that forces authentication in the event there has not been any user activity for a certain period of time • In case SSL cannot be implemented then limit the session cookie expiration time which although does not curtail session hijacking but definitely reduces any hijacking attempts. • To enable user re-authentication by programming for users performing mission critical functions example fund transfers • To ensure that browser options like "save passwords" are disabled. (Meier et al., 2003).
<p>9. Security Misconfiguration</p>	<p>Layer 1- Security Principles, Security Roles, Security Baselines</p> <p>Layer 2- Risk Assessment, Gap Analysis, Security Requirements, Security Threat Model</p> <p>Layer 3- Application security, Network Security, Infra Security</p>	<ul style="list-style-type: none"> • Use standard protocol (SOP) for installation and configuration. • Use the ISO standard for configuration. • Regular updates on SOPs

	Layer4- Security Policy, Security Framework Layer 5- Security Technology Layer 6- Security Mechanism, Security Guidelines, Security Compliance, Security Incident management, Security Awareness	(Meier et al., 2003).
10. Phishing	Layer1- Security Strategy, Security Roles, Security Baselines Layer 2- Risk assessment, Gap Analysis, Security Requirement. Threat Model Layer 4 – Security policy Layer 6- Security Guidelines, Security Incident Management, Security Awareness	To eliminate the phishing attack while transacting or browsing on a banking or a financial website the user can verify the website authentication by checking the padlock icon in the URL bar can be clicked to verify the identity of the website (Bhati & Khan, 2012).

4.8 Summary

In this chapter, the proposed enterprise architecture security framework for banking industry in banking environment has been designed and explained in detail. In the first step, actors and relationships between actors in the enterprise architecture security framework for banking were introduced. The proposed enterprise security architecture framework (ESAF) for banking software development defines six major layers, which include enterprise architecture security fundamentals, enterprise architecture security requirements, enterprise security core, enterprise security assets, security integration and security governance. Then components in the proposed ESAF for banking environment were described. The components were classified into each layer of the framework. Subsequently, design and architecture of the proposed ESAF for banking environment were explained in detail.

CHAPTER 5: IMPLEMENTATION OF ESAF IN BANKING ENVIRONMENTS

5.1 Introduction

The earlier chapters have defined and presented a comprehensive design of this framework. The prevalent technologies to achieving this security mandate in the banking environments were introduced too. This chapter explains the implementation of the framework with software development life cycle (SDLC) phases. Besides, this framework implementation was based on appropriate technologies that address the security needs.

5.2 ESAF Components and Artefacts

Table 5.1 illustrates all the components and artefacts of the ESAF mapping with SDLC stages. Each layer of the ESAF must deliver its corresponding artefacts to accomplish its tasks. Templates of the artefacts are presented in **Appendix K**.

Table 5.1: Mapping of SDLC Stages with Artefacts

Initiation	Development and Acquisition	Deployment and Assessment	Operation/ Maintenance
Security requirement list	Risk & threat assessment	Verified list of operational security controls	Evaluation of security implication list (Due to changes)
Risk management strategy /plan (risk register)	System security plan	Security assessment report	Security Evaluation
List of actors and responsibilities	List of security concept template	Security authorisation list	Documented results of continues monitoring(Security incident report)
List of security baseline security process	List of applicable security standards & compliance	Initial work plan assessment	—
Security architecture risk assessment	Risk management strategy	—	—
List of target	Impact Analysis	—	—





security process			
List of applicable security policies	Penetration test results	—	—
Security Matrix and monitoring plan	Code review results	—	—
Asset list with custodian	Report test result and implication	—	—
List of security assumption and boundaries	List of applicable security models	—	—
List of access control metrics	List of Target security models	—	—
List of applicable Law and Regulations	List of architecture development check point	—	—

5.3 ESAF Incorporated with SDLC

The SDLC phases were identified based on the NIST model. This section elaborates a number of considerations that assist integrating security into the SDLC. All the security aspects are being identified in each of the SDLC phases, hence advancing the business process, business scenarios, and security requirements together to ensure a well-balanced methodology during development. Figures 5.1 to 5.4 present activities in each phase of SDLC and the corresponding ESAF artefacts in each phase.

Each phase identifies and elaborates the security activities. Moreover, each activity further details out the expected outcomes and interdependencies. Each phase describes the step-by-step guideline to achieve the task deliverables and artefacts which along with the recommendations for integration of these work products into the SDLC.

Table 5.2:SDLC Phases Notations

Notation	Description
	Start/End
	Activity
	Iteration
	Artefact

5.3.1 SDLC Phase 1-Initiation

In the initiation, institution has to identify the needs of a particular system and its goals and objectives. Security planning initiates this stage and identifies the key stakeholders involved in building the system. Their roles and responsibilities are defined and documented. Brainstorming and walkthrough sessions need to be carried out to identify the information process, how it is transmitted and stored.

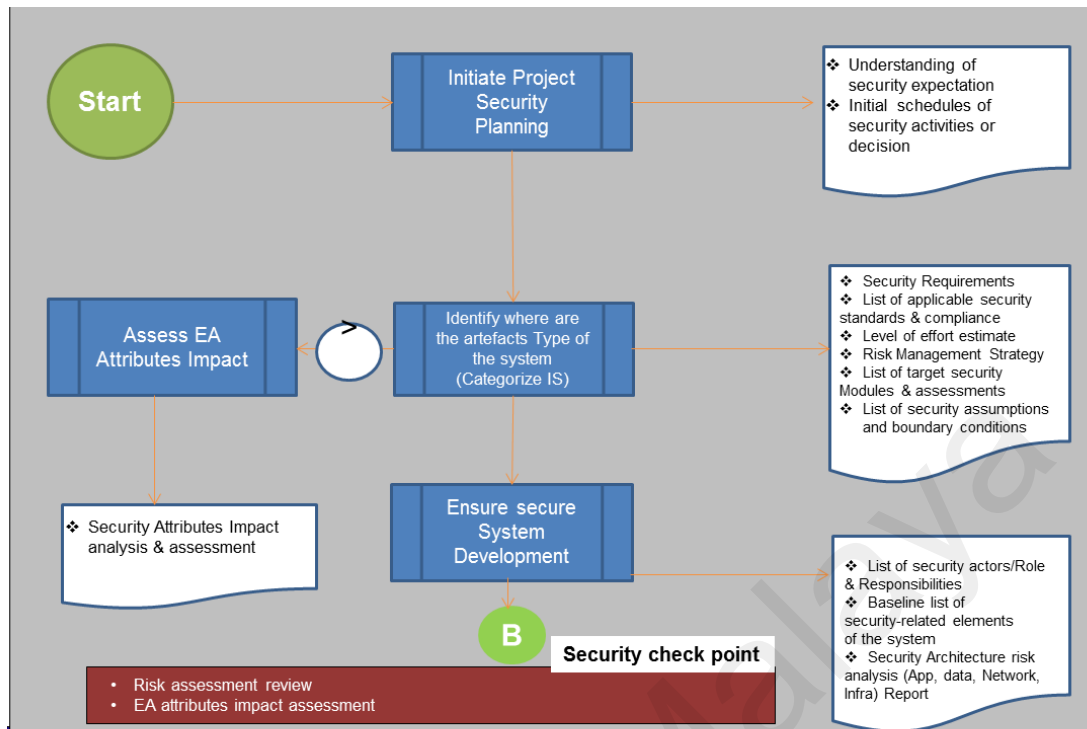


Figure 5.1: SDLC Phase 1 –Initiation

Security considerations play a pivotal role in the early integration of security, and assure that threat, requirements, and potential constraints are taken care in functionality and integration. Requirements such as confidentiality, integrity, and availability of information must be verified at this stage. These requirements will be assessed by a moderator to classify them. Early planning plays a vital role. It saves significant amount of cost and man-days through proper risk management planning. In this stage, the organisation defines their goals and high-level security requirement along with the security- oriented architecture.

5.3.2 SDLC Phase 2- Development and Acquisition

Throughout this phase of development life cycle, six major tasks have to be achieved, that include assessment of risks, select and document the security controls, design security architecture, engineer the security control, conduct testing, and

documentation. Security considerations outline keys to protect the secure development and discipline among the development process. The main task to be carried out in this phase is risk assessment. Results of the risk assessment help to lay the baseline security. Organisation has to evaluate the security requirements and also has to carry out functional security testing. Furthermore, the team has to prepare the documentation for system certification and sign off, deliver security architecture and design documents.

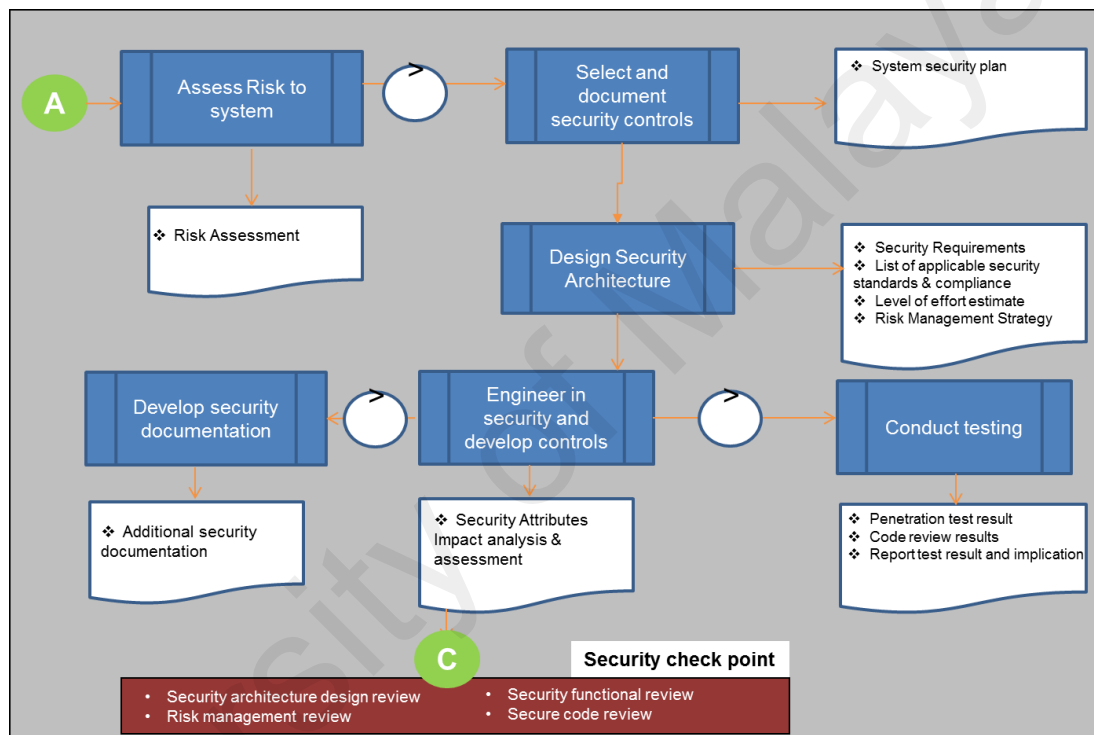


Figure 5.2: SDLC Phase 2- Development & Acquisition

The security plans are delivered in this stage. The plans included security requirements of the banking systems. Detailed descriptions of the security control are stated in the document. Authorised personnel of the process department or custodian of the modules have to select the security controls applicable to them. They have to go through the review process and give the approval, and document the decisions in the security plan. It is necessary to test security features and each function to ensure that they are achieved

as planned. Moreover, this phase elaborates the security checkpoints, which include security architecture design review, risk management review, and code review.

5.3.3 SDLC Phase 3: Deployment Assessment

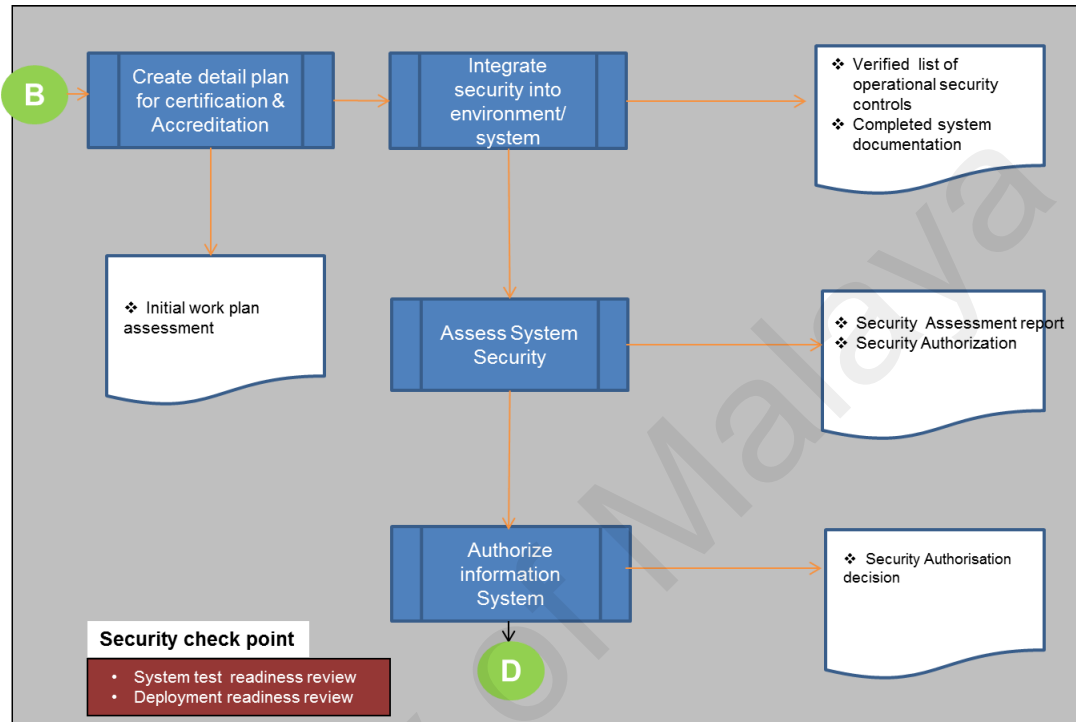


Figure 5.3: SDLC Phase 3: Deployment Assessment

In this phase, the deployment and implementation technical team has to configure the secure environment and carry out the necessary security assessment and authorise the information system. The team has to implement all the applicable security controls and authorise access. Before this exercise, the team must ensure that they have carried out design reviews and necessary testing. According to the system readiness determined through the review results, authorities make a decision to go live. All the test results must be documented.

5.3.4 SDLC Phase 4: Operation /Maintenance

In this stage, systems are in production, but users are demanding for enhancement and modification. The maintenance and support team has to go through the development

cycle again to fulfil the requirements. Meanwhile, hardware and software are upgraded or replaced or new components are added. Therefore, the security team has to continuously monitor their activities and ensure that they constantly practice and apply the security requirements and controls.

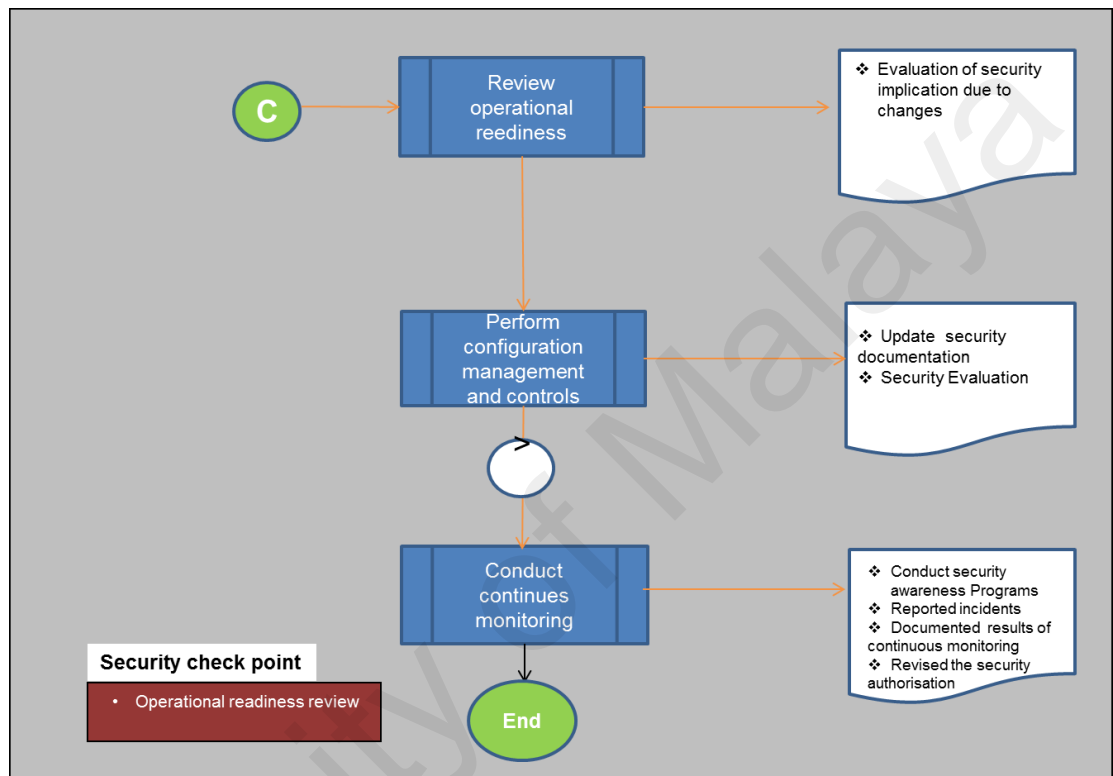


Figure 5.4: SDLC Phase 4: Operation /Maintenance

Configuration management and version control activities also take place in this phase to document any proposed or actual changes in the security plan of the system. As information systems including surrounding environment are regularly updated or upgraded, it is necessary to document all the amendments of the security measurement to track down and monitor the outcome.

5.4 Setting up the ESAF Development Environment

Some services provided by the ESAF need to be programmed, e.g. access control, data encryption and decryption. The Yii framework was chosen as the development framework.

Yii adopts the model-view-controller (MVC) design pattern which is widely used for the web application development. The MVC model helps for rapid changes for business requirements and also developers to change the programs easily without interrupting other components.

Figure 5.5 illustrates the structure of the Yii framework.

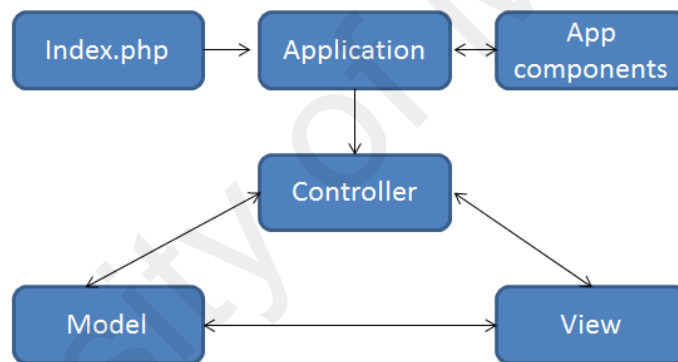


Figure 5.5: Yii MVC Framework

It was essential to select tools which direct and personal support was available during the development of the ESAF for online banking systems. In this implementation, Yii framework has played a critical role in the development of ESAF from its expanded components and third party extensions. The Yii framework supports the complete web services development process, particularly useful for third party integration. Bootstrap is a front-end framework for web development, which included HTML, CSS and JavaScript plugins.

It can also support easy creation of responsive CSS adjustable to phones, tablets, and desktops and compatible with all modern browsers (Chrome, Firefox, Microsoft Edge, Safari, and Opera). Thus, Yii was selected as the development environment, and support was graciously provided by Arun Surendran from Pivot Systems in India.

5.4.1 Setting up the Development Tools

The following sequence of steps were taken to setting up the development tool.

In order to build the ESAF, it is important to set up the environment with the mandatory components. In order to run the Yii framework, environment must require the apache web server and MySQL database. Therefore, the XAMPP environment provide the Apache and MySQL Database.

The first step was setting up the XAMPP environment and Yii (Figures 5.6 and 5.7) as well as configuring configure it (Figure 5.8).

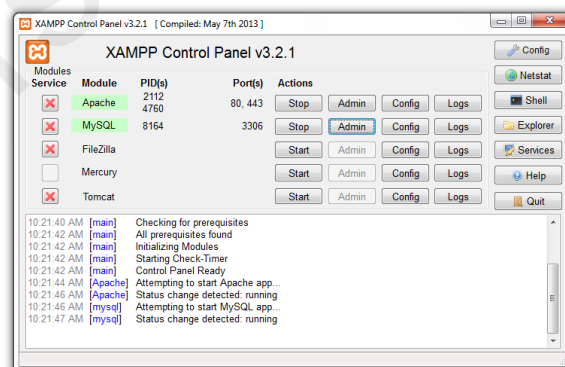


Figure 5.6: Set up XAMPP Environment

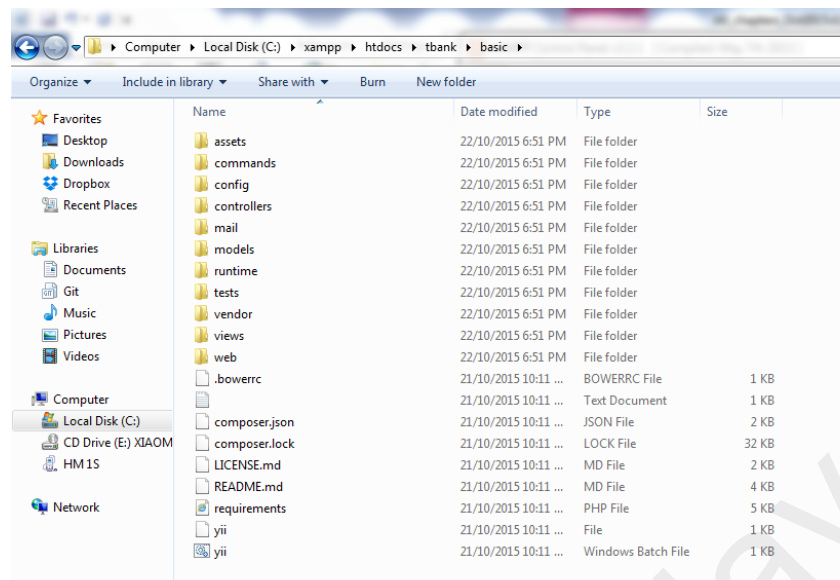


Figure 5.7: Yii Environment Set up

```
if (YII_ENV_DEV) {
    // configuration adjustments for 'dev' environment
    $config['bootstrap'][] = 'debug';
    $config['modules']['debug'] = [ 'class' => 'yii\debug\Module', ];
    $config['bootstrap'][] = 'gii';
    $config['modules']['gii'] = [
        'class' => 'yii\gii\Module',
        'allowedIPs' => ['*', ':::1'], ];
}
return $config;
```

Figure 5.8: Yii Config/Web

5.4.2 Configuring Security Modules and Components

Each module and component defined its own security setting. These setting determine who have the privilege to use the components.

5.4.2.1 Configuring Identity Access Controls

The user application component is designed to perform a group of coordinated functions, tasks, or activities for benefits of the user. It is able to accomplish the user

credential verification status. It encompasses a specific class that comprises the definite verification logic as shown in Figure 5.9.

```
return [
    'components' => [
        'user' => [ 'identityClass' => 'app\models\User', ],
    ],
];
```

Figure 5.9: Sample Code of the User Model

The identified specific class encompasses with a list of methods which are elaborated in Table 5.3.

Table 5.3: Identity Interface Methods

Method	Description
findIdentity()	It searches the identity class and finds the Users ID.
findIdentityByAccessToken()	Authenticated user recognised by access token.
getAuthKey()	It verifies client side login cookies and server side cookies.
validateAuthKey():	Key function of this method is to validate the cookies based key.

5.4.2.2 Access Control Filter (ACF)

Access Control Filter (ACF) is a simple authorization method implemented as `yii\filter\AccessControl` which is best used by applications that only need some simple access control. As its name indicates, ACF is an action filter that can be used in a controller or a module. While a user is requesting to execute an action, ACF check a list of access rules to determine if the user is allowed to access the requested action.

The access control filter (ACF) is an approval method executed in applications. Generally, ACF validates rules in order to permit the requested access as shown in Figure 5.10.

```
[ 'class' => AccessControl::className(), ...
  'denyCallback' => function ($rule, $action) {
    throw new \Exception('You are not allowed to access this page'); } ]
```

Figure 5.10: Snippet of Code of Access Control

ACF performs the authorization check by examining the access rules one by one from top to bottom until it finds a rule that matches the current execution context. The allow value of the matching rule will then be used to judge if the user is authorized or not. If none of the rules matches, it means the user is NOT authorized, and ACF will stop further action execution.

When ACF determines a user is not authorized to access the current action, it takes the following measure by default:

- If the user is a guest, it will call `yii\web\User::loginRequired()` to redirect the user browser to the login page.
- If the user is already authenticated, it will throw a `yii\web\ForbiddenHttpException`

5.4.2.3 Access Rules

The methods are used to specify the access rules. The implemented system uses the access control rules methods as shown in Table 5.4.

Table 5.4: Access Rules

Methods	Description
Allow	It classifies the rules that "allow" or "deny"
Actions	It retrieves rules that are matched with a specific action.
Controllers	It identifies rules that map in the controller.
Roles	User roles mapped with the rule.
IPs	Rules to match the client IP addresses.

5.4.3 Access Control List (ACL)

It introduces privileges of the users which modules they are allowed to access and further it is incorporated to use business-rules. The snippets of code is shown in Figure 5.11.

```
use yii\data\ActiveDataProvider;
use yii\web\Controller;
use yii\web\NotFoundHttpException;
use yii\filters\VerbFilter;
use yii\filters\AccessControl;
/** * UsersController implements the CRUD actions for Users model. */
class UsersController extends Controller
{
    public function behaviors() {
        return [
            'verbs' => [
                'class' => VerbFilter::className(),
                'actions' => [
                    'delete' => ['post'],
                    'create' => ['post'],
                    'index' => ['get'],
                    'view' => ['get'],
                    'update' => ['post'],
                ],
            ],
            'access' => [
                'class' => AccessControl::className(),
                'rules' => [
                    [
                        'actions' => [
                            'create', 'update',
                        ],
                        'allow' => true,
                    ],
                    [
                        'matchCallback' => function ($rule, $action) {
                            $previlege = strtolower(Yii::$app->user->identity->role);
                            return $previlege === 'admin';
                        },
                        'actions' => [
                            'index', 'view',
                        ],
                        'allow' => true,
                    ],
                    [
                        'matchCallback' => function ($rule, $action) {
                            $previlege = strtolower(Yii::$app->user->identity->role);
                            return $previlege === 'admin' || $previlege === 'staff';
                        },
                        'actions' => [
                            'create', 'update',
                        ],
                        'allow' => true,
                    ],
                ],
            ],
        ];
    }
}
```

Figure 5.11: Access Control Filters

5.4.4 Hashing and Verifying Passwords

Resilience of passwords against brute force attacks is achieved through hashing which can be accomplished by using the PHP crypt function as shown in Figure 5.12 and Figure 5.13.

```
if (Yii::$app->getSecurity()->validatePassword($password, $hash)) {
    // all good, logging user in
} else {
    // wrong password
}
```

Figure 5.12: Snippet of Code of Hashing


```

public function beforeSave($insert) {
    if( isset($this->password))
        $this->password = Yii::$app->getSecurity()->generatePasswordHash($this->password);
    return parent::beforeSave($insert);
}

```

Figure 5.13: Snippet of Code of Hashing Validating

5.4.5 Safeguarding XSS

The XSS can be avoided by using plain text and HTML purifier function. Figure 5.14 shows the snippet of code of plain text escaping and HtmlPurifier.

```

<?= \yii\helpers\Html::encode($username) ?>

<?= \yii\helpers\ HtmlPurifier::process($description) ?>

```

Figure 5.14: Plain Text Escaping and HtmlPurifier

5.4.6 Generating Pseudorandom Data

The pseudorandom data is highly use in many circumstances. For instance, when changing a password via email, it creates a token and sends it via email to the account owner for them to verify ownership of that account. It is imperative that this token is unique and hard to predict, or otherwise there is a high probability that attacker guesses the token's value and changes the accounts owner's PIN. The snippet of code is shown in Figure 5.15.

```
$key = Yii::$app->getSecurity()->generateRandomString();
```

Figure 5.15: Snippet of Code of Pseudorandom Code Generation

The OpenSSL extension was configured to create secure random data.

5.4.7 Data Encryption and Decryption

To make use of the helper function to create the secret key as shown in Figure 5.16.

```
// $data and $secretKey are obtained from the form
$encryptedData = Yii::$app->getSecurity()->encryptByPassword($data, $secretKey);
// store $encryptedData to database
Subsequently when user wants to read the data:
// $secretKey is obtained from user input, $encryptedData is from the database
$data = Yii::$app->getSecurity()->decryptByPassword($encryptedData, $secretKey);
```

Figure 5.16: Code Snippet of Secret Key Generation

Figure 5.17 displays the screenshot of user table in the database. It shows passwords are encrypted by hash key.

Logout (admin)

Home / Users

Users

Create Users

Showing 1-4 of 4 items.













#	Username	Password	First Name	Roles	
1	admin	\$2y\$13\$mDDLd6KqN7dX97apvGEv.xZ34pBVdh0D3kIPUpqVchTG274FMXI2	First	Admin	  
2	arun	\$2y\$13\$LfIKVeAcHrDBwdDaMUyhe5O4ekMctHu4FN846TM/0jK1FZSYyPa	First	staff	  
3	ruwan	\$2y\$13\$VEwUQ/omncbUDCAKc0QI7uHr/LkylhsZLDWN0CJPONG2PqszQanJO	First	banker	  
4	Nicholas	\$2y\$13\$CtOIIndgu2/3WD7EHTRHr8utlqy6eQRTVsJxWllyq54Kx9Dqbg7aP2	First	staff	  

Figure 5.17: Users Database Table

5.4.8 Data Integrity

Data integrity can be confirmed by using a helper function. The snippet of code is shown in Figure 5.18.

```
// $secretKey our application or user secret, $genuineData obtained from a reliable source
$data = Yii::$app->getSecurity()->hashData($genuineData, $secretKey);
Checks if the data integrity has been compromised
// $secretKey our application or user secret, $data obtained from an unreliable source
$data = Yii::$app->getSecurity()->validateData($data, $secretKey);
namespace app\controllers;
use yii\web\Controller;
class SiteController extends Controller
{
    public $enableCsrfValidation = false;
    public function actionIndex()
    }
}
```

Figure 5.18: Helper Function to Generate Secret Key

5.4.9 Cookies Validation, Cache, and Error Handling

This is to safeguard the cookies alteration and tempering on client side. By using hash key string, this vulnerability can be protected. The snippet of code is shown in Figure 5.19.

```
$config = [
    'id' => 'basic', 'basePath' => dirname(__DIR__),
    'bootstrap' => ['log'], 'components' => [
        'request' => [ // insert a secret key in cookie validation
            'cookieValidationKey' => 'nick76t58bv232vb', ],
        'cache' => [ 'class' => 'yii\caching\FileCache', ],
        'user' => [ 'identityClass' => 'app\models\User', 'enableAutoLogin' => true, ],
        'errorHandler' => [ 'errorAction' => 'site/error', ],
        'mailer' => [ 'class' => 'yii\swiftmailer\Mailer',
            'useFileTransport' => true, ],
        'log' => [
            'traceLevel' => YII_DEBUG ? 3 : 0, 'targets' => [
                [ 'class' => 'yii\log\FileTarget',
                    'levels' => ['error', 'warning'], ], ], ],
        'db' => require(__DIR__ . '/db.php'), ],
    'params' => $params,
];
```

Figure 5.19: Cookies Validation, Cache, and Error Handling

5.5 Summary

In this chapter, the researcher has discussed the ESAF components and artifacts to accomplish its tasks. This chapter has also elaborated a number of considerations that assist integrating security into the SDLC. All the security aspects were identified in each of the SDLC phases, hence advancing the business process, business scenarios, and security requirements together to ensure a well-balanced methodology during development. The researcher also explained the setting up of the ESAF development environment, which includes setting up development tools and configuring the security modules. In the next chapter, the researcher will present the results of evaluation.

CHAPTER 6: RESULTS EVALUATION AND DISCUSSION

6.1 Introduction

This chapter describes the security evaluations that were conducted and their analytical results on the framework for banking environments. The evaluation results were analysed to ascertain if the framework is in tandem with the requirements established in Chapter 3. This chapter also describes the validation measures used for the framework evaluation.

6.2 ESAF Evaluation Criteria

In order to evaluate the comprehensiveness, effectiveness and ease of use of the proposed ESAF in a banking environment, extensive interviews have been performed with 24 industry experts to assess the proposed ESAF (Interviewees' responses can be found in **Appendix L**). The experts also assessed the ESAF based on some selected scenarios.

6.3 Interviewees' Demographics

Table 6.1: Distribution of Interviewees based on Roles

Roles of Interviewee	Invited	Responded	Percentage (%)
CIO/CTO/CA	8	3	12.5%
VP/SVP	7	3	12.5%
ESA/SA/Application Architect/TA	9	3	12.5%
SME	6	3	12.5%
PM/PMO	6	3	12.5%
Technical Lead	7	3	12.5%
BA	7	3	12.5%
Senior Engineers	8	3	12.5%
	58	24	100%

Table 6.1 shows the distribution of interviewees based on their roles. Out of 58 invitations sent to the interviewees, the researcher received 24 acceptance notices.

6.3.1 Work Experience

Table 6.2: Work Experience of the Interviewees

	Responded	Working Experience			
		5-10Y	10-15y	15-20Y	20+Y
CIO/CTO/CA	3			2	1
VP/SVP	3			2	1
ESA/ SA/Application Architect/TA	3			2	1
SME	3			3	
PM/PMO	3		1	2	
Technical lead	3		1	2	
BA	3		3		
Senior Engineers	3	1	2		
	24	1	7	13	3

As shown in Table 6.2, a healthy group of interviewees have 15-20 years of work experience which was followed by 10-15 years of work experience.

6.3.2 Geographical Location

Table 6.3: Interviewees' Geographic Locations

	Responded	Australia	Czech Republic	India	Malaysia	Poland	Singapore	Sri Lanka	Thailand
CIO/CTO/CA	3		1	1			1		
VP/SVP	3				2		1		
ESA/ SA/Application	3	1			2				
SME	3				3				
PM/PMO	3				1	1			1
Technical lead	3			1	1			1	
BA	3	1			1		1		
Senior Engineers	3			1	2				
	24	2	1	3	12	1	3	1	1

Table 6.3 shows that the interviewees are from eight different countries: Australia, Czech Republic, India, Malaysia, Poland, Singapore, Sri Lanka and Thailand. Nonetheless, the majority of the interviewees were from Malaysia (12).

6.3.3 Interview Methods

Table 6.4: Interview Methods Used

		Interview Method				
	Responded	Face to Face	Skype	WebEX	WhatAPP	Phone Call
CIO/CTO/CA	3		2			1
VP/SVP	3	2	1			
ESA/ SA/Application Architect/TA	3	2	1			
SME	3	3				
PM/PMO	3	1	2			
Technical lead	3	1	1	1		
BA	3	1	1		1	
Senior Engineers	3	2	1			
	24	12	9	1	1	1

Table 6.4 illustrates the interview methods used for the interview sessions. Majority of the interviews were conducted face to face and nine of the interviews were performed using Skype. These methods were proposed by interviewees according to their convenience, familiarity and privacy considerations.

The steps below elaborate on the interview process:

- Send the conceptual model and the corresponding documents to the interviewees for them to review in 3-4 days. The evaluation questionnaire was sent together to the interviewees.
- The researcher contacted the interviewees to clarify their doubts about the model and the questionnaire.
- The interviewees took another 3-4 days to answer the questionnaire and returned the questionnaire to the researcher.
- The templates of artefacts were sent to the interviewees for comments and suggestions for improvement.

The evaluation questionnaire is included in **Appendix M**.

6.4 Assessment One

The first assessment was based on three criteria, which include comprehensiveness, effectiveness, and ease of use.

The researcher used a scoring system to convert the interviewees' responses into scores. Then the researcher ranked the responses based on the scores. The scoring system is similar to the one used for prioritising ES practices and ESA attributes as described in Section 4.2.2.

6.4.1 Comprehensiveness of ESAF

The ESAF criteria of comprehensiveness are intended to evaluate whether an implementation of the proposed ESAF will achieve its security coverage.

Table 6.5 to Table 6.12 depict assessment scoring on comprehensiveness of ESAF by the eight categories of interviewees.

Table 6.5: Interviewees' (CIO/CTO/CA) Response of Comprehensiveness of ESAF

CIO/CTO/CA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 2	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 3	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H

Table 6.6: Interviewees' (VP/SVP) Response of Comprehensiveness of ESAF

VP/SVP														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 2	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 3	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H

Table 6.7: Interviewees' (ESA/SA/TA) Response of Comprehensiveness of ESAF

ESA/SA/TA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M
Layer 2	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 3	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 5	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 6	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M

Table 6.8: Interviewees' (SME) Response of Comprehensiveness of ESAF

SME														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H
Layer 2	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H
Layer 3	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H

Table 6.9: Interviewees' (PM/PMO) Response of Comprehensiveness of ESAF

PM/PMO															
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK	
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H	
Layer 3	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	
Layer 5	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	
Layer 6	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	

Table 6.10: Interviewees' (Technical Lead) Response of Comprehensiveness of ESAF

Technical Lead														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 3	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 5	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 6	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H

Table 6.11: Interviewees' (BA) Response of Comprehensiveness of ESAF

BA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 3	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 6	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H

Table 6.12: Interviewees' (SE) Response of Comprehensiveness of ESAF

Software Engineers														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 3	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 6	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H

6.4.1.1 Overall Comprehensiveness of ESAF

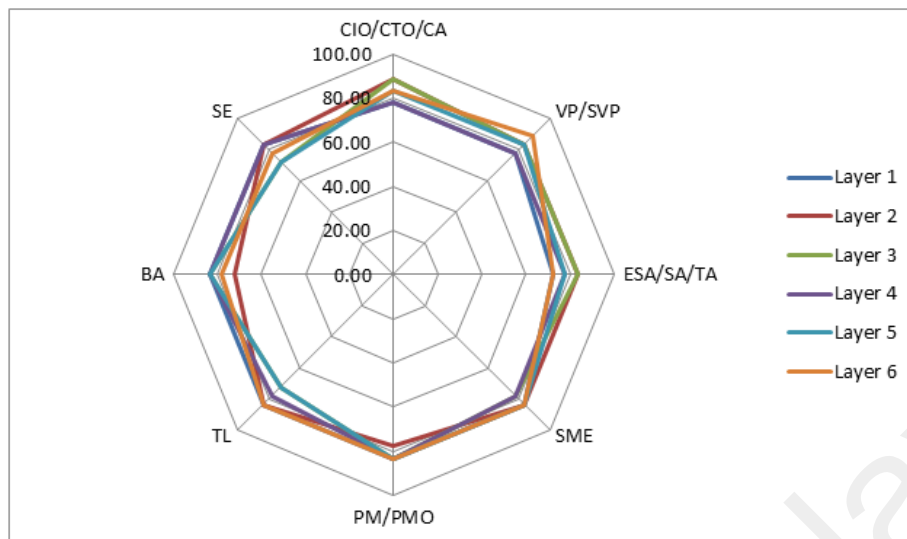


Figure 6.1: Overall Comprehensiveness of ESAF

Figure 6.1 summaries responses from the eight categories of interviewees in relation to comprehensiveness of the ESAF. It shows that the interviewees were satisfied with comprehensiveness of ESAF, with scores ranging between 72% to 88% among all the six layers of the ESAF. Table 6.13 shows the comments given by the interviewees about comprehensiveness of the ESAF.

Table 6.13: Interviewees' Comments on Comprehensiveness of ESAF

Layers	Coverage of ESAF	Drawback/ Improvement
Layer 1	<ul style="list-style-type: none"> Overall, the ESAF has addressed the security elements. According to the interviewees, this layer is important for them to create the baselines of the project. 	None
Layer 2	<ul style="list-style-type: none"> ES requirements fit into the banking industry, and it can be used locally and regionally. It helps bankers to ensure compliance with federal and banking regulatory body. 	None

	<ul style="list-style-type: none"> BA point of view, it is very important for them to identify the requirements at the early stages of the banking project. 	
Layer 3	<ul style="list-style-type: none"> Covered all the necessary elements required for application security, data security and security integration. 	<ul style="list-style-type: none"> Technical Architect suggested to install application firewall with virtual-patch integration capability.
Layer 4	None	<ul style="list-style-type: none"> As per comment by interviewees, to make use of Multi-Factor Authentication including Fingerprint based authentication as the first step so that security can be improved.
Layer 5	<ul style="list-style-type: none"> ESAF helps to protect banking operations against internal and external threats. It also enhances the protection of banking employees and other parties such as banking customers and vendors. 	<ul style="list-style-type: none"> One of the interviewees suggested that ESAF should integrate with remote security monitoring system. It helps to enhance the banking operations.
Layer 6	None	<ul style="list-style-type: none"> One of the SME suggested that there is a need to add sections on security assessment, security maturity matrix of EAF/ESA.

6.4.2 Effectiveness of ESAF

The ESAF evaluation criterion of effectiveness evaluates whether the ESAF has achieved its intended goals. To perform a meaningful assessment of the predicted and actual results, the ESAF evaluation goals have to be conveyed in a method of quantifiable levels of assessment. Meanwhile, the researcher also captured the unpremeditated optimistic or undesirable feedbacks given by the interviewees. Tables 6.14 to 6.21 show the scores given by the eight categories of interviewees in relation to effectiveness of the ESAF.

Table 6.14: Interviewees' Response (CIO/CTO/CA) of Effectiveness of ESAF

CIO/CTO/CA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.33	1.98	0.67	3.35	0	0.00	0	0	0	0	0	0	88.83	H
Layer 2	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 3	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 4	0.33	1.98	0.67	3.35	0	0.00	0	0	0	0	0	0	88.83	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H

Table 6.15: Interviewees' Response (VP/SVP) of Effectiveness of ESAF

VP/SVP														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00		0.00	0	0	0	0	0	0	83.33	H
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 3	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 4	0	0.00	1	5.00	0.33	0.00	0	0	0	0	0	0	83.33	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H

Table 6.16: Interviewees' Response (ESA/SA/TA) of Effectiveness of ESAF

ESA/SA/TA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 2	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M
Layer 3	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 4	0	0.00	1	5.00	0		0	0	0	0	0	0	83.33	H
Layer 5	0	0.00	1	5.00	0		0	0	0	0	0	0	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0.00	0	0	0	0	0	0	88.83	H

Table 6.17: Interviewees' Response (SMEs) of Effectiveness of ESAF

SME														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 3	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 5	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M
Layer 6	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M

Table 6.18: Interviewees' Response (PM/PMO) of Effectiveness of ESAF

PM/PMO														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 3	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 5	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 6	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H

Table 6.19: Interviewees' Response (Technical Lead) of Effectiveness of ESAF

Technical Lead														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 3	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 6	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H

Table 6.20: Interviewees' Response (BA) of Effectiveness of ESAF

BA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H
Layer 2	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 3	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H

Table 6.21: Interviewees' Response (SE) of Effectiveness of ESAF

Software Engineers														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H
Layer 2	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 3	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 6	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H

6.4.2.1 Overall Effectiveness of EASF

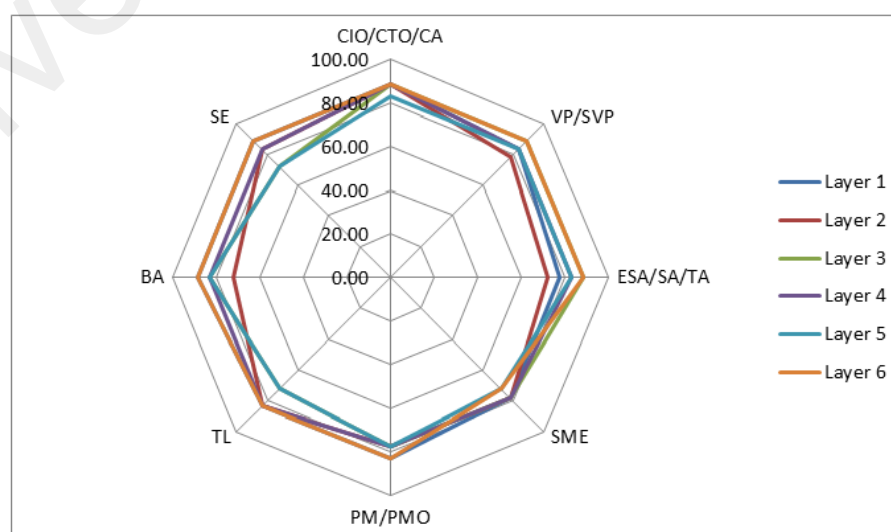


Figure 6.2: Overall Effectiveness of ESAF

Figure 6.2 summaries responses from the eight categories of interviewees in relation to effectiveness of the ESAF. It shows that the interviewees were satisfied with effectiveness of ESAF, with scores ranging between 72% to 89% among all the six layers of the ESAF. Table 6.22 shows the comments given by the interviewees about effectiveness of the ESAF.

Table 6.22: Interviewees' Comments on Effectiveness of ESAF

Layers	Coverage of ESAF	Drawback/ Improvement
Layer 1	<ul style="list-style-type: none">The chief architect and enterprise architects claimed that it is highly effective.	<ul style="list-style-type: none">According to CIO and CTO, there are security principles, baselines, and security concepts and security attributes introduced by the researcher but industry users hardly apply and fulfil those requirements.Many bankers are still yet to embrace the security fundamentals into their environment.Furthermore, they highlighted that lack of security roles is the major alarming factor for bankers.
Layer 2	<ul style="list-style-type: none">General comments from interviewees show that the ESAF is effective.	
Layer 3	<ul style="list-style-type: none">According to the interviewees, it is effective.	<ul style="list-style-type: none">When considering thick client security, it will be advisable to implement OS level security along with the secure access to communicate with the server.Application code also needs to cover all possible HTTP routes that are available in the banking software, Code review can help to achieve this to a greater extent but introducing appropriate frameworks as part of the application architecture can be a much better solution.

		<ul style="list-style-type: none"> • The most challenging part when comes to data security will be the ways to secure the links between the physical and logical data. • Proper rollback schemes have to be implemented in case of the linkage breaks due to logistics or network issues. This mechanism will also help to reduce the data clean up and redundant backlogs.
Layer 4	<ul style="list-style-type: none"> • By using security assets, it is an effective way to cost saving the development. • Furthermore, proven frameworks and models help to eliminate the design flaws. 	None
Layer 5	<ul style="list-style-type: none"> • General comments from interviewees, it is highly effective. 	<ul style="list-style-type: none"> • SME highlighted that it is necessary to continuously improve of the technology stack.
Layer 6	<ul style="list-style-type: none"> • All the best practices, appropriate standards and compliance are the effective way to standardise the security process and software development. 	<ul style="list-style-type: none"> • SME and CIO highlighted that the versions of the standards and regulations must be periodically audit and continuously updated. • VP suggested all the compliance and best practices should be informed to the staff members when they first join the institution.

6.4.3 Ease of Use of ESAF

The ESAF evaluation criterion of ease of use is used to assess whether the ESAF accomplishes significant functions from the implementation perspective. Its security-oriented design was primarily matched to accomplishing the goals aligned with the ESAF outcomes. The evaluation was conducted to determine whether the proposed ESAF aptly emphasises an important development goal of security, considering the

strategic requirements of the bankers, and is coordinated with other professionals.

Tables 6.23 to 6.30 show the scores given by the eight categories of interviewees in relation to ease of use of the ESAF.

Table 6.23: Interviewees' Response (CIO/CTO/CA) of Ease of Use of ESAF

CIO/CTO/CA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.33	1.98	0.67	3.35	0	0.00	0	0	0	0	0	0	88.83	H
Layer 2	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 3	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 4	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H

Table 6.24: Interviewees' Response (VP/SVP) of Ease of Use of ESAF

VP/SVP														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.33	1.98	0.67	3.35		0.00	0	0	0	0	0	0	88.83	H
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 3	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 4	0	0.00	1	5.00	0.33	0.00	0	0	0	0	0	0	83.33	H
Layer 5	0	0.00	1	5.00	0	0	0	0	0	0	0	0	83.33	H
Layer 6	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H

Table 6.25: Interviewees' Response (ESA/SA/TA) of Ease of Use of ESAF

ESA/SA/TA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H
Layer 2	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M
Layer 3	0.33	1.98	0.67	3.35	0	0	0	0	0	0	0	0	88.83	H
Layer 4	0	0.00	1	5.00	0		0	0	0	0	0	0	83.33	H
Layer 5	0	0.00	1	5.00	0		0	0	0	0	0	0	83.33	H
Layer 6	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H

Table 6.26: Interviewees' Response (SMEs) of Ease of Use of ESAF

SME														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 3	0	0.00	1	5.00	0	0.00	0	0	0	0	0	0	83.33	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0	0	0	0	0	77.83	H
Layer 5	0	0.00	0.33	1.65	0.67	2.68	0	0	0	0	0	0	72.17	M
Layer 6	0.33	1.98	0.67	3.35	0	0.00	0	0	0	0	0	0	88.83	H

Table 6.27: Interviewees' Response (PM/PMO) of Ease of Use of ESAF

PM/PMO															
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK	
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	
Layer 2	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M	
Layer 3	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H	
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H	
Layer 5	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H	
Layer 6	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H	

Table 6.28: Interviewees' Response (Technical Lead) of Ease of Use of ESAF

Technical Lead														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 3	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 6	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H

Table 6.29: Interviewees' Response (BA) of Ease of Use of ESAF

BA														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	0.33	1.65	0.67	2.68	0	0.00	0	0.00	0	0.00	72.17	M
Layer 3	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 4	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 5	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 6	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H

Table 6.30: Interviewees' Response (SE) of Ease of Use of ESAF

Software Engineers														
ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 2	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 3	0.33	1.98	0.67	3.35	0	0.00	0	0.00	0	0.00	0	0.00	88.83	H
Layer 4	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H
Layer 5	0	0.00	0.67	3.35	0.33	1.32	0	0.00	0	0.00	0	0.00	77.83	H
Layer 6	0	0.00	1	5.00	0	0.00	0	0.00	0	0.00	0	0.00	83.33	H

Table 6.31 shows the comments given by the interviewees about ease of use of the ESAF.

Table 6.31: Interviewees' Comments on Ease of Use of ESAF

Layers	Coverage of ESAF	Drawback/ Improvement
Layer 1	Easy to focus on given principles with full-fledge coverage of security and concise (Technical lead).	None

Layer 2	BAs and PMO highlighted that this layer helps them to easily focus and prioritise the security requirements.	One of the BAs suggested to add more templates on analysis.
Layer 3	Architects, technical leads and SEs highlighted that it is easy for them to implement.	None
Layer 4	Enterprise architects highlighted that it is easy to use all the security assets listed down in the template.	None
Layer 5	As claimed by interviewees, it is a good example for easy reference to Security Technology Stack.	None
Layer 6	SME's, BAs and technical leads highlighted that it is easy for them to use the security governance because banking regulations, standards and compliance are consolidated into one.	None

6.4.3.1 Overall Ease of Use of EASF

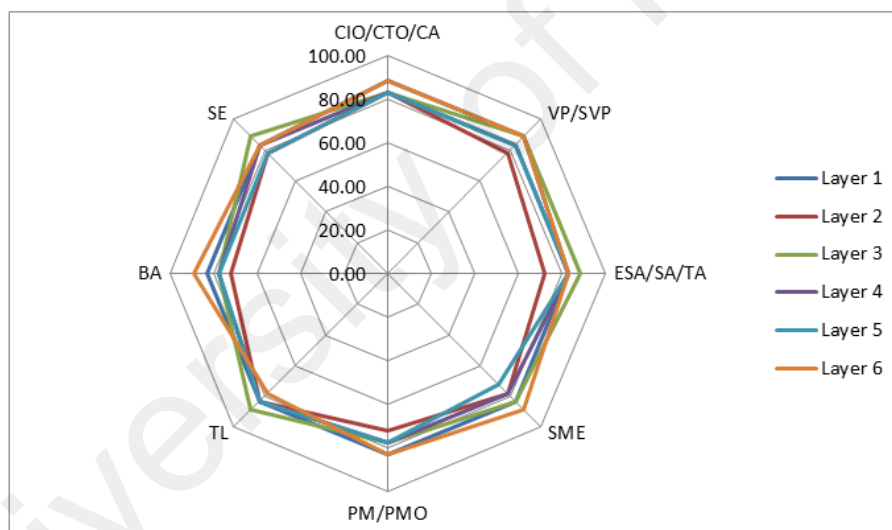


Figure 6.3: Overall Ease of Use of EASF

Figure 6.3 summaries responses from the eight categories of interviewees in relation to ease of use of the EASF. It shows that the interviewees were satisfied with ease of use of EASF, with scores ranging between 72% to 89% among all the six layers of the EASF.

The architects mentioned that some of the attributes such as authentication, authorization, integrity, availability and audit are frequently used in the secure environment. Nevertheless, other attributes are of moderate influence or ignorance from the software developers. Academician should be well equipped, push the boundaries, make efforts to experiment in the pilot project to ensure the framework is successfully implemented, learn about the commercial side of the business, and think of new ways to monetise their ESAF implementation approach beyond what achievable in the short time.

However, there is a lack of proper expertise in the in-house development teams. Organisations have to outsource the development works to vendors or to buy from off-the-shelf products to speed up the process. Therefore, bankers should pay attention and allocate resources to upgrade the in-house team capabilities. Furthermore, bankers should add the budget for security program blueprint for continuous improvement of staff's capabilities.

In order to develop ESAF, bankers need to have security experts and other professionals' involvement. Without their help, it is very difficult to implement. CIO, CTO and VPs suggested that one of the efficient innovations is to use the open-source community to evolve the ESAF. As of now, there is no similar ESAF in open-source community. It is a considerable investment of time and money in the technology start-up.

The criterion of efficiency is used to assess a project's cost-effectiveness. The central issue here is the economical use of resources. As per comments from bankers, applying ESA in a project requires 6-9 months, although whether bankers are willing to invest for this is still questionable. They can get the ROI indirectly. For instance, the average cost

of a data breach to institutions has risen to \$4 million. It is better to spend upfront capital expenditure (CAPEX) but it takes time to return their investment. As from a end-user's point of view, the functional requirements are more critical than the non-functional requirements. Nevertheless, top management is more concerned about the non-functional requirements rather than the functional requirements. Security is one of the vital elements of the non-functional requirements and it is fully achievable by the initial stage of the project. If the security requirement is not fulfilled, bankers are going to take an enormous risk as banking software is highly vulnerable. In the case of violations of security, CTO and CIO are answerable. Therefore, security requirements are compulsory for the banking requirements. For the implementation point of view, without getting basic security fundamentals, systems are unable to go live. According to banking CIOs, small banks typically spend 10 per cent and large banks spend 18 per cent of their non-interest expense on technology. The CTO, CIO and CA interviewed agreed that ESAF is the best way to strengthen the banker's security environment.

6.5 Assessment Two- Based on Scenario

In the second assessment, the experts (24 interviewees) assessed the ESAF based on some designated scenarios (top ten security attacks and threats). Tables 6.32 to 6.41 show the score of each layer in addressing the 10 designated scenarios, i.e. the common banking attacks and threats (see Section 2.2).

Table 6.32: Interviewees' Response of Malware Attack Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.375	1.88	0.625	2.50	0	0.00	0	0.00	0	0.00	72.92	M
Layer 2	0	0.00	0.416667	2.08	0.583333	2.33	0	0.00	0	0.00	0	0.00	73.61	M
Layer 3	0.125	0.75	0.5	2.50	0.375	1.50	0	0.00	0	0.00	0	0.00	79.17	H
Layer 4	0	0.00	0.666667	3.33	0.333333	1.33	0	0.00	0	0.00	0	0.00	77.78	H
Layer 5	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 6	0	0.00	0.666667	3.33	0.333333	1.33	0	0.00	0	0.00	0	0.00	77.78	H

Table 6.33: Interviewees' Response of DDOS Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.583333	2.92	0.416667	1.67	0	0.00	0	0.00	0	0.00	76.39	H
Layer 2	0	0.00	0.416667	2.08	0.583333	2.33	0	0.00	0	0.00	0	0.00	73.61	M
Layer 3	0.041667	0.25	0.75	3.75	0.208333	0.83	0	0.00	0	0.00	0	0.00	80.56	H
Layer 4	0.041667	0.25	0.666667	3.33	0.291667	1.17	0	0.00	0	0.00	0	0.00	79.17	H
Layer 5	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 6	0.125	0.75	0.666667	3.33	0.208333	0.83	0	0.00	0	0.00	0	0.00	81.94	H

Table 6.34: Interviewees' Response of Injection Flows Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.041667	0.25	0.583333	2.92	0.375	1.50	0	0.00	0	0.00	0	0.00	77.78	H
Layer 2	0.083333	0.50	0.333333	1.67	0.583333	2.33	0	0.00	0	0.00	0	0.00	75.00	H
Layer 3	0	0.00	0.375	1.88	0.625	2.50	0	0.00	0	0.00	0	0.00	72.92	M
Layer 4	0.041667	0.25	0.666667	3.33	0.291667	1.17	0	0.00	0	0.00	0	0.00	79.17	H
Layer 5	0	0.00	0.333333	1.67	0.666667	2.67	0	0.00	0	0.00	0	0.00	72.22	M
Layer 6	0	0.00	0.666667	3.33	0.333333	1.33	0	0.00	0	0.00	0	0.00	77.78	H

Table 6.35: Interviewees' Response of Social Engineering Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.583333	2.92	0.416667	1.67	0	0.00	0	0.00	0	0.00	76.39	H
Layer 2	0	0.00	0.416667	2.08	0.583333	2.33	0	0.00	0	0.00	0	0.00	73.61	M
Layer 3	N/A													
Layer 4	N/A													
Layer 5	N/A													
Layer 6	0.125	0.75	0.666667	3.33	0.208333	0.83	0	0.00	0	0.00	0	0.00	81.94	H

Table 6.36: Interviewees' Response of Network Eavesdropping Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.583333	2.92	0.416667	1.67	0	0.00	0	0.00	0	0.00	76.39	H
Layer 2	0	0.00	0.458333	2.29	0.541667	2.17	0	0.00	0	0.00	0	0.00	74.31	M
Layer 3	0	0.00	0.416667	2.08	0.583333	2.33	0	0.00	0	0.00	0	0.00	73.61	M
Layer 4	0	0.00	0.666667	3.33	0.333333	1.33	0	0.00	0	0.00	0	0.00	77.78	H
Layer 5	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 6	0	0.00	0.708333	3.54	0.291667	1.17	0	0.00	0	0.00	0	0.00	78.47	H

Table 6.37: Interviewees' Response of Data Disruption Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.041667	0.25	0.541667	2.71	0.416667	1.67	0	0.00	0	0.00	0	0.00	77.08	H
Layer 2	0	0.00	0.416667	2.08	0.583333	2.33	0	0.00	0	0.00	0	0.00	73.61	M
Layer 3	0	0.00	0.583333	2.92	0.416667	1.67	0	0.00	0	0.00	0	0.00	76.39	H
Layer 4	0.041667	0.25	0.666667	3.33	0.291667	1.17	0	0.00	0	0.00	0	0.00	79.17	H
Layer 5	0	0.00	0.708333	3.54	0.291667	1.17	0	0.00	0	0.00	0	0.00	78.47	H
Layer 6	0.041667	0.25	0.5	2.50	0.458333	1.83	0	0.00	0	0.00	0	0.00	76.39	H

Table 6.38: Interviewees' Response of Identity Theft Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.083333	0.50	0.5	2.50	0.416667	1.67	0	0.00	0	0.00	0	0.00	77.78	H
Layer 2	0	0.00	0.416667	2.08	0.583333	2.33	0	0.00	0	0.00	0	0.00	73.61	M
Layer 3	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 4	0.041667	0.25	0.583333	2.92	0.375	1.50	0	0.00	0	0.00	0	0.00	77.78	H
Layer 5	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 6	0.083333	0.50	0.666667	3.33	0.25	1.00	0	0.00	0	0.00	0	0.00	80.56	H

Table 6.39: Interviewees' Response of XSS Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.583333	2.92	0.416667	1.67	0	0.00	0	0.00	0	0.00	76.39	H
Layer 2	0	0.00	0.291667	1.46	0.708333	2.83	0	0.00	0	0.00	0	0.00	71.53	M
Layer 3	0	0.00	0.625	3.13	0.375	1.50	0	0.00	0	0.00	0	0.00	77.08	H
Layer 4	0.041667	0.25	0.666667	3.33	0.291667	1.17	0	0.00	0	0.00	0	0.00	79.17	H
Layer 5	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 6	0.041667	0.25	0.583333	2.92	0.375	1.50	0	0.00	0	0.00	0	0.00	77.78	H

Table 6.40: Interviewees' Response of Security Misconfiguration Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 2	0	0.00	0.375	1.88	0.625	2.50	0	0.00	0	0.00	0	0.00	72.92	M
Layer 3	0	0.00	0.458333	2.29	0.541667	2.17	0	0.00	0	0.00	0	0.00	74.31	M
Layer 4	0	0.00	0.75	3.75	0.25	1.00	0	0.00	0	0.00	0	0.00	79.17	H
Layer 5	0	0.00	0.541667	2.71	0.458333	1.83	0	0.00	0	0.00	0	0.00	75.69	H
Layer 6	0	0.00	0.708333	3.54	0.291667	1.17	0	0.00	0	0.00	0	0.00	78.47	H

Table 6.41: Interviewees' Response of Phishing Countermeasures from ESAF

ESAF Layers	Strongly Agree	score =6	Agree	Score=5	Some what Agree	Score=4	Some what disagree	Score=3	Disagree	score=2	Strongly Disagree	score=1	Total	RANK
Layer 1	0.166667	1.00	0.625	3.13	0.208333	0.83	0	0.00	0	0.00	0	0.00	82.64	H
Layer 2	0.083333	0.50	0.666667	3.33	0.25	1.00	0	0.00	0	0.00	0	0.00	80.56	H
Layer 3	N/A													
Layer 4	0.25	1.50	0.458333	2.29	0.25	1.00	0	0.00	0	0.00	0	0.00	79.86	H
Layer 5	0.083333	0.50	0.75	3.75	0.166667	0.67	0	0.00	0	0.00	0	0.00	81.94	H
Layer 6	0.208333	1.25	0.666667	3.33	0.125	0.50	0	0.00	0	0.00	0	0.00	84.72	H

6.5.1 Summary of the Countermeasures Interview Results

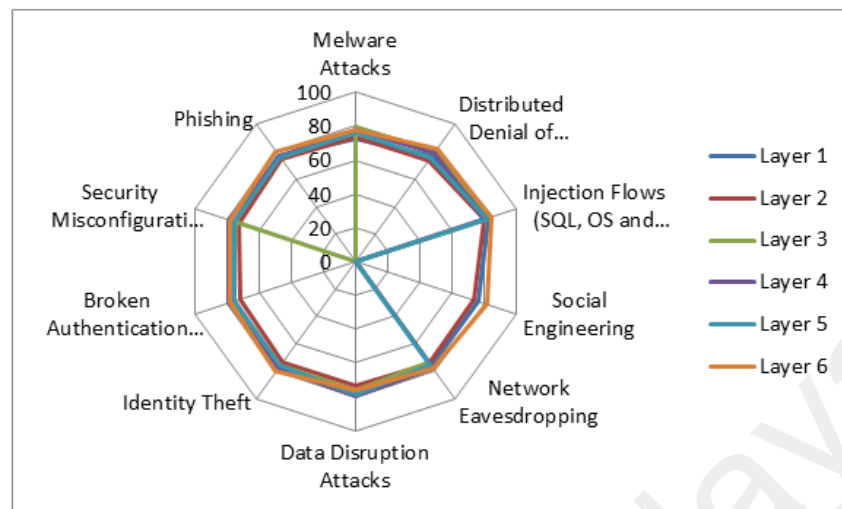


Figure 6.4: Summary of Countermeasures Interview Results

Figure 6.4 summarizes the responses from the ten scenarios of interviewees in relation to scenario-based assessment. It shows that the interviewees were satisfied with countermeasures, with scores ranging between 71% to 85% among all the six layers of the ESAF.

Table 6.42 shows the interviewees comments' of the scenario-based assessment.

Table 6.42: Scenario Responses

Scenario	Coverage of ESAF	Drawback/ improvement
1.Malware Attack	Full coverage	None
2.Distributed Denial of Service Attacks	Full coverage	None
3.Injection Flows (SQL, OS and LDAP)	Full coverage	None
4.Social Engineering	Full coverage	None
5.Network Eavesdropping	Full coverage	None

6.Data Disruption Attacks	Full coverage	None
7.Identity Theft	Full coverage	To incorporate multi factor authentication including finger print based authentication
8.Broken Authentication & Session Management and Cross-Site Scripting(XSS)	Full coverage	An internal security quality auditing process should be followed to catch the XSS vulnerabilities prior to production release
9. Security Misconfiguration	Full coverage	To install application firewall with virtual-patch integration capabilities.
10.Phishing	Full coverage	To install remote monitoring systems into banking environment to enhance banking operation capabilities.

Based on a scenario-based assessment, the experts interviewed agreed that ESAF is the best way to countermeasures the banker's security environment.

6.6 Summary

In this chapter, the researcher has discussed the evaluation results of the proposed ESAF in banking environments. The researcher examined the comprehensiveness, effectiveness, and ease of use of the proposed ESAF by inviting 24 experts in the banking domain to assess the ESAF. The experts play eight types of role in the banking domain. They also provided qualitative assessment on robustness of the ESAF in addressing 10 types of attacks and threats common to the banking domain. The evaluations have shown satisfactorily results. The next chapter concludes this research.

CHAPTER 7: CONCLUSION

7.1 Introduction

This chapter is organised into two sections. Section 7.2 includes the summary of the research, contributions, and the achievement of the objectives. The limitations of the research and future work that can be conducted are presented in Section 7.3.

7.2 Contributions and Achievement of the Objectives

In the present day, one of the major obstacles to embracing the enterprise architecture in the banking environment is security. A framework is effective only when its design meets the requirements. By conducting a literature review of the existing works, it was found that although there were disparate instances of frameworks and models on this subject, there wasn't a single comprehensive framework or model that addresses all the necessary components of the enterprise security architecture in the banking environment. The fundamental objective of the proposed framework is to fill this gap both in existing body of knowledge and in practice.

This research carefully examined the use of framework to enhance the security of the enterprise architecture of the banking systems in the banking environment. The study began with reviewing the existing concepts in theory and practice pertaining to enterprise architecture, enterprise architecture models, security architecture, security frameworks and related works on enterprise architecture security.

Theoretical research on security in the enterprise architecture is still in its preliminary stage. It is hoped that in times to come, the security models must leverage on a vital position and would emerge at the helm of the enterprise architecture. In this

research, efforts at enhancing the security of the enterprise architecture of the banking systems in banking environment consist of the following:

- To design a systematic and comprehensive security framework for banking systems in the banking environment
- Evaluate the security framework for banking systems in the banking environment

In this thesis, a comprehensive framework has been introduced which covers the significant security requirements of ESA reflecting the vitality of this subject. In the proposed ESAF for banking environments, the key components of security are defined.

The foremost contributions of this research study are stated as follows:

- Systematically analysed the strengths and weaknesses of EAF, SAF and BSF and further identified ES practices and ESA attributes in the banking environments.
- Proposed an ESAF for the banking environment.
- Detailed industrial experts' evaluations of the proposed ESAF.

Therefore, the primary objectives of the study have been achieved:

1. The goal of this research is to establish, and enable an ESA framework (ESAF) in the banking industry. This research objective has been accomplished through:
 - a) Outlining and examining the EA security requirements
 - b) Defining and detailing the EA security scenarios for banking environments
 - c) Determining the suitability of the enterprise security architecture for banking environments

2. By proposing and developing an ESAF for the banking industry. This research objective has been accomplished through:
 - a) Defining an ESAF for the banking environments.
 - b) Defining all the ESA components in the framework.
 - c) Classifying key components in the ESAF.
3. The evaluation of the proposed ESAF for the banking industry. This research objective has been accomplished through:
 - a) Designing evaluation criteria for assessment of the ESAF
 - b) Applying evaluation criteria by industrial experts who are in the banking and security domain to assess comprehensiveness, effectiveness, and ease of use of the ESAF for the banking industry.

7.3 Limitations and Future Work

The following are the limitations of this research:

- It was a difficult task to get the bankers to cooperate and take part in the study, and thus obstructed an extensive implementation of the proposed framework for banking systems.
- Most of the bankers stated that it is necessary to test the feasibility of this proposed framework in a practical environment with reference site or customer.
- Bankers were sceptical to disclose systems and sensitive data to the researcher. Thus, the design of the ESAF was mainly based on literature and feedback from a limited number of participants in the industry.
- Currently, the evaluation of ESAF is focused only on three key areas, but it should add more criteria to improve the assessment.

The research ought to pave the way for further research on improving the ESAF in the banking environment. Future research perspectives should consider the following:

- The proposed ESAF for the banking environment can be applied in core banking or any of the financial related systems, focusing on some key security modules and system behaviours.
- An inclusive evaluation of ESAF that encompasses further case studies aligned with the coherent approach, shall further enlighten the use of the proposed ESAF for banking systems.
- The assessment of ESA standards and methods in banking system development is at a premature stage and it is necessary to conduct more research in these areas. The new finding in these areas shall be incorporated into the proposed ESAF to further enhance it.

REFERENCES

- Ahlemann, F., Stettiner, E., Messerschmidt, M., & Legner, C. (2012). *Strategic enterprise architecture management: challenges, best practices, and future developments*: Springer Science & Business Media.
- Alkassar, A., Husseini, R., Stüble, C., & Hartmann, M. (2007). A Security Architecture for Enterprise Rights Management *ISSE/SECURE 2007 Securing Electronic Business Processes*, Springer.
- Allen, J. (2005). Governing for enterprise security: DTIC Document.
- Ampratwum, F. E., (2009). Advance fee fraud “419” and investor confidence in the economies of sub-Saharan African (SSA). *Journal of Financial Crime*, 16(1), 67-79.
- Anderson, A. I., Compton, D., & Mason, T. (2004). Managing in a dangerous world—the national incident management system. *Engineering Management Journal*, 16(4), 3-9.
- Anderson, J. A., & Rachamadugu, V. (2008). *Managing security and privacy integration across enterprise business process and infrastructure*. Paper presented at the IEEE International Conference on Services Computing.
- Arconati, N. (2002). One approach to enterprise security architecture. *SANS Infosec Reading room*. Retrived September 5, 2012, From <http://www.sans.org/rr/whitepapers/policyissues/504.php>
- Atashzar, H., Torkaman, A., Bahrololom, M., & Tadayon, M. H. (2011). *A survey on web application vulnerabilities and countermeasures*. Paper presented at the 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), International Convention Center Jeju, Korea (South).
- Atoum, I., Ootom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3), 251-264.
- Back, A. (2002). Hashcash-a denial of service counter-measure.
- Baggen, R., Correia, J. P., Schill, K., & Visser, J. (2012). Standardized code quality benchmarking for improving software maintainability. *Software Quality Journal*, 20(2), 287-307.
- Bahmani, F., Shariati, M., & Shams, F. (2010). *A survey of interoperability in Enterprise Information Security Architecture frameworks*. Paper presented at the The 2nd International Conference on Information Science and Engineering (ICISE), Hangzhou, China.
- Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. *Computers & Security*, 43, 77-89.

- Baker, E. M., Tedesco, J. C., & Baker, W. H. (2008). Consumer privacy and trust online: An experimental analysis of anti-phishing promotional effects. *Journal of Website Promotion*, 2(1-2), 89-113.
- Barateiro, J., Antunes, G., & Borbinha, J. (2011, April 27-29, 2011). *Long-term security of digital information: Assessment through risk management and Enterprise Architecture*. Paper presented at the EUROCON-International Conference on Computer as a Tool (EUROCON), Lisbon, Portugal.
- Bass, T., & Mabry, R. (2004). *Enterprise architecture reference models: A shared vision for Service-Oriented Architectures*. Paper presented at the IEEE MILCOM.
- Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. *British Journal of Management*, 18(1), 63-77.
- Berg, B. L., Lune, H., & Lune, H. (2004). *Qualitative research methods for the social sciences* (Vol. 5): Pearson Boston, MA.
- Berio, G., & Vernadat, F. (2001). Enterprise modelling with CIMOSA: functional and organizational aspects. *Production Planning & Control*, 12(2), 128-136.
- Bernroider, E. W., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, 29(3), 325-336.
- Beyleveld, D. (2007). Data protection and genetics: medical research and the public good. *King's Law Journal*, 18(2), 275-289.
- Bhati, M., & Khan, R. (2012). Prevention Approach of Phishing on Different Websites. *International Journal of Engineering and Technology*, 2(7).
- Biswas, S., Taleb, A., & Shinwary, S. S. (2011). Electronic Banking in Bangladesh: Security Issues, Forms, Opportunities and Challenges. *Canadian Journal on Scientific and Industrial Research*, 2(5), 181-194.
- Blackwell, C. (2010). *A Security Architecture to Protect Against Data Loss. Information Security and Digital Forensics*, Springer.
- Blake, E. A. (2007). Network and Database Security: Regulatory Compliance, Network, and Database Security-A Unified Process and Goal. *Journal of Digital Forensics, Security and Law*, 2(4), 77-106.
- Bleumer, G. (2007). General Security Architecture. *Electronic Postage Systems: Technology, Security, Economics*, 119-125.
- Bodkin, R. (2004). *Enterprise security aspects*. Paper presented at the AOSD'04 International Conference on Aspect-Oriented Software Development.

- Bowman-Amuah, M. K. (2001). System, method and article of manufacture for security management in a development architecture framework: Google Patents.
- Bradley, D., & Josang, A. (2004). *Mesmerize: an open framework for enterprise security management*. Paper presented at the Proceedings of the Second Workshop on Australasian Information Security (AISW2004), Dunedin, New Zealand.
- Breu, R., Oberperfler, F. I., & Yautsiukhin, A. (2008). *Quantitative assessment of enterprise security system*. Paper presented at the Third International Conference on Availability, Reliability and Security, 2008(ARES 08).
- Brown, A., Hossain, M., & Nguyen, D.-T. (2005). *Telecommunications reform in the Asia-Pacific region*: Edward Elgar Publishing.
- Buckl, S., Ernst, A. M., Matthes, F., Ramacher, R., & Schweda, C. M. (2009). *Using enterprise architecture management patterns to complement TOGAF*. Paper presented at the Enterprise Distributed Object Computing Conference, 2009. EDOC'09. IEEE International.
- Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal: A Global Perspective*, 21(1), 47-54.
- Bylund, M., & Waern, A. (1998). Service contracts: coordination of user-adaptation in open service architectures. *Personal Technologies*, 2(3), 188-199.
- Camp, L. J., & Johnson, M. E. (2012). *The economics of financial and medical identity theft*: Springer Science & Business Media.
- Campbell, D., & Campbell, C. T. (2009). *Legal aspects of doing business in Asia and the Pacific*: Lulu. com.
- Caralli, R. A., Allen, J. H., Stevens, J. F., Willke, B. J., & Wilson, W. R. (2004). Managing for enterprise security: DTIC Document.
- Caralli, R. A., Stevens, J. F., Willke, B. J., & Wilson, W. R. (2004). The critical success factor method: establishing a foundation for enterprise security management: DTIC Document.
- Casado, M., Garfinkel, T., Akella, A., Freedman, M. J., Boneh, D., McKeown, N., & Shenker, S. (2006). *SANE: A Protection Architecture for Enterprise Networks*. Paper presented at the Usenix Security.
- Casey, E. (2006). Investigating sophisticated security breaches. *Communications of the ACM*, 49(2), 48-55.
- Chabanel, P.-E. (2011). Implementing Basel III: challenges, options & opportunities. *AmericAS*, 1, 553.1658.

- Chew, E. K. (2009). *Information Technology Strategy and Management: Best Practices: Best Practices*: IGI Global.
- Chmielecki, T., Cholda, P., Pacyna, P., Potrawka, P., Rapacz, N., Stankiewicz, R., & Wydrych, P. (2014). *Enterprise-oriented cybersecurity management*. Paper presented at the Federated Conference on Computer Science and Information Systems (FedCSIS), 2014
- Conklin, A., White, G., Cothren, C., Williams, D., & Davis, R. L. (2004). *Principles of computer security: security and beyond*: McGraw-Hill, Inc.
- Council, C. (1999). Federal enterprise architecture framework version 1.1. Retrieved September 5, 2012, from <http://www.whitehouse.gov/omb/egov/a-1-fea.html> CIO Council.
- Covington, M. J., Fogla, P., Zhan, Z., & Ahamad, M. (2002). *A context-aware security architecture for emerging applications*. Paper presented at the 18th Annual Computer Security Applications Conference (ACSAC), Las Vegas, NV.
- Cramer, R., & Shoup, V. (1998). *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*. Paper presented at the Advances in Cryptology—CRYPTO'98.
- Curts, R. J., & Campbell, D. E. (1999). *Architecture: the road to interoperability*. Paper presented at the Command & Control Research & Technology Symposium (CCRTS), US Naval War College, Newport, RI.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.
- Da Silva, F. Q., Santos, A. L., Soares, S., França, A. C. C., Monteiro, C. V., & Maciel, F. F. (2011). Six years of systematic literature reviews in software engineering: An updated tertiary study. *Information and Software Technology*, 53(9), 899-913.
- Dacey, R. F. (2010). *Federal Information System Controls Audit Manual (FISCAM)*: DIANE Publishing.
- Dai, L., & Cooper, K. (2007). Using FDAF to bridge the gap between enterprise and software architectures for security. *Science of Computer Programming*, 66(1), 87-102.
- Davis, N., Humphrey, W., Redwine, S. T., Zibulski, G., & McGraw, G. (2004). Processes for producing secure software. *IEEE Security & Privacy*, 2(3), 18-25.
- De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, 27(1), 307-324.

- Delrue, G. (2014). *Money Laundering and Terrorist Financing* (2nd edition). Maklu.
- Demchenko, Y., De Laat, C., Koeroo, O., & Groep, D. (2008). *Re-thinking grid security architecture*. Paper presented at the Fourth IEEE International Conference on eScience, Indianapolis, USA.
- Demme, J., Maycock, M., Schmitz, J., Tang, A., Waksman, A., Sethumadhavan, S., & Stolfo, S. (2013). On the feasibility of online malware detection with performance counters. *ACM SIGARCH Computer Architecture News*, 41(3), 559-570.
- Dhinakaran, C., Nagamalai, D., & Lee, J. K. (2011). Multilayer approach to defend phishing attacks. *Journal Internet Technology*, 11(3), 417-425
- Dimitriadis, C. K. (2007). Analyzing the security of Internet banking authentication mechanisms. *Information Systems Control Journal*, 3, 34.
- Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., & Tang, J.-M. (2002). *Framework for security and privacy in automotive telematics*. Paper presented at the Proceedings of the 2nd international workshop on Mobile commerce.
- Ekstedt, M., & Sommestad, T. (2009). *Enterprise architecture models for cyber security analysis*. Paper presented at the Power Systems Conference and Exposition (PSCE'09), Seattle, Washington.
- Elgamal, T., Treuhaft, J., & Chen, F. (1996). Securing Communications on the Intranet and over the Internet. *White Paper, Netscape Communications Corporation*.
- Enose, N. (2014). *Implementing an integrated security management framework to ensure a secure smart grid*. Paper presented at the International Conference on Advances in Computing, Communications and Informatics (ICACCI, 2014).
- Ericsson, G. N. (2007). Toward a framework for managing information security for an electric power utility—CIGRÉ experiences. *IEEE Transactions on Power Delivery*, 22(3), 1461-1469.
- Etaher, N., Weir, G. R., & Alazab, M. (2015). *From Zeus to Zitmo: Trends in Banking Malware*. Paper presented at the 2015 IEEE Trustcom/BigDataSE/ISPA.
- Falcioni, D., Ippoliti, F., Marcantoni, F., & Re, B. (2013). *Digital Identity into Practice: The Case of UniCam Technology-Enabled Innovation for Democracy, Government and Governance*, Springer.
- Farooqui, K., Logrippo, L., & de Meer, J. (1995). The ISO reference model for open distributed processing: an introduction. *Computer Networks and ISDN Systems*, 27(8), 1215-1229.
- Fay, J. (2007). *Encyclopedia of security management*. Butterworth-Heinemann.

- Field, K. M. (2009). Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act. *Michigan Law Review*, 819-852.
- Fitzgerald, K. J. (1994). Establishing Security in a Multi-platform, Multi-vendor Enterprise-wide IT Environment. *Information Management & Computer Security*, 2(4), 9-15.
- Fogie, S., Grossman, J., Hansen, R., Rager, A., & Petkov, P. D. (2011). *XSS attacks: cross site scripting exploits and defense*. Syngress.
- Fong, E. N., & Goldfine, A. H. (1989). Information management directions: the integration challenge. *ACM SIGMOD Record*, 18(4), 40-43.
- Fonseca, J., Vieira, M., & Madeira, H. (2007). *Testing and comparing Web vulnerability scanning tools for SQL injection and XSS attacks*. Paper presented at the International Symposium on 13th Pacific Rim Dependable Computing, 2007. PRDC 2007.
- Fonseca, J., Vieira, M., & Madeira, H. (2009). *Vulnerability & attack injection for web applications*. Paper presented at the IEEE/IFIP International Conference on Dependable Systems & Networks, 2009. (DSN'09).
- Foorhuis, R., & Brinkkemper, S. (2007). A framework for local project architecture in the context of enterprise architecture. *Journal of Enterprise Architecture*, 3(4), 51-63.
- Force, I.-I. T. (1999). GERAM: Generalised enterprise reference architecture and methodology. *IFIP-IFAC Task Force on Architectures for Enterprise Integration March Version*, 1(3).
- Foster, I., Kesselman, C., Tsudik, G., & Tuecke, S. (1998). *A security architecture for computational grids*. Paper presented at the Proceedings of the 5th ACM Conference on Computer and Communications Security.
- Framework, N. (2010). Roadmap for smart grid interoperability standards. *National Institute of Standards and Technology*.
- Franke, U., Johnson, P., Ericsson, E., Flores, W. R., & Zhu, K. (2009). *Enterprise architecture analysis using fault trees and MODAF*. Paper presented at the Proceedings of CAiSE Forum.
- Friedrichs, O. (2008). *Cybercrime and the Electoral System*: forthcoming, Symantec Press.
- Fultz, N., & Grossklags, J. (2009). Blue versus red: Towards a model of distributed security attacks; *Financial Cryptography and Data Security*, Springer.
- Galinec, D., & Luić, L. (2011). *The Impact of Application Non-Functional Requirements on Enterprise Architecture*. Paper presented at the CECIIS-2011.

- Ganame, A. K., Bourgeois, J., Bidou, R., & Spies, F. (2008). A global security architecture for intrusion detection on computer networks. *Computers & Security*, 27(1), 30-47.
- Garfinkel, S. (2002). *Adopting fair information practices to low cost RFID systems*. Paper presented at the Privacy in Ubiquitous Computing Workshop.
- Gasmi, Y., Sadeghi, A.-R., Stewin, P., Unger, M., Winandy, M., Husseini, R., & Stübke, C. (2008). *Flexible and secure enterprise rights management based on trusted virtual domains*. Paper presented at the Proceedings of the 3rd ACM workshop on Scalable trusted computing.
- Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, 26(3), 298-303.
- Giri, M., & Singh, D. D. (2014). Analysis of recognition based authentication system hybrid with text based password mix with random generated password. *International Journal of Research in Computer Engineering & Electronics*, 3(3).
- Glukhov, V., Ilin, I., & Anisiforov, A. (2015). *Problems of data protection in industrial corporations enterprise architecture*. Paper presented at the Proceedings of the 8th International Conference on Security of Information and Networks.
- Goikoetxea, A. (2007). *Enterprise architectures and digital administration: Planning, design and assessment*. World Scientific.
- Golden, C. (1994). A standard satellite control reference model.
- Grandry, E., Feltus, C., & Dubois, E. (2013). *Conceptual integration of enterprise architecture management and security risk management*. Paper presented at the 17th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW).
- Grid, N. S. (2010). Introduction to NISTIR 7628 guidelines for smart grid cyber security. *Guideline, Sep*.
- Gutiérrez, C., Fernández-Medina, E., & Piattini, M. (2005). *Web services enterprise security architecture: a case study*. Paper presented at the Proceedings of the 2005 Workshop on Secure Web Services.
- Hagan, P. (2004). 2.5 Historical Developments in EA 9. *Guide to the (Evolving) Enterprise Architecture Body of Knowledge*, 22.
- Haigh, T. (1995). *Virtual enterprises and the enterprise security architecture*. Paper presented at the New Security Paradigms Workshop, 1995.
- Hamilton Jr, J. A., Rosen, J. D., & Summers, P. A. (2002). An interoperability road map for C4ISR legacy systems. DTIC Document.

- Harkins, M. (2013). *A New Security Architecture to Improve Business Agility Managing Risk and Information Security*, Springer.
- Harle, P., Luders, E., Pepanides, T., Pfetsch, S., Poppensieker, T., & Stegemann, U. (2010). Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation., EMEA Banking.
- Härtig, H. (2002). *Security architectures revisited*. Paper presented at the Proceedings of the 10th Workshop on ACM SIGOPS European Workshop.
- Hartig, H., Kowalski, O., & Kuhnhauser, W. (1993). *The Birlix security architecture*. *Journal of Computer Security*, 2 (1), 5-21.
- Heffner, C., & Yap, D. (2009). Security Vulnerabilities in SOHO Routers. Retrieved September 15, 2014 from <https://www.exploit-db.com/docs/252.pdf>.
- Henning, R. R. (1999). *Security service level agreements: quantifiable security for the enterprise?* Paper presented at the Proceedings of the 1999 Workshop on New Security Paradigms.
- Hinde, S. (2002). Spam, scams, chains, hoaxes and other junk mail. *Computers & Security*, 21(7), 592-606.
- Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243-248.
- Hood, K. L., & Yang, J.-W. (1998). Impact of Banking Information Systems Security on Banking in China: The Case of Large State-Owned Banks in Shenzhen Economic Special Zone - An Introduction. *Journal of Global Information Management (JGIM)*, 6(3), 5-16.
- Hutchinson, D., & Warren, M. (2003). Security for internet banking: A framework. *Logistics Information Management*, 16(1), 64-73.
- II, R. T., Beamer Jr, R. A., & Sowell, P. K. (2000). Civilian Application of the DOD C4ISR Architecture Framework: A Treasury Department Case Study.
- Ingalsbe, J. A., Shoemaker, D., Mead, N. R., & Drommi, A. (2008). Threat Modeling the Enterprise. *AMCIS 2008 Proceedings*, 133.
- Isomäki, H., & Liimatainen, K. (2008). Challenges of government enterprise architecture work—stakeholders' views *Electronic Government*, Springer.
- Itani, W., & Kayssi, A. (2004). SPECSA: a scalable, policy-driven, extensible, and customizable security architecture for wireless enterprise applications. *Computer Communications*, 27(18), 1825-1839.
- Jabbour, G. G., & Menasce, D. A. (2009). *The insider threat security architecture: a framework for an integrated, inseparable, and uninterrupted self-protection*

mechanism. Paper presented at the International Conference on Computational Science and Engineering, 2009 (CSE'09).

Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Jardine, E. (2015). Global cyberspace is safer than you think: Real trends in cybercrime. Available at SSRN 2634590 Retrieved April 15, 2016 from <https://www.cigionline.org/publications/global-cyberspace-safer-you-think-real-trends-cybercrime>.

Jesudoss, A., & Subramaniam, N. (2014). A Survey on Authentication Attacks and Countermeasures in a Distributed Environment. *International Journal of Computer Sciences and Engineering (IJCSE)*, 5(2) 152- 164.

Josey, A. (2009). TOGAF Version 9.1 Enterprise Edition: An Introduction. *The Open Group*, 11.

Joshi, J., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. *Communications of the ACM*, 44(2), 38-44.

Joshi, K., Yesha, Y., Finin, T., & Yesha, Y. (2013). A policy-based cloud broker for the VCL platform. *International Journal of Cloud Computing I*, 2(2-3), 288-303.

Kang, D., Lee, J., Choi, S., & Kim, K. (2010). An ontology-based enterprise architecture. *Expert Systems with Applications*, 37(2), 1456-1464.

Kark, K., Stamp, O., Koetzle, L., & Mulligan, J. (2007). Defining a high-level security framework: Putting basic security principles to work: Cambridge Forrester Research.

Kee, J. (2008). Social engineering: Manipulating the source. *GCIA Gold Certification*.

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical report, Ver. 2.3: EBSE Technical Report*.

Kern, A., Kuhlmann, M., Schaad, A., & Moffett, J. (2002). *Observations on the role life-cycle in the context of enterprise security management*. Paper presented at the Proceedings of the seventh ACM symposium on Access control models and technologies.

Khattak, N. A., Chadwick, D., Bhatti, R. A., Shad, S. A., Butt, F. S., & Munir, E. U. (2014). Assessment of anti spyware tools for signature and behavior base techniques. *Science International*, 26 (5).

Kim, D., & Solomon, M. G. (2013). *Fundamentals of information systems security*: Jones & Bartlett Publishers.

- Kim, J.-S., Lee, S., Kim, M., Seo, J.-H., & Noh, B.-N. (2006). A security architecture for adapting multiple access control models to operating systems ; *Computational Science and Its Applications-ICCSA 2006*, Springer.
- Kim, S., & Seong Leem, C. (2005). Enterprise security architecture in business convergence environments. *Industrial Management & Data Systems*, 105(7), 919-936.
- Kim, Y.-G., & Cha, S. (2012). Security Engineering Methodology for Developing Secure Enterprise Information Systems: An Overview *Embedded and Multimedia Computing Technology and Service*, Springer.
- Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering—a systematic literature review. *Information and Software Technology*, 51(1), 7-15.
- Kocher, P., Lee, R., McGraw, G., Raghunathan, A., & Moderator-Ravi, S. (2004). *Security as a new dimension in embedded system design*. Paper presented at the Proceedings of the 41st Annual Design Automation Conference.
- Kolter, J., Schillinger, R., & Pernul, G. (2007). Building a Distributed Semantic-aware Security Architecture *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 397-408): Springer.
- Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, 58, 39-46.
- Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.
- Kozina, M. (2006). Evaluation of Aris and Zachman frameworks as enterprise architectures. *Journal of Information and Organizational sciences*, 30(1), 115-136.
- Krafzig, D., Banke, K., & Slama, D. (2005). *Enterprise SOA: Service-oriented architecture best practices*: Prentice Hall Professional.
- Kruchten, P. (1995). Architectural Blueprints—The “4+ 1” View Model of Software Architecture. *Proceedings of Tri-Ada Tutorial*, 95, 540-555.
- Kruchten, P. B. (1995). The 4+ 1 view model of architecture. *IEEE Software*, 12(6), 42-50.
- Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing*. Sage.
- Lankhorst, M. (2009). Enterprise Architecture at Work: Modelling, Communication and Analysis (The Enterprise Engineering Series).

- Lapkin, A. (2005). Gartner's enterprise architecture process and framework help meet 21st century challenges. *Gartner Research Paper, ID(G00133132)*.
- Leitold, H., Hollosi, A., & Posch, R. (2002). *Security architecture of the Austrian citizen card concept*. Paper presented at the 2002 18th Annual Computer Security Applications Conference.
- Li, F., Luo, B., & Liu, P. (2010). *Secure information aggregation for smart grids using homomorphic encryption*. Paper presented at the 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm).
- Liao, Z., & Cheung, M. T. (2005). *Service quality in internet e-banking: a user-based core framework*. Paper presented at the The 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2005. EEE'05.
- Librero, F., & Arinto, P. B. (2007). Digital review of Asia Pacific, 2007-2008.
- Lillehagen, F., & Krogstie, J. (2008). *Active knowledge modeling of enterprises*. Springer Science & Business Media.
- Lim, N., Yeow, P. H., & Yuen, Y. Y. (2010). An online banking security framework and a cross-cultural comparison. *Journal of Global Information Technology Management, 13*(3), 39-62.
- Linstrom, P., & Mallard, W. (2003). National Institute of Standards and Technology. Gaithersburg, MD, March, 20899.
- Lowman, T., & Mosier, D. (1997). *Applying the DoD Goal Security Architecture as a methodology for the development of system and enterprise security architectures*. Paper presented at the 1997 13th Annual Computer Security Applications Conference.
- Ludl, C., McAllister, S., Kirda, E., & Kruegel, C. (2007). *On the effectiveness of techniques to detect phishing sites*. Paper presented at the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).
- Ma, F. (2010). *Automation Flow for Defence Architecture Operational Sub-Views of Canadian Forces Operational Commands*. Paper presented at the Proceedings of the World Congress on Engineering and Computer Science.
- Maes, R., Rijsenbrij, D., Truijens, O., & Goedvolk, H. (2000). *Redefining business: IT alignment through a unified framework*. Universiteit van Amsterdam, Department of Accountancy & Information Management.
- Mahmood, Z. (2013). *Developing E-Government Projects: Frameworks and Methodologies*, IGI Global.
- Malin, C. H., Casey, E., & Aquilina, J. M. (2008). *Malware forensics: Investigating and analyzing malicious code*, Syngress.

- Malveau, R., & Mowbray, T. J. (2003). *Software Architect Bootcamp*. Prentice Hall Professional Technical Reference.
- Mary, S. R., & Rodrigues, P. (2011). Survey and Comparison of Frameworks in Software Architecture; *Advances in Computing and Communications*, Springer.
- Mason, S. (2012). *Electronic signatures in law*. Cambridge University Press.
- Mazziotti, G. (2008). *EU digital copyright law and the end-user*. Springer Science & Business Media.
- McCombie, S., & Pieprzyk, J. (2010). *Winning the phishing war: A strategy for Australia*. Paper presented at the 2010 Second Cybercrime and Trustworthy Computing Workshop (CTC).
- McGovern, J., Sims, O., Jain, A., & Little, M. (2006). *Enterprise Service Oriented Architectures: Concepts, Challenges, Recommendations*, 189-234.
- Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (2003). *Improving web application security: Threats and countermeasures*. Microsoft Redmond, WA.
- Mellado, D., Fernández-Medina, E., & Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces*, 29(2), 244-253.
- Mellado, D., Fernández-Medina, E., & Piattini, M. (2010). Security requirements engineering framework for software product lines. *Information and Software Technology*, 52(10), 1094-1117.
- Minoli, D. (2008). *Enterprise architecture A to Z: Frameworks, business process modeling, SOA, and infrastructure technology*. CRC Press.
- Möckel, C. (2011). *Usability and Security in EU E-Banking Systems-Towards an Integrated Evaluation Framework*. Paper presented at the 2011 IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT).
- Model, M. The DoDAF Architecture Framework Version 2.02. Retrieved April 25, 2016 from <http://dodcio.defense.gov/Library/DoD-Architecture-Framework/>
- Mohammadi, N. G., Paulus, S., Bishr, M., Metzger, A., Könnecke, H., Hartenstein, S., Pohl, K. (2014). Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems *Cloud Computing and Services Science* (pp. 19-35), Springer.
- Molva, R. (1999). Internet security architecture. *Computer Networks*, 31(8), 787-804.
- Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4), 248-263.

- Moore, A. P., Ellison, R. J., & Linger, R. C. (2001). Attack modeling for information security and survivability. DTIC Document.
- Moral-García, S., Moral-Rubio, S., Fernández, E. B., & Fernández-Medina, E. (2014). Enterprise security pattern: A model-driven architecture instance. *Computer Standards & Interfaces*, 36(4), 748-758.
- Moriconi, M., Qian, X., Riemenschneider, R. A., & Gong, L. (1997). *Secure software architectures*. Paper presented at the 1997 IEEE Symposium on Security and Privacy, 1997.
- Mousa, A., & Hamad, A. (2006). Evaluation of the RC4 Algorithm for Data Encryption. *International Journal of Computer Science & Applications (IJCSA)*, 3(2), 44-56.
- Mukkamala, R., Chekuri, L., Moharrum, M., & Palley, S. (2004). Policy-Based Security Management for Enterprise Systems. *Research Directions in Data and Applications Security XVIII* (pp. 219-233): Springer.
- Murphy, B., Boren, R., & Schlarman, S. (2000). Enterprise security architecture.
- Murray, W. H. (1998). Enterprise security architecture. *Information Systems Security*, 6(4), 43-54.
- Myagmar, S., Lee, A. J., & Yurcik, W. (2005). *Threat modeling as a basis for security requirements*. Paper presented at the Symposium on requirements engineering for information security (SREIS).
- Nagaratnam, N., Janson, P., Dayka, J., Nadalin, A., Siebenlist, F., Welch, V., Foster, I., Tuecke, S. (2002). The security architecture for open grid services. *Open Grid Service Architecture Security Working Group (OGSA-SEC-WG)*, 1-31.
- Nakamura, Y., Hada, S., & Neyama, R. (2002). *Towards the integration of Web services security on enterprise environments*. Paper presented at the 2002 Symposium on Applications and the Internet (SAINT) Workshops.
- Narendiran, C., Rabara, S. A., & Rajendran, N. (2008). *Performance evaluation on end-to-end security architecture for mobile banking system*. Paper presented at the 1st IFIP Wireless Days, 2008. WD'08..
- Narendiran, C., Rabara, S. A., & Rajendran, N. (2009). *Public key infrastructure for mobile banking security*. Paper presented at the Global Mobile Congress 2009.
- Nazario, J. (2004). *Defense and detection strategies against Internet worms*. Artech House.
- Noran, O. (2003a). An analysis of the Zachman framework for enterprise architecture from the GERAM perspective. *Annual Reviews in Control*, 27(2), 163-183.

- Noran, O. (2003b). A mapping of individual architecture frameworks (GRAI, Pera, C4ISR, CIMOSA, Zachman, ARIS) onto GERAM. *Handbook on enterprise architecture* (pp. 65-210): Springer.
- Norige, A., Yenson, S., Elkin, G., Mapar, J., & Legary, J. (2012). *Homeland Security Exercise and Evaluation Program-Enterprise platform (HSEEP-EP): An innovative service oriented architecture approach*. Paper presented at the 2012 IEEE Conference on Technologies for Homeland Security (HST).
- Norman, T. L. (2014). *Integrated Security Systems Design: A Complete Reference for Building Enterprise-wide Digital Security Systems*. Butterworth-Heinemann.
- Nyanchama, M., & Sop, P. (2001). Enterprise security management: Managing complexity. *Information Systems Security*, 9(6), 1-8.
- Nyang, D., Mohaisen, A., Kwon, T., Kang, B., & Stavrou, A. (2011). Decryptable to Your Eyes: Visualization of Security Protocols at the User Interface. *1112.2245*.
- Oda, S. M., Fu, H., & Zhu, Y. (2009). *Enterprise information security architecture a review of frameworks, methodology, and case studies*. Paper presented at the 2nd IEEE International Conference on Computer Science and Information Technology, 2009 (ICCSIT 2009).
- Okuhara, V. T. S. V. M., & Yoshikawa, V. N. (2007). Fujitsu enterprise security architecture. *FUJITSU Sci. Tech. J*, 43(2), 153-158.
- Onwubiko, C. (2009). A security audit framework for security management in the enterprise. *Global Security, Safety, and Sustainability*, Springer.
- Ota, D., & Gerz, M. (2011). Benefits and challenges of architecture frameworks: DTIC Document.
- Overton, M. (2007). An African AFF-air. *Spam Bulletin*, April, 2007.
- Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud computing: Security issues and research challenges. *International Journal of Computer Science and Information Technology & Security* 1(2), 136-146.
- Pereira, C. M., & Sousa, P. (2004). *A method to define an enterprise architecture using the Zachman framework*. Paper presented at the Proceedings of the 2004 ACM symposium on Applied computing.
- Peristeras, V., & Tarabanis, K. (2004). Advancing the government enterprise architecture—GEA. the service execution object model *Electronic Government*, Springer.
- Petty, C., & Stevens, H. (2009). Gartner says number of phishing attacks on us consumers increased 40 percent in 2008: April. from <https://www.gartner.com/newsroom/id/936913>

- Pfleeger, C. P., & Pfleeger, S. L. (2002). *Security in computing*. Prentice Hall
- Piaszczyk, C. (2011). Model based systems engineering with Department of Defense Architectural Framework. *Systems Engineering*, 14(3), 305-326.
- Pistoia, M., Fink, S. J., Flynn, R. J., & Yahav, E. (2007). *When role models have flaws: Static validation of enterprise security policies*. Paper presented at the 29th International Conference on Software Engineering, 2007 (ICSE 2007).
- Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services business–enterprise architecture as a coordination tool. *Journal of Systems and Software*, 80(10), 1607-1620.
- Ramachandran, J. (2002). *Designing security architecture solutions*: John Wiley & Sons.
- Ramadan, A., & Hefnawi, M. (2007). A Network Security Architecture Using The Zachman Framework. *Managing Critical Infrastructure Risks* (pp. 133-143): Springer.
- Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. DTIC Document.
- Rathwell, G. A., & Williams, T. J. (1996). Use of the Purdue enterprise reference architecture and methodology in industry (the Fluor Daniel example) *Modelling and Methodologies for Enterprise Integration* (pp. 12-44): Springer.
- Reedy, P., & Buzzeo, J. (2013) *Digital Evidence*. Paper presented at the 17th Interpol International Forensic Science Managers Symposium, Lyon.
- Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIREs: A policy framework for information security. *Communications of the ACM*, 46(7), 101-106.
- Reid, J., & Du Preez, N. (1998). Evaluation of the GRAI Integrated Methodology and the IMAGIM Supportware.
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5-32.
- Sandkuhl, K., Stirna, J., Persson, A., & Wißotzki, M. (2014). Frameworks and Reference Architectures. *Enterprise Modeling* (pp. 273-289): Springer.
- Schekkerman, J. (2004a). Extended enterprise architecture framework (E2AF) essentials guide. *Institute For Enterprise Architecture Developments*.
- Schekkerman, J. (2004b). *How to survive in the jungle of enterprise architecture frameworks: Creating or choosing an enterprise architecture framework*. Trafford Publishing.

- Schmidt, F. L., & Hunter, J. E. (2014). *Methods of meta-analysis: Correcting error and bias in research findings*. Sage publications.
- Sengupta, A., Mazumdar, C., & Bagchi, A. (2011). A formal methodology for detecting managerial vulnerabilities and threats in an enterprise information system. *Journal of Network and Systems Management*, 19(3), 319-342.
- Seo, D., Lee, H., & Perrig, A. (2013). APFS: adaptive probabilistic filter scheduling against distributed denial-of-service attacks. *Computers & Security*, 39, 366-385.
- Seo, J., Kim, H.-S., Cho, S., & Cha, S. (2004). *Web server attack categorization based on root causes and their locations*. Paper presented at the ITCC 2004. International Conference on Information Technology: Coding and Computing.
- Shaikh, R., Rajput, S., Zaidi, S., & Sharif, K. (2005). *Comparative analysis and design philosophy of next generation unified enterprise application security*. Paper presented at the 2005 IEEE Symposium on Emerging Technologies.
- Shariati, M., Bahmani, F., & Shams, F. (2011). Enterprise information security: A review of architectures and frameworks from interoperability perspective. *Procedia Computer Science*, 3, 537-543.
- Sharma, R. (2006). Security architecture for integration of enterprise information system with J2EE platform. Google Patents.
- She, W., & Thuraisingham, B. (2007). Security for enterprise resource planning systems. *Information systems security*, 16(3), 152-163.
- Shen, Y.-T., Lin, F., & Rohm, C. (2014). A framework for enterprise security architecture and its application in information security incident management. *Communications of the IIMA*, 9(4), 2.
- Sherstobitoff, R., & Itai Liba, M. (2013). Dissecting Operation Troy: Cyberespionage in South Korea. *White Paper developed by McAfee Labs*. from <https://securingtomorrow.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea/>
- Sherwood, J. (1996). SALSA: A method for developing the enterprise security architecture and Strategy. *Computers & Security*, 15(6), 501-506.
- Sherwood, J., Clark, A., & Lynas, D. (1995). Enterprise security architecture. *SABSA White Paper2009*. from <http://www.sabsa.org/sabsa-white-paper>
- Sherwood, N. A. (2005). *Enterprise security architecture: A business-driven approach*. CRC Press.
- Shin, M. E., & Gomaa, H. (2007). Software requirements and architecture modeling for evolving non-secure applications into secure applications. *Science of Computer Programming*, 66(1), 60-70.

- Shin, T., Jung, J., Kim, H., & Lee, S.-W. (2014). Enhanced MAC-based Efficient Message Authentication Scheme over VANET. from https://www.researchgate.net/publication/289042935_Enhanced_MAC-based_efficient_message_authentication_scheme_over_VANET
- Sinn, R. (2007). *Software security technologies*. Cengage Learning.
- Sinnar, S. (2003). Patriotic or unconstitutional? The mandatory detention of aliens under the USA Patriot Act. *Stanford Law Review*, 1419-1456.
- Smith, R. E. (2007). Trends in security product evaluations. *Information Systems Security*, 16(4), 203-216.
- Soltani, S., Seno, S. A. H., Nezhadkamali, M., & Budiarto, R. (2014). A survey on real world botnets and detection mechanisms. *International Journal of Information and Network Security*, 3(2), 116.
- Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE*, 7(3), 363-373.
- Sommestad, T., Ekstedt, M., & Johnson, P. (2008). *Combining defense graphs and enterprise architecture models for security analysis*. Paper presented at the 12th International IEEE Enterprise Distributed Object Computing Conference (EDOC'08)
- Sowa, J. F., & Zachman, J. A. (1992). Extending and formalizing the framework for information systems architecture. *IBM systems journal*, 31(3), 590-616.
- Spewak, S., & Tiemann, M. (2006). Updating the enterprise architecture planning model. *Journal of Enterprise Architecture*, 2(2), 11-19.
- Standardization, I. O. f., & Commission, I. E. (2005). *Information Technology: Security Techniques: Code of Practice for Information Security Management*. ISO/IEC.
- Steel, C., Nagappan, R., & Lai, R. (2005). The alchemy of security design methodology, patterns, and reality checks. *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management*, Prentice Hall, 1088.
- Stevenson, R. J. (1998). *The boiler room and other telephone sales scams*. University of Illinois Press.
- Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. *Economic Review-Federal Reserve Bank of Kansas City*, 5.
- Sweeney, R. (2010). *Achieving service-oriented architecture: Applying an enterprise architecture approach*. John Wiley & Sons.
- Szor, P. (2005). *The art of computer virus research and defense*. Pearson Education.

- Tahajod, M., Iranmehr, A., & Darajeh, M. R. (2009). *A roadmap to develop enterprise security architecture*. Paper presented at the International Conference for Internet Technology and Secured Transactions, 2009 (ICITST 2009).
- Talukder, A. K., & Chaitanya, M. (2008). *Architecting secure software systems*. CRC Press.
- Tarantino, A. (2008). *Governance, risk, and compliance handbook: Technology, finance, environmental, and international guidance and best practices*. John Wiley & Sons.
- Temnenco, V. (2010). UML, RUP, and the Zachman Framework, Better together.
- Tipton, H. F., & Krause, M. (2003). *Information security management handbook*. CRC Press.
- Tive, C. (2006). *419 scam: Exploits of the Nigerian con man*. iUniverse.
- Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, 1-12.
- Urbaczewski, L., & Mrdalj, S. (2006). A comparison of enterprise architecture frameworks. *Issues in Information Systems*, 7(2), 18-23.
- Vachharajani, N., Bridges, M. J., Chang, J., Rangan, R., Ottoni, G., Blome, J. A. August, D. I. (2004). *RIFLE: An architectural framework for user-centric information-flow security*. Paper presented at the 37th International Symposium on Microarchitecture, 2004 (MICRO-37 2004).
- Van't Wout, J., Waage, M., Hartman, H., Stahlecker, M., & Hofman, A. (2010). *The integrated architecture framework explained: Why, what, how*. Springer Science & Business Media.
- van der Beek, W. t. H., Trienekens, J., & Grefen, P. (2012). The Application of Enterprise Reference Architecture in the Financial Industry. *Trends in Enterprise Architecture Research and Practice-Driven Research on Enterprise Transformation* (pp. 93-110): Springer.
- Van Lamsweerde, A. (2004). *Elaborating security requirements by construction of intentional anti-models*. Paper presented at the Proceedings of the 26th International Conference on Software Engineering.
- Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. *Information Management & Computer Security*, 16(4), 415-430.
- Vernadat, F. B. (2007). Interoperable enterprise systems: Principles, concepts, and methods. *Annual Reviews in Control*, 31(1), 137-145.

- Vernadat, F. B. (2010). Technical, semantic and organizational issues of enterprise interoperability and networking. *Annual Reviews in Control*, 34(1), 139-144.
- Viega, J., & McGraw, G. (2001). *Building secure software: How to avoid security problems the right way*. Pearson Education.
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99-104.
- von Wangenheim, C. G., Hauck, J. C. R., Salviano, C. F., & von Wangenheim, A. (2010). *Systematic literature review of software process capability/maturity models*. Paper presented at the international conference on software process improvement and capability determination-spice.
- Walton, J. P. (2002). *Developing an enterprise information security policy*. Paper presented at the Proceedings of the 30th Annual ACM SIGUCCS Conference on User Services.
- Wassermann, R., & Cheng, B. H. (2003). *Security patterns*. Paper presented at the Michigan State University, Pattern Languages of Programs (PLoP) conference (PLoP Conf).
- Weerasinghe, D., Rakocevic, V., & Rajarajan, M. (2012). Security framework for mobile banking *Trustworthy Ubiquitous Computing* (pp. 207-225): Springer.
- Welch, B. (1999). *Electronic banking and treasury security*. Woodhead Publishing.
- Westby, J. R., & Allen, J. H. (2007). Governing for Enterprise Security (GES) Implementation Guide. DTIC Document.
- Williams, T. J., & Li, H. (1999). PERA and GERAM—enterprise reference architectures in enterprise integration *Information Infrastructure Systems for Manufacturing II* (pp. 3-30). Springer.
- Wood, D. L., Pratt, T., Dilger, M. B., Norton, D., & Nadiadi, Y. (2004). Security architecture with environment sensitive credential sufficiency evaluation: Google Patents.
- Wood, P., Egan, G., Haley, K., Tran, T., Cox, O., Lau, H., & Nahorney, B. (2014). Internet security threat report. 2011, 17.
- Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks *Wireless Network Security* (pp. 103-135): Springer.
- Wu, T.-H., & Liu, S.-C. (2009). *A research on the establishment of enterprise information architecture*. Paper presented at the International Conference for Internet Technology and Secured Transactions, 2009. (ICITST 2009).
- Yang, H., Liu, K., & Li, W. (2010). Adaptive requirement-driven architecture for integrated healthcare systems. *Journal of Computers*, 5(2), 186-193.

- Yialelis, N., Lupu, E., & Sloman, M. (1996). *Role-based security for distributed object systems*. Paper presented at the 5th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1996.
- Zachman, J. A. (1996). Concepts of the framework for enterprise architecture. *Los Angeles, CA*.
- Zachman, J. A. (1997). Enterprise architecture: The issue of the century. *Database Programming and Design*, 10(3), 44-53.
- Zachman, J. A. (1999). A framework for information systems architecture. *IBM Systems Journal*, 38(2/3), 454-470.
- Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2046-2069.
- Zelm, M., & Kosanke, K. (2001). *A modelling language for user oriented enterprise modelling*. Paper presented at the 3rd Conference Francophone de Modelisation et SIMulation" Conception, Design, Analysis and Management of Industrial Systems" MOSIM'01.