

INFORMATION SYSTEMS SECURITY MANAGEMENT MATURITY MODEL
FOR ELECTRONIC COMMERCE SMALL MEDIUM INDUSTRIES AND
ENTERPRISES (SMI/E) USING TECHNOLOGY, ORGANIZATION AND
ENVIRONMENT FRAMEWORK

AZAH ANIR BINTI NORMAN

DEPARTMENT OF INFORMATION SYSTEMS
FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2014

INFORMATION SYSTEMS SECURITY MANAGEMENT
MATURITY MODEL FOR ELECTRONIC COMMERCE SMALL
MEDIUM INDUSTRIES AND ENTERPRISES (SMI/E) USING
TECHNOLOGY, ORGANIZATION AND ENVIRONMENT
FRAMEWORK

AZAH ANIR BINTI NORMAN

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

DEPARTMENT OF INFORMATION SYSTEMS
FACULTY OF COMPUTER SCIENCE AND INFORMATION
TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2014

UNIVERSITI MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: (I.C./Passport No.:)
Registration/Matrix No.:
Name of Degree:
Title of Project Paper/Research Report/Dissertation/Thesis (“this Work”):

Field of Study:

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 right 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 subjected 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:

Success in any task can only come from *ALLAH*

...to Abah Hj. Norman Ibrahim and Mama Hjh. Sadiyah Mustajab...your blessings have helped
me through my hard-times

AND

...to my confidante and companion; Abang, you have always inspired me to be strong... I am
blessed and am sincerely thankful to Allah for all the beautiful "gifts", for which I am
indepted to you.

ABSTRACT

Today, the Information Systems Security Management (Information Systems Security Management (ISSM)) maturity framework has been recognized and accepted by businesses globally. This ISSM maturity phenomenon has shifted many business perspectives on the importance of security management towards business information systems. The development of current ISSM maturity framework, based on tried-and-true practices by security experts, have also expanded many issues in the IS research scenario among which are: (i) lack of flexible framework: the current framework developed and designed to suit brick and mortar traditional business, but not for e-commerce that has a volatile structure; (ii) lack of theory supported framework: the current ISSM framework is developed using tried-and-true practices of experts' experiences rather than based on excepted theories.

The main objective of this research is to address these two issues. The research aim is to construct an ISSM maturity model to suit e-commerce using Technology, Organization and Environment framework (Technology-Organization-Environment Framework (TOE)), DeLone and McLean Information System (IS) Success Factors, Diffusion of Innovation Theory (Diffusion of Innovation Theory (DOI)) and Ein-Dor Organizational Factors. The IS theory, IS model, IS framework and IS organization factors were selected to help develop a flexible and theoretically-based ISSM maturity model for the benefit of Small Medium Industries/Enterprises (SMI/Es) that are involved in e-commerce.

This study employs a mixed-method research using the sequential mix-method procedure to predict the conceptual relationship: (i) the research quantitative phase adopts a structural equation modelling (Structural Equation Modelling (SEM)) technique using Partial Least Square

(Partial Least Square (PLS)) method, (ii) semi-structured interviews with the selected Small Medium Industry/Enterprise (SMI/E)s business Chief Executives Officers (Chief Executive Officer (CEO)s) and business owners that are involved in e-commerce. The results show high reliability of predicted variables with minimal reading of reliability score of more than 0.85, displaying average variance extracted (Average Variance Extracted (AVE)) exceeding 0.5, indicating adequate convergent validity of all the predicted variables developed in the conceptual framework. The predicted relationship was proved to be significant with the score of 50.4% showing the high influences of latent variables discussed in this ISSM maturity research.

The findings show three significant influences in ISSM maturity in e-commerce (i) technology which are the technology usage, compatibility, complexity, relative advantage and technology availability, (ii) organization including the human resources, formal and informal linking structures and the communication process and (iii) the environment of which consisted of user satisfaction, government regulations, technology support characteristics, industry characteristics and market structure. Based on both quantitative and qualitative results, four quadrant of ISSM maturity were presented. These quadrants were then organized to construct the ISSM maturity model. The research contributes to the body of knowledge in twofolds: practically and academically whereby (i) the research contributed to the development of theoretically-based ISSM maturity model for SMI/E involved in the e-Commerce, and (ii) the research justified the theoretical consideration (based on the selected IS theory, IS framework, IS model and IS factors) which formed the conceptual research framework of this thesis. This research has successfully answered all research questions where it deduced the ISSM maturity factors and described the relationship between identified factors, hence conclusively build the ISSM maturity model.

ABSTRAK

Hari ini, rangkakerja kematangan Sistem Maklumat Pengurusan Keselamatan (ISSM) telah diiktiraf dan diterima oleh banyak perniagaan pada peringkat global. Fenomena kematangan ISSM telah mengalih banyak perspektif perniagaan tentang kepentingan pengurusan keselamatan terhadap sistem maklumat (IS) perniagaan. Pembangunan rangkakerja kematangan ISSM sedia ada berdasarkan amalan cuba-dan-benar oleh pakar-pakar keselamatan juga telah mengembangkan lebih banyak isu dalam senario penyelidikan IS : (i) kekurangan rangkakerja fleksibel: rangkakerja sedia-bangun direka untuk disesuaikan pada perniagaan tradisional berheirarki tetapi bukan untuk e-dagang yang mempunyai struktur yang tidak menentu; (ii) kekurangan rangkakerja yang disokong teori: rangkakerja ISSM semasa dibangunkan menggunakan amalan cuba-dan-benar penulis tetapi bukannya berdasarkan teori yang diterima. Objektif utama kajian ini adalah untuk menangani kedua-dua isu di atas. Penyelidikan adalah bertujuan untuk membina model ISSM matang untuk memenuhi keperluan industri kecil dan sederhana (SMI/E) yang memiliki e-dagang menggunakan rangkakerja Teknologi, Organisasi dan Alam Sekitar (TOE), DeLone dan McLean Faktor Kejayaan Security Management (SM), Teori Resapan Inovasi (DOI) dan Dor-Ein Faktor Organisasi. Teori-teori ini membantu untuk membangunkan fleksibiliti dalam model ISSM yang berasaskan teori.

Kajian ini menggunakan campuran penyelidikan kuantitatif dan kualitatif dengan menggunakan prosedur kaedah campuran berjujukan untuk meramalkan hubungan konseptual: (i) fasa penyelidikan kuantitatif menggunakan model persamaan struktur (SEM) dengan teknik Separa Least Square (PLS), (ii) semi temu bual berstruktur untuk pemilik perniagaan yang dipilih, yang terlibat dalam e-dagang. Keputusan menunjukkan kebolehpercayaan pembolehubah yang tinggi yang meramalkan bacaan minimum 0.85, memaparkan purata varians diekstrak

(AVE) melebihi 0.5 yang menunjukkan kesahihan pembolehubah mencukupi kepada semua pembolehubah yang diramalkan dalam membangunkan kerangka konseptual. Ramalan hubungan membuktikan tahap pengaruh yang ketara sebanyak 50.4 peratus di mana pembolehubah menunjukkan pengaruh yang tinggi ke arah kematangan ISSM e-dagang.

Dapatan kajian menunjukkan tiga pengaruh penting dalam kematangan ISSM dalam e-dagang (i) teknologi iaitu penggunaan teknologi , keserasian , kerumitan , kelebihan relatif dan ketersediaan teknologi, (ii) organisasi termasuk sumber manusia , struktur hubungan formal dan tidak formal dan proses komunikasi dan (iii) alam sekitar terdiri kepuasan pengguna , peraturan kerajaan, ciri-ciri industri dan struktur pasaran dan ciri-ciri sokongan teknologi. Berasaskan keputusan dari segi kuantitatif dan kualitatif , empat kuadran kematangan ISSM telah diketengahkan . Dengan menggunakan kuadran yang telah diketengahkan, kajian telah menganjurkan satu model kematangan ISSM. Kajian ini menyumbang kepada badan pengetahuan dalam dua lipatan : praktikal dan akademik yang mana (i) penyelidikan telah menyumbang kepada pembangunan model kematangan ISSM yang dibina berasaskan teori untuk kegunaan SMI/E yang terlibat dalam e-perdagangan, (ii) penyelidikan membenarkan pandangan teori (berdasarkan teori IS yang dipilih, rangkakerja IS , model IS dan faktor IS) yang membentuk konsep rangkakerja penyelidikan tesis ini. Kajian ini telah berjaya menjawab semua soalan-soalan penyelidikan di mana ia menyimpulkan faktor kematangan ISSM dan membincangkan hubungan antara faktor-faktor yang telah dikenal pasti, seterusnya membina model kematangan ISSM.

ACKNOWLEDGEMENT

Alhamdulillah. Success in all my task comes only from Allah SWT.

Heartiest thanks to all who have directly and indirectly supported this research. My gratitude goes to Malaysia Productivity Corporation (MPC) and Women Entrepreneur Network (WENA) for invaluable advise and support. To my supervisor, Dr. Norizan Mohd Yasin, thank you for all the comments and critics. Thank you Prof. Ramayah for all the statistical guidance and "wise-quotes", to Prof. Imam Ghozali and Mr. Dwiratmono, for the PLS introduction and guides. This thesis also could not be realized without the help of friends who have shared knowledge, information, tips and wisdom, that which I would not have been able to gather through my readings.

I am also thankful to Along and Adik for your never ending help and support. Sayang Mohd Anuar Mustafa- thank you for believing in me. Ain Zahirah, Afiah Zaheen, Auni Zakiyah and Ahmad Zuhayr- your patience, love, laughers and cries have make this journey more valuable and worthwhile. Subhanallah and Alhamdulillah, I am blessed.

Gratitude also goes to families and friends, for without them I may not be here. Finally to RESTU, only Allah could repay the unconditional support you've provided me.

TABLE OF CONTENTS

ORIGINAL LITERARY WORK DECLARATION	ii
DEDICATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	viii
TABLE OF CONTENTS	ix
LIST OF FIGURES	xiv
LIST OF TABLES	xvi
LIST OF SYMBOLS AND ACRONYMS	xviii
LIST OF APPENDICES	xix
CHAPTER 1: INTRODUCTION	1
1.1 Overview	1
1.2 Context of Research	6
1.3 Overview of Research Problem	6
1.4 Research Objectives	8
1.5 Research Questions	8
1.6 Scope of Research	11
1.7 Research Methodology	12
1.8 Contribution of the Research	13
1.8.1 Academic benefits	13
1.8.2 Practical or applied benefits	14
1.9 Structure of the research	15
CHAPTER 2: LITERATURE REVIEW	18
2.1 Introduction	18
2.2 The Information Systems Security Management (ISSM)	21
2.2.1 The Past ISSM Research Highlights	26
2.2.2 The Present ISSM Research Highlights	28
2.2.2 (a) The characteristics of the standards	30
2.2.2 (b) Socio-technical factors derived from Information Systems Security Management Research	34
2.3 Information systems security management (ISSM) Maturity	39
2.3.1 The Information systems security management ISSM Maturity Standards	40
2.3.1 (a) Software Security Metrics by Murine and Carpenter (1984)	41
	ix

2.3.1 (b) Information Security Management Maturity Grid by Stacey (1996)	42
2.3.1 (c) Systems Security Engineering Capability Maturity Model (SSE-CMM)(Carnegie-Mellon, 1999) or the ISO/IEC21827:2008	44
2.3.1 (d) Information security management maturity model (ISM3) (Aceituno, 2006)	46
2.3.2 Theoretical perspective of Information Systems Security Management (ISSM) Maturity	49
2.3.2 (a) Definition of Attributes in Technology, Organization and Environment	55
2.4 The Study: Malaysia SMI/E with e-commerce	58
2.4.1 Malaysian SMI/E	59
2.4.2 E-commerce scenario in Malaysia	60
2.4.3 The need for ISSM Maturity Model for the Small Businesses	63
2.5 Summary	64
CHAPTER 3: RESEARCH FRAMEWORK	67
3.1 Introduction	67
3.2 The Information Systems Security Management (ISSM) Maturity Conceptual Framework	68
3.2.1 The ISSM Maturity Independent, Mediating and Dependent Factors	69
3.2.1 (a) The ISSM Maturity Independent Factors	69
3.2.1 (b) The ISSM Maturity Mediating Factors	70
3.2.1 (c) The ISSM Maturity Dependent Factor	73
3.2.2 Research Hypotheses	74
3.3 Summary	79
CHAPTER 4: RESEARCH METHODOLOGY	81
4.1 Introduction	81
4.2 Procedural Issues in the Mixed-Methods Sequential Explanatory Design	84
4.2.1 Priority	85
4.2.2 Implementation	85
4.2.3 Integration	86
4.3 Introduction of the research	87
4.4 The Selection of research	87
4.5 The Selected research	88
4.5.1 Organization A	88
4.5.2 Organization B	90
4.5.3 Organization C	92
4.6 Phase One: Quantitative Research Investigations	93
4.6.1 Population and Sample	93
4.6.2 Establishing contacts	95
4.6.3 Research Measurements	97
4.6.3 (a) Development of the quantitative research instrument	97
4.6.3 (b) Measures of elements	98

4.6.3 (c) Validation from expert	99
4.6.4 Pilot test (analysis and improvement)	101
4.6.5 Conducting the actual questionnaire	102
4.7 Qualitative Research Investigations	104
4.7.1 Research procedure	105
4.7.2 Selection of cases and establishing contacts	106
4.7.3 Research measurements	107
4.7.3 (a) Development of interview guide	107
4.7.3 (b) The pilot test	109
4.7.4 Conducting the actual interview	110
4.8 Analysis strategy	112
4.8.1 Visual representation	112
4.8.2 Analytic strategy for research	114
4.8.2 (a) Quantitative analytic strategy: Structural Equation Modelling (SEM) using Partial Least Square (PLS) technique in quantitative data analysis	114
4.8.2 (b) Overview of quantitative analysis	116
4.8.2 (c) Definition of Operational Elements for Quantitative Analysis	118
4.8.2 (d) Qualitative analytic strategy	121
4.9 Conclusion	125
CHAPTER 5: DATA ANALYSIS AND FINDINGS	127
5.1 Introduction	127
5.2 Quantitative Investigation Analysis	128
5.2.1 Model Validation in PLS: Reflective, Formative Model and Structural Model	128
5.2.1 (a) Model Validation- Reflective Measurement Model: Outer Loadings	129
5.2.1 (b) Model Validation- Reflective Measurement Model: Internal Consistency Reliability (Cronbach's Alpha and Composite Reliability)	132
5.2.1 (c) Model Validation- Reflective Measurement Model: Convergent Validity	133
5.2.1 (d) Model Validation- Reflective Measurement Model: Discriminant Validity-Cross Loadings	133
5.2.1 (e) Model Validation- Formative Measurement Model: Indicator Validity	136
5.2.1 (f) Model Validation- Formative Measurement Model: Construct Validity	137
5.2.1 (g) PLS Structural Model	138
5.2.2 Quantitative Results Analysis	143
5.3 Qualitative Investigation Analysis	149
5.3.1 Overview	149
5.3.2 Interview analysis: Section 1 - Technology-related elements	150
5.3.2 (a) Technology Availability, Compatibility and Complexity	150
5.3.2 (b) Technology Characteristics	152
5.3.3 Interview analysis: Section 2 - Organization-related elements	158
5.3.3 (a) Formal and informal linking structures	158

5.3.3 (b) Human resources	161
5.3.3 (c) Utilization: Communication process	162
5.3.3 (d) Slack	163
5.3.4 Interview analysis: Section 3 - Environment-related elements	165
5.3.4 (a) Government regulations	165
5.3.4 (b) Technology support infrastructure	167
5.3.4 (c) Industry characteristics and market structure	168
5.3.4 (d) User influence/satisfaction	169
5.4 Quantitative and Qualitative Analysis Integration and Interpretation	174
5.5 Validity and Reliability of Data	183
5.5.1 Quantitative: Data Validity	183
5.5.1 (a) Quantitative: Content Validity	183
5.5.1 (b) Quantitative: Construct validity	185
5.5.2 Qualitative: Data Validity	186
5.5.2 (a) Credibility	186
5.5.2 (b) Transferability	187
5.5.3 Reliability in Quantitative and Qualitative Data Analysis	187
5.5.3 (a) Reliability in Quantitative Data Analysis	187
5.5.3 (b) Reliability in Qualitative Data Analysis	188
5.6 Conclusion	188
CHAPTER 6: MODEL BUILDING	190
6.1 Introduction	190
6.2 Model Building Process	191
6.2.1 The Model Selection	191
6.2.1 (a) Model deduction	194
6.2.2 The Model Fitting	201
6.2.3 The model validation	203
6.3 Case conclusion and findings	206
6.4 Development of ISSM maturity prototype	211
6.4.1 Business demography	211
6.4.2 Factor interrelation	212
6.4.3 Business Forces or Dynamics	213
6.4.4 ISSM level of practice	214
6.4.5 Prototype technological considerations	216
6.4.6 Prototype design and layout	216
6.4.7 Prototype evaluation	217
6.4.8 Problems and issues	219
6.5 Conclusion	220
CHAPTER 7: DISCUSSION AND CONCLUSION	222
7.1 Overview	222
7.2 Question addressed in this research	225
7.3 Contribution	233
7.4 Implications	234
7.4.1 Theoretical implications	234

7.4.2	Practical implications	236
7.5	Limitation	238
7.5.1	Theoretical limitation	238
7.5.2	Methodological limitation	239
7.6	Future research and recommendations	240
7.7	Summary	241
APPENDICES		242
REFERENCES		319

LIST OF FIGURES

Figure 1.1	Research objectives and questions mapping	12
Figure 1.2	Research process, input and output	14
Figure 1.3	Chapter organization of the research	17
Figure 2.1	Literature review flow	20
Figure 2.2	Information Systems Security Management (ISSM) development waves adopted from Von Solms, 2006	23
Figure 2.3	ISSM Standards Characteristics	33
Figure 2.4	ISSM Success Factors	38
Figure 2.5	Capability level of SSE-CMM by Carnegie Mellon University (1999)	44
Figure 2.6	High-level abstractions from SSE-CMM by Carnegie Mellon University (1999)	46
Figure 2.7	ISSM maturity theoretical model	54
Figure 3.1	Relationship of TOE elements to ISSM Maturity	69
Figure 3.2	Independent factors for ISSM Maturity	71
Figure 3.3	Mediating factors for ISSM Maturity	72
Figure 3.4	Dependent factors for ISSM Maturity	73
Figure 3.5	Independent and mediating factors for ISSM Maturity	74
Figure 3.6	Research Conceptual Framework for ISSM Maturity	79
Figure 4.1	ISSM maturity research method	83
Figure 4.2	Interview Protocol- Demographics Questions	108
Figure 4.3	Interview Protocol	110
Figure 4.4	Visual representation of the ISSM Maturity Research	113
Figure 4.5	Independent construct	117
Figure 4.6	Technology Construct (Communication structure elements)	118
Figure 4.7	Organization Constructs (Purpose, Usage and Utilization elements)	118
Figure 4.8	Environment constructs (Support and Stimuli elements)	119
Figure 4.9	ISSM maturity dependent construct	119
Figure 4.10	ISSM Maturity conceptual relationship model in SmartPLS	122
Figure 4.11	Data reduction process	123
Figure 4.12	Qualitative analysis data display	124
Figure 4.13	Qualitative analysis table representations	125
Figure 5.1	Analysis paths to formulate ISSM Maturity Framework	127
Figure 5.2	Independent Factors and Variables Loading	130
Figure 5.3	Technology, Organization and Environment (TOE) Factors and Variables Loading	131
Figure 5.4	Dependent Factor and Variables Loading	131

Figure 5.5	The Variance Inflation Factor (VIF) assessment for Indicator validity	136
Figure 5.6	The Outer Weight Results for Construct Validity	137
Figure 5.7	The ISSM maturity result from the quantitative analysis	143
Figure 5.8	ISSM maturity factors derived from mix-method analysis	175
Figure 6.1	Model Building Process	191
Figure 6.2	Four quadrant of ISSM model	193
Figure 6.3	Independent circles of TOE in the Novice level	195
Figure 6.4	TOE factors interrelation and forces in the Intermediate Level	196
Figure 6.5	Overlapping circles of ISSM dynamics of Advance level of ISSM	197
Figure 6.6	Matured ISSM quadrant	199
Figure 6.7	Four-quadrant model of ISSM maturity	200
Figure 6.8	ISSM maturity model	201
Figure 6.9	ISSM maturity in intermediate maturity stage	208
Figure 6.10	ISSM maturity in advanced maturity stage	209
Figure 6.11	ISSM maturity in matured stage	209
Figure 6.12	ISSM Prototype: Business Demography	212
Figure 6.13	ISSM Prototype: Factor inter-relation	213
Figure 6.14	ISSM Prototype: Forces/dynamics	214
Figure 6.15	ISSM Prototype: ISSM Security Practices	215
Figure 6.16	ISSM Prototype: Result page	217
Figure 7.1	ISSM maturity model based on TOE	233

LIST OF TABLES

Table 2.1	Summary of Information Systems Security Management (ISSM) development waves	25
Table 2.2	Standards for information Security Management	32
Table 2.3	Software Security Metrics Milestone by Murine and Carpenter (1984)	41
Table 2.4	Software Security Metrics Criteria Definition by Murine and Carpenter (1984)	42
Table 2.5	Maturity stages in Information security management maturity grid by Stacey (1996)	43
Table 2.6	ISM3 Maturity Capability Definitions by Aceituno (2006)	47
Table 2.7	ISM3 Maturity Level by Aceituno (2006)	48
Table 2.8	Relationship of elements with the IS theory	52
Table 2.9	Definition of Attributes in Technology, Organization and Environment	55
Table 2.10	ISSM Issues of Importance	57
Table 4.1	Sample size and unit of analysis	94
Table 4.2	Research Investigation 1: Quantitative Investigation	95
Table 4.3	Experts and Reviewer Background involved in Content Validation	100
Table 4.4	Sample size and unit of analysis	103
Table 4.5	Research Investigation 2: Qualitative Investigation	105
Table 4.6	Rules to Drawing Visual Models for Mixed-Methods Designs adopted from Ivankova et. al., 2006	114
Table 5.1	Composite Reliability and Cronbach's Alpha for ISSM maturity factors	132
Table 5.2	Average Variance Extracted (AVE) for ISSM maturity factors	133
Table 5.3	Latent Variable Correlations	134
Table 5.4	Reflective Model Validation Results	135
Table 5.5	Formative Model Validation Results	138
Table 5.6	R ² Value for ISSM Maturity in SMI/E e-Commerce Malaysia	139
Table 5.7	Result of Hypothesis	141
Table 5.8	Hypothesis decision	142
Table 5.9	Technology related elements of qualitative analysis	157
Table 5.10	Organization related elements of qualitative analysis	164
Table 5.11	Environment related elements of qualitative analysis	170
Table 5.12	Factor Inter-relationship from Qualitative Findings	173
Table 5.13	Forces associated to TOE factors observed from the Qualitative Findings	174
Table 5.14	Business forces associated to TOE inter-relation observed from the Qualitative Findings	178
Table 5.15	Seven cases business demography	179
Table 5.16	Business forces and dynamics identified issues	179
Table 5.17	Factor inter-relation identified issues	180

Table 5.18	Percentage of Maturity in seven selected SMI/E	181
Table 5.19	Percentage of Maturity in fourteen selected SMI/E	181
Table 5.20	Fourteen cases business demography	182
Table 6.1	Expert Validation Result on Factor Inter-relation and forces/dynamics	206
Table 6.2	Prototype evaluation results	218
Table 6.3	Prototype evaluation conclusion	220
Table B.1	Independent constructs and indicators	257
Table B.2	Mediator constructs and indicators	257
Table B.3	Dependent constructs and indicators	263
Table C.1	Outer Loading Score for Variables involved in the ISSM Maturity	267
Table C.2	Cross Loading Score for Variables involved in the ISSM Maturity	269

LIST OF SYMBOLS AND ACRONYMS

APAC	Asia Pacific.
ASEAN	Association of Southeast Asian Nations.
AVE	Average Variance Extracted.
BNM	Bank Negara Malaysia.
BS	British Standard.
CC	Common Criteria.
CEO	Chief Executive Officer.
CMM	Capability Maturity Model.
CS	computer security.
CVR	Content validity ratio.
DOI	Diffusion of Innovation Theory.
EFA	Exploratory Factor Analysis.
GAISP	Generally Accepted Information Security Principles.
GLC	Government Link Companies.
IS	Information System.
ISM3	Information security management maturity model.
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission.
ISSA	Information Systems Security Association.
ISSM	Information Systems Security Management.
IT	Information Technology.
MCMC	Malaysia Communication Multimedia Commission.
MIS	Management Information Systems.
MITI	Ministry of International Trade and Industry.
MoA	Memorandum of Agreement.
MoU	Memorandum of Understanding.
NGO	Non-profit organization.
PLS	Partial Least Square.
ROI	Return of Investment.
SEM	Structural Equation Modelling.
SM	Security Management.
SMI/E	Small Medium Industry/Enterprise.
SMI/Es	Small Medium Industries/Enterprises.
SSE-CMM	Systems Security Engineering Capability Maturity Model.
SSM	Software Security Metrics.
TOE	Technology-Organization-Environment Framework.

LIST OF APPENDICES

Appendix A	Survey Instrument	243
Appendix B	Operational Variables and Indicators	257
Appendix C	Quantitative Data Analysis Results Using Partial Least Square (PLS)	267
Appendix D	Qualitative Analysis Table	272
Appendix E	Prototype Manual	306
Appendix F	ISSM Validation and Evaluation Form with Experts	314

CHAPTER 1

INTRODUCTION

1.1 Overview

Information system (IS) security is defined as an expansive view of the computer security (computer security (CS)) term; whereby IS security incorporates system analysis and design method, manual information systems, managerial issues and both societal and ethical problems (Baskerville, 1988). IS security involves holistic security implementation. However, exercising IS security can be demanding and exhaustive, if there is no clear procedures. The information systems security management (ISSM) procedure was created to address these issues, thus provide a foundation for the business to conduct security practices effectively. Many standards and best practices were produced to help realize business desires towards security implementation. As such, ISSM has become an indispensable issue in businesses today. An effective ISSM should provide procedures or requirements for a business to manage its IS towards an acceptable risk (Abu-Musa, 2010). Often, the business security rule is operationalized using the ISSM function deployed by the business. As for example for controlling assets towards business information system, business deployed user access control.

The ISSM requirement heightens as many businesses highly depend on the IS to conduct and support business processes (Torres, Sarriegi, Santos, & Serrano, 2006). The increase of Internet dependency has increasingly changed the way a business conducts its processes (Nasir & Ponnusamy, 2007; Kaynak, Tatoglu, & Kula, 2005; Furnell & Karweni, 1999), hence this intensifies the tendency to ensure higher security practices that accompany (Zuccato, 2007) a

business. This is because the Internet is vulnerable and is exposed to a variety of security risk and threats.

In this research, electronic commerce is interchangeably used with e-commerce. Electronic commerce is one very notable online commerce process that has since benefited from the Internet's development. This is a form of business process evolution which involves high IS elements. E-commerce created a new dimension of selling and buying without geographical boundaries in 24X7 time frames. It has increased business productivity and efficiency, and as such, has become an alternative revenue generator of a business (Wirtz, Piehler, & Ullrich, 2013; Mora & Barnes, 2011; Kaynak et al., 2005; Furnell & Karweni, 1999). Through e-commerce, businesses, particularly the small businesses, such as the small and medium industries and enterprises (SMI/E), could manipulate the Internet's remarkable features to reach customers globally and promote business using minimal resources (Ramdani, Chevers, & Williams, 2013; Kartiwi & MacGregor, 2007; Taylor & Murphy, 2004). However, as already mentioned, the Internet does not promise 100% secure connectivity. This is because the Internet was designed with the main objective to enable data to be communicated transparently across multiple, linked packet networks (Cerf, 2001). Data are transmitted freely and insecurely over the network. Therefore, the Internet has attracted many hackers and abusers attempting to steal and manipulate available information via the network (Siponen, 2002a). Due to this situation, businesses that are involved in e-commerce are highly advised and required to apply and practice ISSM to ensure business safety.

Many businesses implement ISSM according to current standards and best practices. There is a variety of ISSM standards that oversee the IS security practices of a business, for example

the ISO/IEC 27001:2005. However, current standards are lengthy and very much appropriated towards certain businesses, e.g., the traditional business compared to e-commerce business (Zuccato, 2007; Siponen, 2006). Typically, SMI/E are very much concerned with security management, especially in Information Technology (IT) (Hsu, Lee, & Straub, 2012; Tan, Chong, Lin, & Eze, 2009). The service providers and vendors apply IS security practice towards these SMI/E as an effort to secure the business, by using common security practices (Tan et al., 2009). Business is consisted of its own characteristics, as such a flexible and simple security management support and practice which are very much needed by this business. Unless this is implemented, the business will be in a dangerous state due to the inappropriate security management conducted by a business.

The ISSM maturity framework can be used to assess current IS security practices of a business, consistent with the current standard requirements. Besides, the ISSM maturity standard is used to implement and practice effective ISSM. The Information Systems Security Management (ISSM) maturity is defined as a concept which is an alternative IS security practice in the SMI/E to ensure effective IS practices. It is an administrative innovation (Hsu et al., 2012) to help a particular business apply security management effectively, hence determines the business maturity in its security management effort. The importance of ISSM maturity is that it reflects the business security management adoption of a business. ISSM maturity is able to help a business identify the business maturity level in their IS security practices, and as such defines the level of security measures implemented and practiced, hence accentuating the successful practices of a business. Based on the ISSM maturity framework, SMI/E could move towards appropriate and leverage the ISSM maturity concept and leverage onto effective IS security practice in the business (Zuccato, 2007). Besides determining the IS practice level, the

maturity concept can forecast the IS security improvement for overall business improvement.

However, the current ISSM maturity framework addresses security management maturity most commonly practiced in the computer security field. There is limited open literatures on the ISSM maturity especially in the context of SMI/E e-commerce. The majority of the maturity standards are based on the computer science field, where requirements are specifically addressed on the computer science subject matter. As mentioned earlier, all businesses including the SMI/E, consist of unique characteristics, hence requires different attention to its own ISSM practices.

Besides, the current ISSM maturity frameworks were created based on practical foundations owned by the practitioners, which means that the design of the model and framework were based on experts knowledge and experience in the security management field. For example, the model and framework such as the Information Security Program Maturity Grid (Stacey, 1996), Software security Metrics (Murine and Carpenter, 1984) and the Information Security Management Maturity Model (Aceituno, 2006). The current ISSM discussion lacks theoretical-based literature, making it less accessible by scholars in the field (Siponen, Willison, & Baskerville, 2008). Using a combination of theory, model, framework and IS factors in this research which are: (i) the Diffusion of Innovation Theory (DOI) by Rogers (1995), (ii) the IS Success Model by DeLone and McLean (1992, 2003), (iii) the Technology, Organization and Environment Framework (TOE) by Tornatzky, Fleischer, and Chakrabarti (1990) and the (iv) Ein-Dor management information systems success factors (Ein-Dor & Segev, 1978). This research will provide a research theoretical-lens towards understanding the main influences of ISSM maturity on SMI/Es conducting e-commerce.

Reflecting on the advantages available in the ISSM maturity concept has, this concept is considered as a suitable approach to tackle and improve IS practices in the SMI/Es that are involved with e-commerce. This is because the ISSM maturity concept provides a flexible yet dynamic approach towards effective ISSM in a business.

This research is carried out to identify and discuss the possible factors influencing ISSM maturity in the SMI/E which conduct e-commerce. As IS security encompasses technology, organization and environment related issues (Monfelt, Pilemalm, Hallberg, & Yngström, 2011; Kraemer, Carayon, & Clem, 2009; Chang & Ho, 2006; Kankanhalli, Teo, Tan, & Wei, 2003), the same issues should persist in the ISSM maturity. An indepth research is embarked upon to determine the possible influential factors under these three subjects. Using the sequential mixed method, this research examines technology, organization and environment issues governing ISSM maturity of SMI/E involved in e-commerce. This research then evaluates the relationship between technology, organization and environment-associated factors to identify the underlying phenomena of the ISSM maturity, in the context of the SMI/E which are involved in e-commerce. This research will explicitly explore the internal and external surroundings of the SMI/E which influence and contribute to the ISSM Maturity Model of SMI/E with e-commerce in Malaysia.

The intention of the research is to contribute to the body of knowledge related to the design and development of the ISSM Maturity Model for e-commerce in relation to the SMI/E context.

1.2 Context of Research

The context of the research seeks to understand the contribution of the socio-technical components and practices involved in attaining ISSM maturity in the SMI/Es that are involved with e-commerce in Malaysia. The fundamentals of social and technical dynamics in the contribution to ISSM maturity of a business depends particularly on the business set-up. As such, it is important to identify the socio-technical factors influencing the SMI/E set-up to enable this business to practice IS security, thus attain ISSM maturity. As e-commerce has transformed many SMI/E business processes, these businesses are challenged with the required socio-technical elements to support business in reaching ISSM maturity. Due to minimal research which has discussed SMI/E and its ISSM maturity effort, this research strives to understand the underlying phenomena of this context.

1.3 Overview of Research Problem

The IS security discipline addresses the concern of protecting information assets through technical security mechanisms and information quality promotion encompassing the people, process and technology attributes (Baskerville, 1988; Chang & Ho, 2006; Dhillon & Backhouse, 2001; Kankanhalli et al., 2003; Zuccato, 2007). As for the Information Systems Security Management (ISSM), it addresses concerns on security governance of an organization (Da Veiga & Eloff, 2007; von Solms, 2006). The ISSM field defines ways to realize the security management concepts through a variety of techniques, thus ensuring these techniques are at the operational level (Baskerville & Myers, 2009; M. Eloff & Von Solms, 2000a). As many businesses have advanced in accordance to the progress of current technology, the ISSM Maturity concept was used to assess the level of ISSM of a business. The same ISSM maturity concept has also been adopted as a technique to implement effective ISSM in a business (Zuccato, 2007). There are

many issues in ensuring appropriate and effective ISSM of a business, particularly due to the unique structure of each business possesses (Monfelt et al., 2011; Tryfonas, Kiountouzis, & Poulymenakou, 2001; Yildirim, Akalp, Aytac, & Bayram, 2011).

There is very limited discussions on ISSM maturity in the chosen business context of this research. In current studies, there is much available literature addressing the technology, organization and environment issues in ISSM. Unfortunately, this literature is mostly centered on big organizations with already stable business structure, e.g., the traditional businesses with clear hierarchical business structure (Monfelt et al., 2011; Tsohou, Kokolakis, Lambrinouidakis, & Gritzalis, 2010). While discussion refers to SMI/E, which have a volatile business nature, the current literature is not applicable to address similar security management issues appropriately. Much of the current literature addresses the adoption and need of security standards by SMI/E (Yildirim et al., 2011; Gillies, 2011). However in terms of ISSM maturity, few literature is available to support and assist the SMI/Es. This is especially true when discussion is oriented on developing countries, Malaysia for example. The world Internet statistic report in 2012 shows that Malaysia is ranked at the tenth position among Asian countries with Internet users, amounting to 17.7 million users (Stats, 2012). Whilst a high number of Internet users is reported, there are also high Internet consumers in the Malaysian market. With the high number of Internet users in Malaysia, SMI/Es are exposed to high security risk and threats. Hence, the ISSM of SMI/E involved in e-commerce must be taken seriously. SMI/Es could enhance their security management exercise through the ISSM maturity concept and framework as these are an alternative IS security practice in the current business security practice.

This research is conducted to research ISSM maturity in SMI/E businesses that has deployed

e-commerce as part of their business process, especially in Malaysia. The main research problem this research addresses is:

What are the core elements needed to be addressed, managed and structured in order to achieve information systems security management (ISSM) maturity for effective IS security practices in SMI/E in Malaysia involved with e-commerce?

The research problem above has become the main motivation for this research. Through this research we will provide appropriate solutions and useful recommendations to the CEO and business owners, of chosen business context, to structure their business strategy for effective IS security practices, and thus achieve ISSM maturity.

1.4 Research Objectives

The objectives of the research are to:

- 1) Identify and determine factors governing ISSM maturity in SMI/Es in e-commerce.
- 2) Evaluate the relationships between the ISSM maturity factors.
- 3) Design and develop a ISSM Maturity Model to guide and assist the SMI/Es to develop and deploy ISSM, and successively attain ISSM maturity in e-commerce.

1.5 Research Questions

The current literature in security management addresses the importance of defining factors towards effective ISSM (Yeo, Rahim, & Miri, 2007; Caralli, Stevens, Willke, & Wilson, 2004; Torres et al., 2006; Wood, 1987). Through the literature analysis, the technology, organization and environment (TOE) framework has shown seven possible factors that have influenced

the ISSM maturity of a business. These factors include technology availability (Tsohou et al., 2010), organization processes (Yildirim et al., 2011), human resources (Da Veiga & Eloff, 2010, 2007) and organization formal and informal linking structure in terms of business policies (Ozkan & Karabacak, 2010; Barlette & Fomin, 2008; Baskerville & Myers, 2002). As for environment related factors, the industry's characteristics (Werlinger, Hawkey, & Beznosov, 2009), technology infrastructure support (Kraemer et al., 2009) and government regulations (Farn, Lin, & Fung, 2004) become the basis for a business to achieve ISSM maturity. Under the diffusion of innovation theory (DOI), technology compatibility (Fomin & Vries, 2008; Hu, Hart, & Cooke, 2007), complexity (Werlinger et al., 2009) and relative advantage (Al-Awadi & Saidani, 2010; Kankanhalli et al., 2003) become the crucial factors leading to ISSM maturity. Finally, under the Delone and McLean IS Success Model, research defines technology usage (Werlinger et al., 2009) and user satisfaction (Ozkan & Karabacak, 2010) as a common influence towards ISSM maturity achievement. Using the theories, model, framework and IS success factors mentioned in subchapter 1.0, these theories become the fundamentals of the research. It provide the theoretical lens in order to understand the underlying phenomena of ISSM maturity.

IS security practices in a business have become an important task to ensure security of a business. The current available literature shows a small number of ISSM discussions, specifically in the context of SMI/E involved with e-commerce. There is a need to research the ISSM underlying phenomena to discover what influences IS security practice in these businesses. Hence, appropriate measures to assist these businesses to have matured IS security practices could be achieved. The current literature finds that the most important ISSM influencing factors are based on the elements of technology, organization and environment (Monfelt et al., 2011; Kraemer et al., 2009; Chang & Ho, 2006; Kankanhalli et al., 2003). It is essential to understand the

associated factors in the three identified elements to gear businesses towards achieving ISSM maturity for the businesses benefits.

The first research question seeks to investigate and discuss current ISSM practices in the context of SMI/Es with e-commerce in Malaysia. The technology, organization and environment associated factors are analysed, first through the available literature. It is then followed by a quantitative research investigation using a survey. The data collected using the survey method will help determine important factors related to SMI/Es, which were first derived from literature analysis. The same data from the quantitative investigation will be used to assess the second research question.

As such, based on the issues discussed above, there is the need for this research to understand research questions discussed below:

RQ1) What are the factors that influence the SMI/Es in e-commerce to reach ISSM maturity? ISSM is a holistic approach in securing business. It is also important to understand the relationship of the factors and the effect of these relationships towards achieving successful ISSM (Werlinger et al., 2009; Chang & Ho, 2006; Kankanhalli et al., 2003), where business could reach its ISSM maturity through holistic IS security practices. As the context of research defines specific organization characteristics, Ein-Dor and Segev (1978) define the importance of organization factors including business type, business size and top management support in foreseeing the success of any IS management. Specifically in IS security practices, Kankanhalli et al. (2003), Chang and Ho (2006) and Yildirim et al. (2011) show in their research findings the importance of organization factors as influencers in ISSM effort.

The technology, organization and environment factors will not contribute to ISSM maturity of a business if they are not leveraged and holistically interconnected with each other. The most common example is the technology availability in an organization with market support.

A business will not achieve effective technology usage if there is no continuity between these elements. The technology usage, organization and environment relationship and adaption involved in a business justify the respective maturity level owned by a business. Hence, the second research question seeks to understand the ISSM maturity of SMI/Es by assessing the relationship of the determined factors. These relationships will suggest how a business should apply the resources available to attain the required ISSM maturity. The second research question addresses the following:

RQ2) What are the underlying relationships of the factors in stimulating ISSM maturity in SMI/E involved with e-commerce?

The third and final research question seeks to find how the first and second research questions are associated. Through the analysis of the first research question with the second qualitative data results, the research should be able to develop a proposed ISSM Maturity Model in order to assist the deployment of ISSM in the SMI/E businesses in Malaysia. Hence, the third research question is:

RQ3) How has the factors and factors relationship helped in designing the ISSM Maturity Model?

The linkage of research objectives and research questions are referred to in Figure 1.1.

1.6 Scope of Research

This research focuses on the Small Medium Industries and Enterprises (SMI/Es). The selected SMI/Es must also have e-commerce in their business process. Besides practising e-commerce, the selected businesses have to also implement at least minimal security practices to support their businesses, especially in terms of securing their online transactions. The unit of analysis is the business owner or CEO of the company, because in most small businesses, owners and

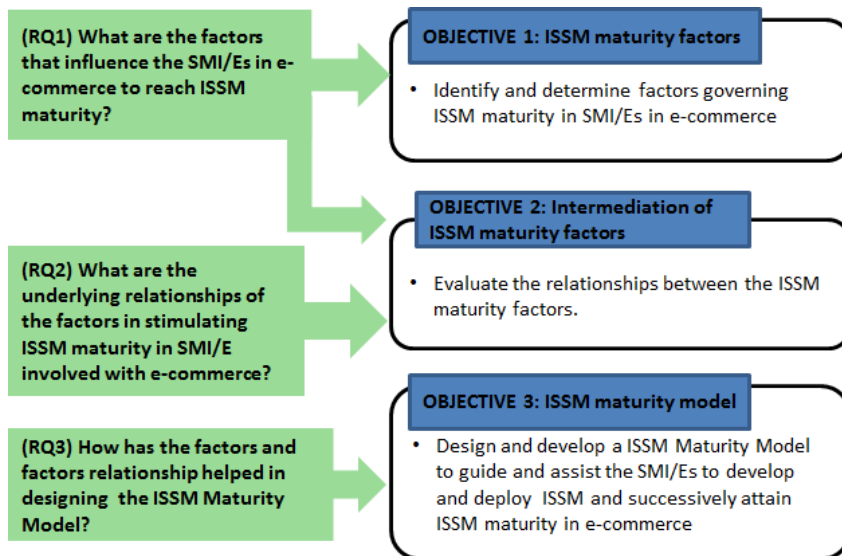


Figure 1.1: Research objectives and questions mapping

CEOs are the persons who champion and foresee business processes and policies of the company. CEOs are the best point of contact as this research involved small SMI/E. As such they are the best entity to provide in-depth information for the research to understand the underlying phenomena of ISSM maturity in SMI/E involved with e-commerce.

1.7 Research Methodology

This research sets out by defining the research problems, context and the underlying phenomena of the chosen context. Through literature analysis, the research problem was identified. Successively, a research strategy was defined to research the defined problem, thus deriving an appropriate solution. Following this, the research objectives and research questions were derived to address the research problems, and thus understand the underlying phenomena. A sequential mixed method is chosen as the research strategy, to fulfill the objectives of the research.

The first data collection involved quantitative data collection and analysis, where a survey was

conducted. Through the survey, the research tries to identify and verify the ISSM maturity factors. A SEM via PLS technique, which is the second generation of statistical analysis, was conducted to comprehend the factors relationship illustrated in the proposed framework. Using the first research findings, the researcher then carried out a qualitative research investigation and analysis. The sequential qualitative investigation was carried out to gather in-depth information and experience of the business owners in their task of practicing IS security to achieve ISSM maturity. The combination of first and second findings was then used to design and develop the ISSM maturity model for the purpose of SMI/E involved with e-commerce. Figure 1.2 depicts the research process, input and output expected from this research.

1.8 Contribution of the Research

The benefits of the research are observed in twofolds. The first benefit is in the academic field and the second is referring to the practical or applied benefits towards the business in the defined scope of the research. Nevertheless, the research also sees the possibility of providing benefits towards other business types as it can become a source of reference for other businesses.

1.8.1 Academic benefits

The academic benefits expected through this research are the knowledge contributions the research add to the IS security management study. Firstly, the researcher discussed the ISSM maturity phenomena in selected business context according to the selected IS theory, framework and model. Findings through the discussion determined socio-technical factors consisting of TOE involved in the SMI/Es to achieve ISSM maturity. Secondly, the research identified the TOE factors relationship and business forces/dynamics which influenced the SMI/Es in im-

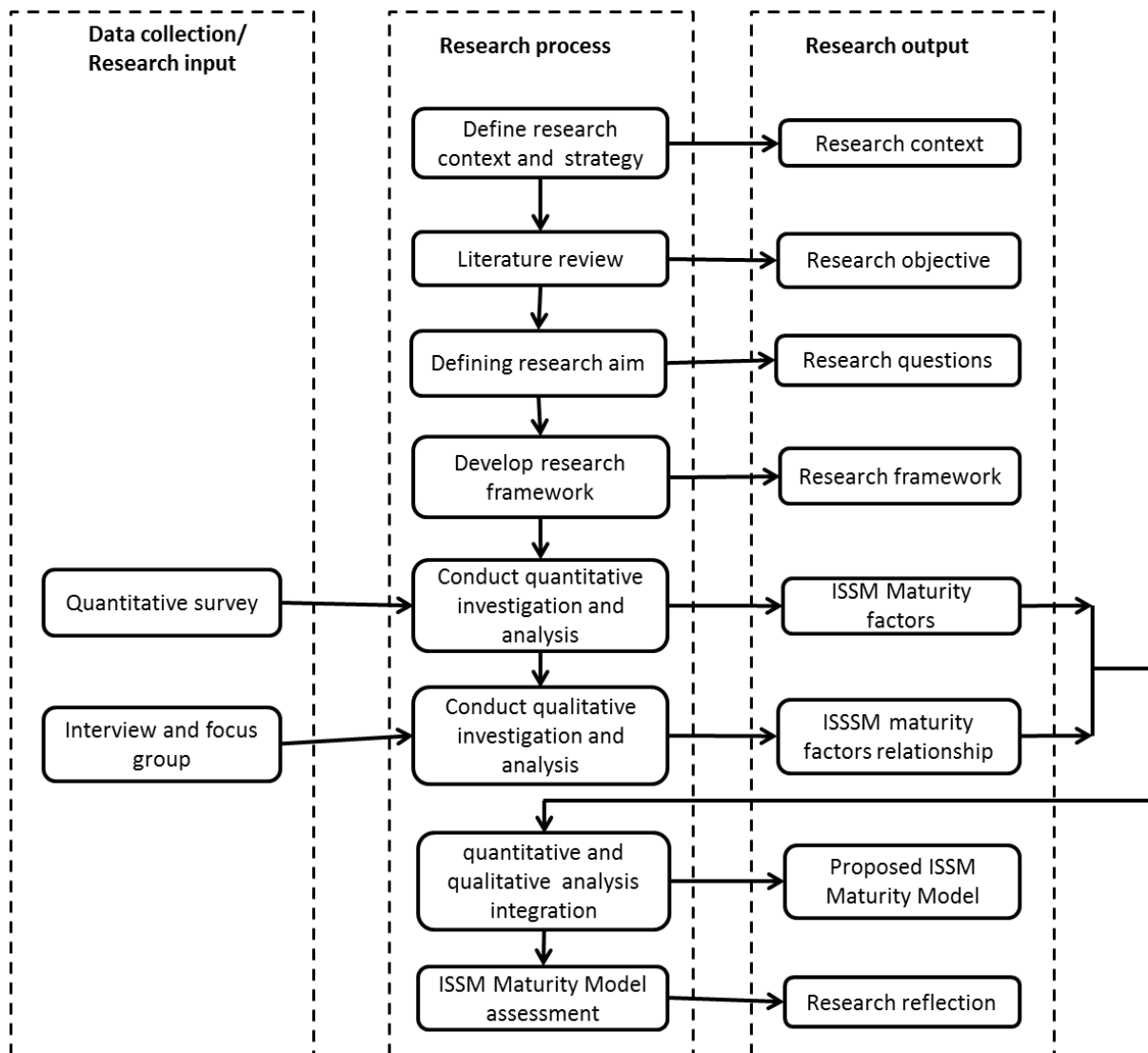


Figure 1.2: Research process, input and output

proving their current ISSM maturity.

1.8.2 Practical or applied benefits

This research will be beneficial to the SMI/Es especially those that are involved in e-commerce. Nonetheless, the outcome of this research also contributes to the other business types in a different manner. For example, the discussion of this research can be a source of reference or assistance for other businesses to exercise ISSM maturity in their particular fields. The ex-

pected benefits directly referred to the research are:

- a) Provide a proposed ISSMs Maturity Model to guide SMI/E when adopting IS security practices based on the identified factors, and their relationships;
- b) Establish as one of the source of reference for SMI/E that are being planned to use the practise of IS security and simultaneously achieve ISSM maturity in their e-commerce practice.

1.9 Structure of the research

Chapter 1 provides the general overview on the research conducted . The definition of the research objectives, scope and research questions are presented to address the issue of the research. The data collections and analysis method are briefly presented providing the intended research outcomes and contribution. This chapter also provides the background of the overall research process, motivation and basis of this research.

The literature findings are in Chapter 2. Thus helps to define the research objectives, scope and research questions to address the phenomena of the research. It acts as the foundation of the research. This literature review started off with a review on ISSM, the security management maturity and its benefits, and the importance of ISSM maturity in SMI/Es involved with e-commerce. Finally the literature review ends with a discussion on the developed research framework, which was initiated based on the reviewed topics mentioned earlier.

Chapter 3 is the research methodology. A sequential mixed method research is used to conduct the data collection and analysis. The research background is discussed and the intended protocol used to carry out the research is presented in this chapter. The strategy to carry out the analysis is also discussed in this chapter. This chapter highlights the processes and procedures involved in the research investigation.

In Chapter 4 the cases involved in this research are presented. The involved organizations are

three important organizations which are directly involved in SMI/Es productivity and development. Here, details on the organizations involved are discussed and the rationale of choosing the case studies are presented. The contributions of selected organizations are discussed in this chapter.

Chapter 5 presents the data analysis and findings. Discussion on the quantitative and qualitative analysis is conducted in this chapter. Results and findings are highlighted. This chapter also puts forward the validity and reliability of data collection and procedures.

Chapter 6 is the discussions focused on the building of the ISSM maturity model. This chapter concentrates on the schematic way of the model design and steps associated in model-building. The model-building process relates to the data interpretation from the previous chapter.

Chapter 7 is the summary of the whole research. It discusses how issues are investigated in accordance to the theory selected. The findings and solutions are discussed and concluded in this chapter.

Figure 1.3 depicts the chapter organization of this research.

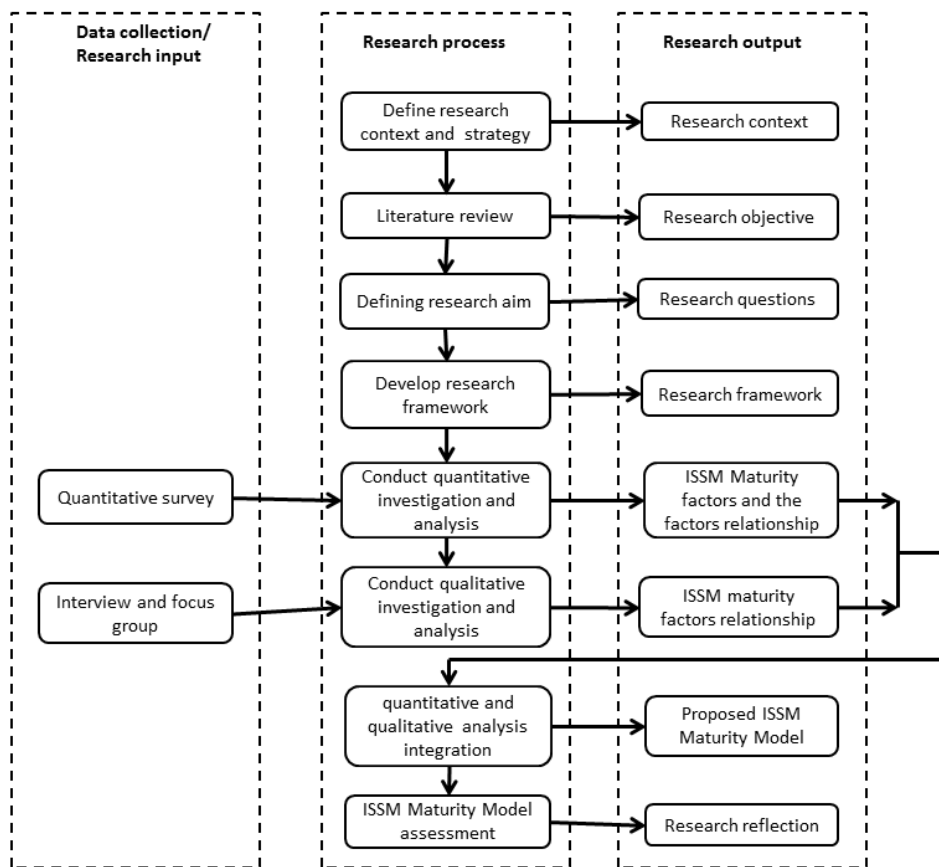


Figure 1.3: Chapter organization of the research

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The objective of this review is to identify characteristics that embody ISSM maturity in SMI/E conducting e-commerce. The literature review begins with the ISSM perspective. Using the ISSM maturity perspective by von Solms (2006), the researcher highlight the research focus involved in each ISSM wave which was incorporated in the ISSM perspective discussed. Continuing the preceding discussion on the research focus earlier, emphasis was also given to compare the past ISSM issues and current ISSM features. As a result of the ISSM perspective discussion, the ISSM characteristics were then identified.

The researcher compares and contrasts the identified ISSM characteristics with the current ISSM maturity literature to develop an understanding on the current problem in ISSM maturity. In the ISSM maturity reviews, two significant types of businesses were determined, which are the traditional business, or also known as hierarchical organization, and the emergent organization such as the SMI/Es. The traditional businesses are businesses that have strong business hierarchy and have been in the scene for a long time, such as huge corporations. As for the emergent organizations, these are businesses that practice flat organization structure, usually with a small number of resources e.g. the SMI/Es. Literature reviews highlight problems on ISSM maturity in SMI/Es as both business types exhibit different business issues, characteristics and position in their IS security practices. The researcher then highlights the importance and advantages of ISSM maturity in the SMI/E. Current literature highlights ISSM maturity

issues available in the hierarchical business. However, a few discussions have been found to address the SMI/E problem in their ISSM maturity exercise. Due to this, this research is conducted to focus on the SMI/Es which are involved in e-commerce to combat their problems and issues in ISSM maturity.

In the following literature analysis, there are many articles iterating the importance of technology, organization and environment TOE, including a recent paper by Hsu et al. (2012). In the IS field, there is no specific IS security theory to associate socio-technical with security context, hence being used as the theoretical ground for this research. Socio-technical issues are important because the value it provides towards a business (Mumford, 2000). The socio-technical concept was a concept discussed in 1949 as a result of the post-war reconstruction of industry. In the discussion, organization was approached as a social system. The discussion then continued with the discussion of technology elements due to the diffusion of innovation within the organization, hence it became an important field of enquiry in any research involving organization (Trist, 1981). In the socio-technical design and development, equal weight should be given to the social and technical factors, because it improved the quality of working life (Mumford, 2000, 1994). In addition to above discussions, Checkland (2000) argues that in the real-world system study (e.g. the SMI/E) it is important to relate the human situation with purposeful activity, where addressed issues must not only include the obvious but the problematic situations consisting of a real world-view. Hence, this research used the same concept to understand the ISSM maturity through the socio-technical elements. It involved different human situations (in different SMI/E businesses) to address businesses problematic situations in achieving ISSM maturity. Selected IS theory, framework and model were used in assisting the researcher to understand the socio-technical factors that influenced the ISSM maturity in

the SMI/E context. The IS theories also become the research lens of this research, providing support in building the research framework. Owing to this condition, the IS theories, model and framework chosen include (i) the DOI by Rogers (1995), (ii) IS Success Model by DeLone and McLean (2003, 1992), (iii) TOE by Tornatzky et al. (1990) and the (iv) MIS organization factors by Ein-Dor and Segev (1978).

Apart from the theories, model and framework above, the literature also highlighted the importance of organizational factors (Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) and business length (Prananto, McKay, & Marshall, 2003a) as part of management maturity influence. On this basis, the researcher then develops a research framework to research the ISSM maturity factors and the association of these factors in realizing ISSM maturity. The literature review covers the following scope as depicted in Figure 2.1.

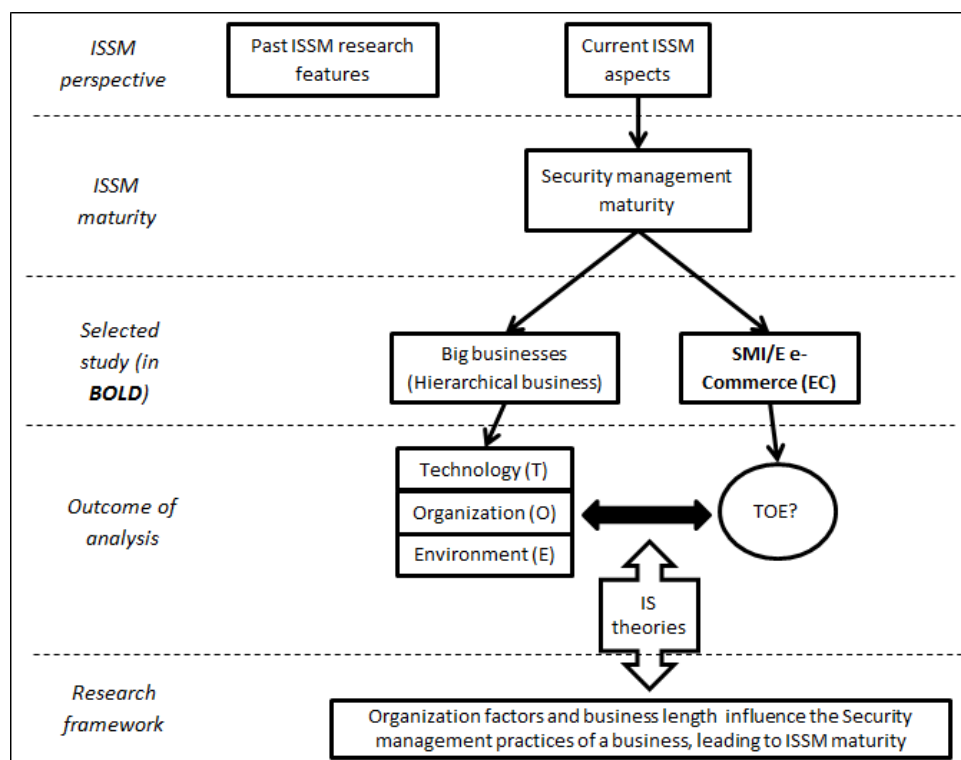


Figure 2.1: Literature review flow

2.2 The Information Systems Security Management (ISSM)

In the previous research carried out by Brancheau and Wetherbe (1987) on the key issues of IS management, the security issue was identified as an important issue in IS management. The same research also predicted that the security will become key issues in IS management within three to five years. A following research to Brancheau and Wetherbe (1987) was conducted by Niederman, Brancheau, and Wetherbe (1991), whereby, he found security issues a critical issue in a business. Due to the importance of IS management issue, Brancheau, Janz, and Wetherbe (1996) conducted a continuation study to explore issues of IS management between 1994-1995. The security issues were again defined as part of key issue in business IS. The predictions by Brancheau et al. (1996); Niederman et al. (1991); Brancheau and Wetherbe (1987) were proven to be true to date, as many studies such as Cardholm (2014); Sahama, Simpson, and Lane (2013); S. Thompson (2013); Crossler et al. (2013); Warkentin and Willison (2009); Teubner and Klein (2007) continue to discussed information security as an important issue required to be addressed, where it involved different contexts and aspects of the business IS.

The introduction of the Internet has brought many changes in the IS applications within a business. The advances of Internet have improved the human computer interface, enhanced the richness of electronic communication, and automated many information systems (Straub & Welke, 1998). The expanded usage of the Internet invites new development of IS packages. Whilst the organizational dependence on IS has increased, the impact of security abuse also increased correspondingly (Kankanhalli et al., 2003). Threats magnified and evolved in many different forms such as common hacking to high-level security re-engineering threats, which is no longer limited to virus attacks and the environmental threats (Jang-Jaccard & Nepal, 2014; Zhou & Jiang, 2012; Chen, Li, Ma, & Li, 2011; Dlamini, Eloff, & Eloff, 2009; Im & Baskerville, 2005;

Fitzgerald, 1995; Loch, Carr, & Warkentin, 1992). However, security attacks and threats now looks at cloud computing (van Niekerk & Jacobs, 2013; Kandias, Virvilis, & Gritzalis, 2013; Ayala, Vega, & Vargas-Lombardo, 2013; Zissis & Lekkas, 2011), social networking (Dong, Cheng, & Wu, 2014; Mohamed & Ahmad, 2012; Gao, Hu, Huang, Wang, & Chen, 2011) and quantum computing (Mayes & Markantonakis, 2014; Fisher et al., 2014). This has driven many businesses to impose security features to protect their business assets.

The prediction of security issues as an important business issue continues to be confirmed as true as security studies continue to proliferate with the expanded usage of the Internet by many businesses and individuals (Jang-Jaccard & Nepal, 2014; Ayala et al., 2013; Mohamed & Ahmad, 2012; Zissis & Lekkas, 2011; Kritzinger & von Solms, 2010; Dlamini et al., 2009; Kankanhalli et al., 2003; Siponen, 2002a; Straub & Welke, 1998). According to von Solms (2006), the ISSM perspective consisted of four waves. Each wave represents the ISSM practice in its respective time line. In respect to the prediction by Brancheau et al. (1996) and Niederman et al. (1991), von Solms (2006) has explained that in ISSM, there are four stages involved in the ISSM headway. The ISSM four waves concept is represented in the Figure 2.2.

The first wave, known as the technical wave, represents security management studies up to the early 1980s. In this wave, many technical security developments were involved in addressing security problems, for example, solutions on how to share secrets via the Internet using cryptography (Shamir, 1979), solutions on how to protect online data (Denning, 1976) and discussions on how to ensure password security (Morris & Thompson, 1979).

The second wave demonstrates the management wave (1980s- mid 1990s). In this wave, aca-

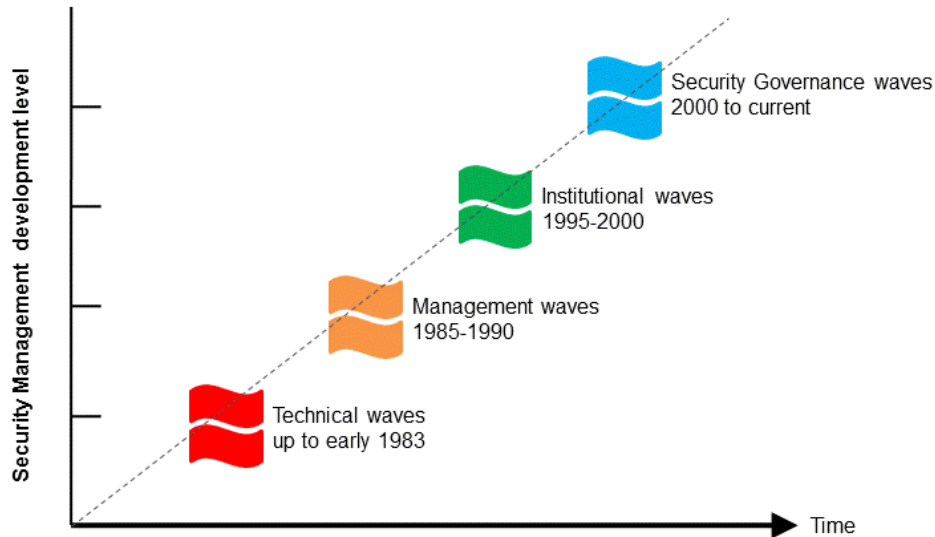


Figure 2.2: Information Systems Security Management (ISSM) development waves adopted from Von Solms, 2006

academic research had started to focus towards discussion on security management issues, examples of which are the seminal paper on computer abuse by Goodhue and Straub (1991), Straub Jr and Nance (1990), Hoffer and Straub (1989) and Straub (1986); and security management success factors by Wood (1987). Although security management issues were discussed in this wave, much of the research was still closely tied to the first wave, for example, the research on security management measurement by Murine and Carpenter (1984), designing IS security by Baskerville (1988) and the computer security TOE by J. Eloff (1988). In this particular wave, there was also research which had started to assess the security management measurement (Murine & Carpenter, 1984), signifying the importance of having good practices in security management.

The following third wave, the institutional wave (late 1990s) represented the institutional security management effort, where discussions were very much focused on the institutional security management issues and problems (Straub & Welke, 1998; Gritzalis, 1997; Parker, 1997). During the third wave, many security good practices and standards were being introduced such

as the Generally Accepted Information Security Principles (GAISP) (ISSA, 2004), British Standard (BS) International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001/2 (formerly known as ISO/IEC 17799) (SIRIM, 2007) and the Standard of Good Practice for Information Security (ISF, 2003).

Finally, the fourth wave, also known as the information security governance wave, starting in early 2000 up to the present time. The security governance wave sets forth the importance of security management regime in a business, where it emphasize on the holistic business perspective. It is in this wave, many scholars presented the importance of security governance (Abu-Musa, 2010; Ruighaver, Maynard, & Chang, 2007; Da Veiga & Eloff, 2007; von Solms, 2006) and security management maturity (Dzazali, Sulaiman, & Zolait, 2009; AlAboodi, 2006; Siponen, 2002b) of a business, hence defining effective security management. Each of the mentioned waves involves different ISSM research characteristics and business involvements, starting with technically oriented characteristics to organizational maturity state of ISSM focus. The ISSM waves discussed above are summarized in Table 2.1.

Table 2.1: Summary of Information Systems Security Management (ISSM) development waves

Waves	Description	Issues addressed
1st wave- Technical waves (up to early 1980s)	The 1st wave has a strong technical security management characteristic. Most of the issues are on technical security measures	Technical issues especially on access to systems (ID and passwords)
2nd wave- Management waves (1980s - mid 1990s)	In the 2nd wave, the business management has shown growing realization of the importance of security management. The 2nd waves have a strong connection with the 1st waves in terms of the security management research.	Management issues were being addressed. Growing number of management realization on the importance of security management
3rd wave- Institutional waves (late 1990s)	In 3rd wave, business include best practices and good code of conduct in their security management implementation. There is a growing need of certification. Strong efforts was cultivation an effective security culture on the institution.	Standards and best practices, information security certification and corporate culture
4th wave- Information security governance early 2000 up to current)	In the current wave, there is a strong drive on corporate governance. Policies and procedural inclusion in the business security management has lead to good corporate governance. The progression of good governance has contributed to the maturity of information systems security management of a business.	Legislation and legal issues, diffusion of best practices as the corporate governance and the information systems security governance maturity of the business

Through this discussion, there are two main categories of security management identified. First, is the past security management issues and perspective, and second, is the current security management perspective, which sets forth the security management research path for business improvement. Discussion on ISSM continues with the past and present features of the ISSM perspective based on the four waves mentioned earlier. The past ISSM research includes first, second and third ISSM waves; whereas the present ISSM research is based on the fourth wave.

2.2.1 The Past ISSM Research Highlights

Past research highlights intensive technology related security research and development. This is because in the late 1970s, there was a major introduction of technology such as the network related communication and the introduction of personal computers. These two important chapters in the history of technology have driven more provisions on security. Unfortunately, security was not only driven by sheer introduction of technology, but security was demanded by the need to communicate securely. Looking back at the history of security development, secret communication was introduced as early as the history, due to the need of having secured communication.

Reflecting on the ISSM studies, the technical wave pioneered the security management research. Security management solutions were developed based on systematic protocols and structured techniques (Burrell & Morgan, 1994). During this era, researchers mainly provided practical solutions to each of the practical problems (Dhillon, 1995). Most of the research in the first wave of security management research were geared toward finding functional tools to help and protect systems. For example, the data confidentiality and how to share secrets virtually (Shamir, 1979). It is in this technical wave that the world witnessed the birth of the very famous cryptography algorithm of the decade, i.e. the Diffie-Hellman cryptographic techniques (Diffie & Hellman, 1976). It is a scheme specifically created for cryptographic key exchange by establishing a shared secret key over an insecure communication channel. The research continued and famous cryptographic technique was then introduced which was the RSA) algorithm by Rivest, Shamir, and Adleman (1978).

In the first wave of ISSM, strong technical security management studies followed, including computer security (Morris & Thompson, 1979), database security (Denning, Denning, & Schwartz, 1979) and other technical security solutions (Cohen, 1987; Denning, 1976). At this time, the ISSM solutions strictly emphasized on technical solutions in response to practical ISSM problems and issues.

Contradictory to the first wave of ISSM scenarios, the second wave started to look into other security issues, not only on the technical related solutions to address security management problems. Although there are still strong numbers of technically related research solutions, nonetheless, the research perspective started to see security from a different angle. Researchers such as Baskerville (1993); Straub (1990); Wood (1987) had started to address the important issues of information security management from the business management perspective. This encompassed socio-technical issues surrounding technology related problems, such as the computer security and abuse (Straub & Welke, 1998; J. Eloff, 1988; Cohen, 1987; Straub, 1986; Murine & Carpenter, 1984). Here, problems such as systems users were addressed, bringing in meaning that ISSM is not only related to technical solutions, but human issues altogether.

The third wave showed research concerning with ISSM using best practices and good code of conduct. Here, there is a growing need of certification towards cultivating effective security culture in the institution. It is also in this wave that many standards and good code of conduct were introduced (Carnegie-Mellon, 1999; Stacey, 1996). Researchers started to investigate the viability of standards and best practices in the business environment (Dhillon & Backhouse, 2000; M. Eloff & Von Solms, 2000a, 2000b; Siponen, 2000). Issues on security management framework, approaches and planning were important topics during this wave. Many socio-technical

issues were brought up including the environmental issues which referred to the importance of standardization and its function (Straub & Welke, 1998; Parker, 1997; Fitzgerald, 1995); and enforcement by the authoritative body (Straub & Welke, 1998; Loch et al., 1992).

2.2.2 The Present ISSM Research Highlights

The fourth wave of ISSM research reflects the present ISSM research. There are wide varieties of issues presented in the recent articles in the security management context. However, through reading, the researcher could identify that there are three important issues encompassing (i) technology, such as security tools (Monfelt et al., 2011; Yildirim et al., 2011; Ozkan & Karabacak, 2010; Tsohou et al., 2010; Da Veiga & Eloff, 2010); (ii) organizations including business security policies and processes (Barlette & Fomin, 2008; Fomin & Vries, 2008; Siponen et al., 2008; Da Veiga & Eloff, 2007; S'anchez, Villafranca, Fernandez-Medina, & Piattini, 2006; Siponen, 2006; Von Solms, 2005; Rees, Bandyopadhyay, & Spafford, 2003; Baskerville & Myers, 2002); and finally, the (iii)environment related issues such as the external users and market structure (Barlette & Fomin, 2008; Albrechtsen, 2007; Zuccato, 2007; Ruighaver et al., 2007; Torres et al., 2006).Baskerville (1988) defined ISSM as a broader view of computer security term incorporating system analysis and design method, manual information systems, managerial issues and both societal and ethical problems. This shows that ISSM is the way and means used by a business to manage information systems towards having acceptable risk (Abu-Musa, 2010).

The current literature highlights the importance of IS security practices in a holistic manner (Werlinger et al., 2009; Zuccato, 2007). The technology has to be able to assist the business in implementing ISSM (Anderson & Choobineh, 2008; Zuccato, 2007). For example, security

technology such as the antivirus software, cryptographic methods and the intrusion detection systems have their own functions to ensure safety of a business. These security technologies were developed to provide countermeasure for businesses to control risks. These technologies deploy secure countermeasure by deploying unique features to address specific security management problems. Different business context may deploy different types of security technologies to protect its business environment. As for the organization issues, it entails the systems users, internally and externally (Yildirim et al., 2011; Albrechtsen, 2007). Organization issues involved the business owner's responsibility and the human issues surrounding the business. These would include human resources management such as training, knowledge upskill, competencies and awareness level (Tsohou et al., 2010; Da Veiga & Eloff, 2010). Besides involving the human development, organization issues must also cover the TOE and procedure governing a business. This is important because without the policies, system users may not have any manual to refer to whilst conducting everyday business tasks in case of any security emergencies. Human related issues also surround the business owner's motivation and support, which is essential in making the security management of a business successful (Gillies, 2011; Siponen & Willison, 2009). A business TOE is often built based on the current security standards (Baskerville & Myers, 2002; Gritzalis, 1997). As such, business policies become the standard procedure to exercise ISSM in a business. This shows that current security standards become an important support tool for the business to conduct good code of conduct. Finally, the environment issue, where government enforcement and market infrastructures are seen to influence ISSM (Monfelt et al., 2011; Werlinger et al., 2009) many businesses in implementing security management. In environment issues, government enforcement on security is referred to authoritative actions taken (Gillies, 2011; Fomin & Vries, 2008; Hu et al., 2007). Many enforcement by the government are highly based on the current standards (Gillies, 2011; Tso-

hou et al., 2010). Besides the government enforcement, industry influence is also an important environment factor as many security management conducted by business are supported by the suppliers who are the industry players.

In this present ISSM research, an analysis on selected standards was conducted. The purpose on conducting this analysis is to understand the socio-technological factors involved in the standard. The literature review then continued with discussion on the ISSM issues discussed in current research articles. The purpose of this review is to conclude on the present and current issues from the academic research context. From the two types review based on the (i) the research articles and followed by the (ii) standards ; the research concluded three important factors of TOE, which are further discussed in the mentioned subchapter.

2.2.2 (a) The characteristics of the standards

The importance of standards in ISSM is clearly reflected in many present studies including the information security measurement roles by Stoll and Breu (2013), the studies on quality improvement in ISSM by Gillies (2011) and the security management communication by Monfelt et al. (2011). In this research, the characteristics of standards are highlighted to provide understanding in implementing ISSM. ISSM implementation lies in many reference models available where most are found in the form of standards created by the international standardization body. Standards and best practices are mostly created practically for the business usage. Most of these standards and best practices were built and developed based on the traditional or conventional business, also known as hierarchical business (Zuccato, 2007; Siponen, 2006). Unfortunately, only a small amount of these standards and best practices support specific business contexts especially the SMI/E e-commerce business context such as the ISO/IEC27001/2 and the Information systems security management maturity framework by Aceituno (2006a).

As all businesses are affected by security risks, a SMI/E with e-commerce is also required to protect its business through effective ISSM. By using the current standard available, such as the ISO/IEC27001/2 and the Information systems security management maturity framework by Aceituno (2006a), SMI/E with e-commerce should be able to implement ISSM in the business. However, the fact that current standards support the SMI/E with e-commerce minimally, the task of adopting may be challenging and daunting sometimes. Hence, the business will take a longer time to achieve ISSM maturity due to this drawback. As such, it is important to understand the characteristics of standards to identify the elements that lie in a standard, whereby the business could set an aim to achieve ISSM maturity promptly. The three most commonly used standards are selected to provide comparison of standards' characteristics. Among the three most influential security management models for information security management mentioned in Siponen (2006), are the Generally Accepted Information Security Principles GAISP, the BS ISO/IEC 27001/2 and the Standard of Good Practice for Information Security. However, the GAISP related work was dropped from the Information Systems Security Association (ISSA) few years back, hence it is not related for this discussion. The researcher has added in one more security standards for the purpose of comparison which is the ISO/IEC 15408 also commonly known as the Common Criteria (Common Criteria (CC)).

Three mentioned security management standards characteristics are summarized in Table 2.2. The three mentioned standards were developed to address ISSM issues of security management in the organization. Each one of these standard look at accepted and the usage of the standard in a business environment. The standards provide principles and practices which business could use to implement effective ISSM. Besides that, the scope of usage is appropriate for security practitioners who are involved in the organization information systems that have the authority to safeguard business by implementing appropriate and effective security management practices.

Although these standards are widely used, these standard processes, guidelines, and the principles provided are abstracted and simplified (Siponen, 2006; Zuccato, 2007). These standards were used to provide reference on the important characteristics available in the commonly used standards.

Table 2.2: Standards for information Security Management

No	Standards	Year	Goal and aims	Scope
1	ISO/IEC 27001/2	2005	It is intended for use in involved organization to secure its information systems	Security practitioner to assist in securing organizations' information systems
2	The Standard of Good Practice for Information Security	1996	To provide international, authoritative and comprehensive benchmark for information systems security	Organization information systems security managers and implementers
3	ISO/IEC 15408 (Evaluation Criteria for IT Security)	2005	This standard helps evaluate, validate, and certify the security assurance of a technology product. It is done by comparing the technology product against a number of factors, such as the security functional requirements specified in the standard	Information security practitioners

A comparison was made between the mentioned ISSM standards. Through the comparison, the research concludes important socio-technical factors in achieving effective ISSM for a business. The comparison presented five important socio-technical factors or also referred to the ISSM standard characteristics, which are the:

- (i) design and implementation drivers which include the business structure and business requirement;
- (ii) governance addressing the TOE and security roles;
- (iii) organization processes internally and externally;
- (iv) technology encompassing physical and logical structure; and finally the (v) behaviours

which address the issues of belief and motivation.

The design and implementation drivers are important for the businesses to assess their ISSM implementation. The governance means a system by which an organization directs and controls IT security (ISO/IEC, 2008). This refers to the policies and procedures, risk assessments, roles, assurance, compliance and baseline available which are being practised in a business. Organizational elements refer to the internal and external issues, where it comprises business process involved in the business. Business users include the employees, customers and suppliers. Technology refers to the physical equipment and utilities comprising the security technologies and security techniques such as access control, access rights and authority level, which are some of the examples of logical security techniques. Finally the behaviour/culture refers to ethics and moral principles (attitude) important in having ISSM. A summary of the two influential ISSM standards based on the five important factors or characteristics identified is concluded in Figure 2.3.

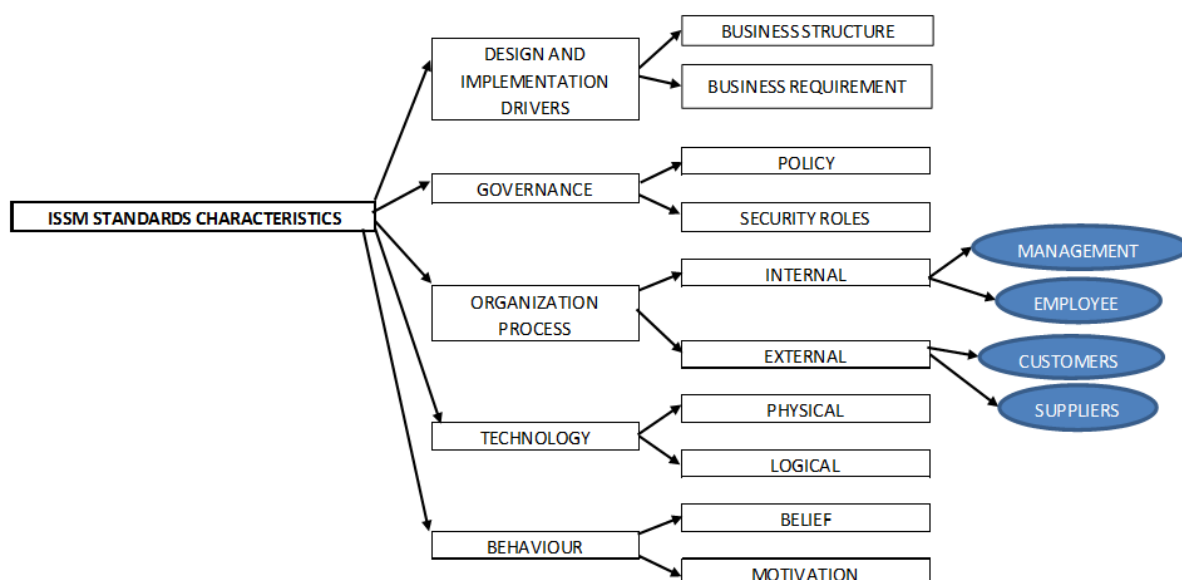


Figure 2.3: ISSM Standards Characteristics

The ISSM standard characteristics define the importance of technology aspects, organization aspects and environment aspect as the root matters. Although Figure 2.3 does not show explicitly show these three aspects, the same figure illustrated that TOE are the substances of the standards. Therefore, subsequent discussion is focused to analyse the characteristics defined in the standards from the standpoint of the research perspective. The following literature review analysed the ISSM articles from the academic research perspective to understand the aspects of TOE associated to ISSM implementation.

2.2.2 (b) Socio-technical factors derived from Information Systems Security Management Research

In the introduction of this chapter, socio-technical elements are mentioned as the main causes of implementing effective ISSM. Through effective ISSM, the business has the opportunity to achieve ISSM maturity. Studies have been conducted on ISSM in a business, where many have mentioned that the success factors in implementing ISSM are the distinctive nature of TOE involved in the business (Caralli et al., 2004; Torres et al., 2006; Wood, 1987). Wood (1987) highlighted the ISSM issues from the managerial perspectives. There is an appropriate balance between managerial and technical issues to address effective ISSM of a business. There are ten managerial perspective determined which are:

- (i) personal responsibility designation;
- (ii) authority role;
- (iii) group responsibility;
- (iv) reporting relationship;
- (v) alternative responsibility allocation for small business context;
- (vi) independence;

- (vii) management hierarchy level;
- (viii) system security responsibility assignment;
- (ix) financial support; and finally
- (x) management personal liability.

The ten issues addressed stressed on the importance of the combination of socio-technical factors which were determined by Wood (1987) as crucial in any ISSM in a business. The factors emphasised on TOE related issues including organizational issues of IS such as the personal responsibility, management hierarchy level; the technological issues which are the system security responsibilities and finally the environment issue such as the financial support required. Through Wood (1987) discussion, we could identified items under the technology, organization and the environment aspects. This paper was chosen to start the ISSM discussion from the point of academic research to show that the idea of ISSM implementation is closely related to the three socio-technical of TOE at the early stage of the introduction of ISSM which was back in 1987. These socio-technical issues have stood through more than twenty years of research, where similar factors were identified in later research investigations as mentioned in Straub Jr and Nance (1990); von Solms (2006); Werlinger et al. (2009); Monfelt et al. (2011); Hsu et al. (2012).

An empirical research carried out by Straub Jr and Nance (1990) and Straub (1990) using the general deterrence theory adopted from criminology, has reported some similar issues as where security countermeasures and administrative deterrence procedures (Straub, 1990) could distinctively prevent and deter computer abuse. This marked that security infrastructure, tools and support mechanisms for security management are very much required in any type of business.

Tools and support mechanisms can be in the format of simple support programmes such as security support programmes (D'Arcy & Hovav, 2009), TOE making (Baskerville & Myers, 2002), specific modelling (Anderson & Choobineh, 2008; Siponen & Oinas-Kukkonen, 2007) and robust security framework (Zuccato, 2007; Tryfonas et al., 2001). Although this means more resources are required, companies with available expertise may consider this as effective. These technical components should be formed under the management security practices, which will determine the best and most resourceful tools and mechanism to design an effective security management in a business.

Information security awareness is one issue which was given a clear emphasis by Wood (1987). His concern on information security awareness in the organizational context has been reiterated by many scholars including Kowalski, Pavlovska, and Goldstein (2013); Kritzinger and von Solms (2010); Werlinger et al. (2009); Siponen (2005); Kankanhalli et al. (2003); Fitzgerald (1995); Loch et al. (1992). Awareness usually comes from solid founding of staff competency and cognizance of top management. Thus, high motivation from the staff, plus top management support could also cultivate the awareness level in the security management of a business. Awareness could be cultivated in the organization through many different approaches including training (Kowalski et al., 2013; Kritzinger & von Solms, 2010; Dlamini et al., 2009; Kankanhalli et al., 2003; Heikka, Baskerville, & Siponen, 2006), assigning responsibility (Van Niekerk & Von Solms, 2010; Von Solms & Von Solms, 2004; Wood, 1987) and effective communication (Eickelmann, 2004; Schlarman, 2002). Top management as a role model (Gillies, 2011; Monfelt et al., 2011; Yildirim et al., 2011) could increase staff motivation to be mindful of the importance of security management. Human issues are strongly seen as a contributing factor (Werlinger et al., 2009; Kraemer et al., 2009; Albrechtsen, 2007) towards an effective security management.

IS security objective in the businesses lay the foundation of the business direction in their security management effort. Together with clear strategy and guided with elucidative TOE, businesses can focus on the type of security management effort they should be having. Besides acting as guidelines, these procedural references could protect the businesses from further liability posed by the users (Hone & Eloff, 2002). They also serve as a point of reference when there are threats towards the business information systems (Baskerville & Myers, 2002). A security TOE developed by a business usually refers to available standards and best practices (Da Veiga & Eloff, 2007). Standards and best practices act as a catalyst to accelerate the development of effective policies and guidelines (Fomin & Vries, 2008). The businesses that have good security governance are businesses that exercise their security policies and procedures implemented in the businesses for the businesses safety (Abu-Musa, 2010; Da Veiga & Eloff, 2007). It is clear that there is a strong dependence between business policies with standards and best practices. A successful security management relies on practicable policies for executable security management tasks in the business (Gillies, 2011; Monfelt et al., 2011).

Besides the logical entity of the businesses such as the IS security objectives and policies, business physical characteristics were found to influence ISSM of the businesses. The organization size and industry or business type are two factors that influence security management in a business (Kraemer et al., 2009; Chang & Ho, 2006; Kankanhalli et al., 2003). Physical characteristics refer to the size and type. The logical structure refers to how business is being set up in terms of the business objectives, policies and procedure. As such, the logical structure refers to the business objectives, direction, policies, security requirements and business needs. Logical structure represents the organization characteristics, hence this research set logical characteris-

tics under the organization elements.

Finally, environmental influence is also seen to contribute towards successful ISSM. This statement holds true as many articles collectively agreed that external factors consist of government enforcement and user involvement (end-users or suppliers) (Gillies, 2011; Monfelt et al., 2011; Fomin & Vries, 2008; Torres et al., 2006). Government enforcement is important as it influences IS security exercise in a business. This is because legislative issues are rules and are governed by the administrative bodies, usually from the government. Once the government legislates ISSM as a compulsory assignment in all types of businesses, it is necessary for the businesses to adhere to it so they could achieve compatibility within market players (Fomin & Vries, 2008; Hu et al., 2007). In conclusion, there are three major elements contributing to the success of ISSM, which are the TOE. The socio-technical factors involved in ISSM success are depicted in the Figure 2.4 below.

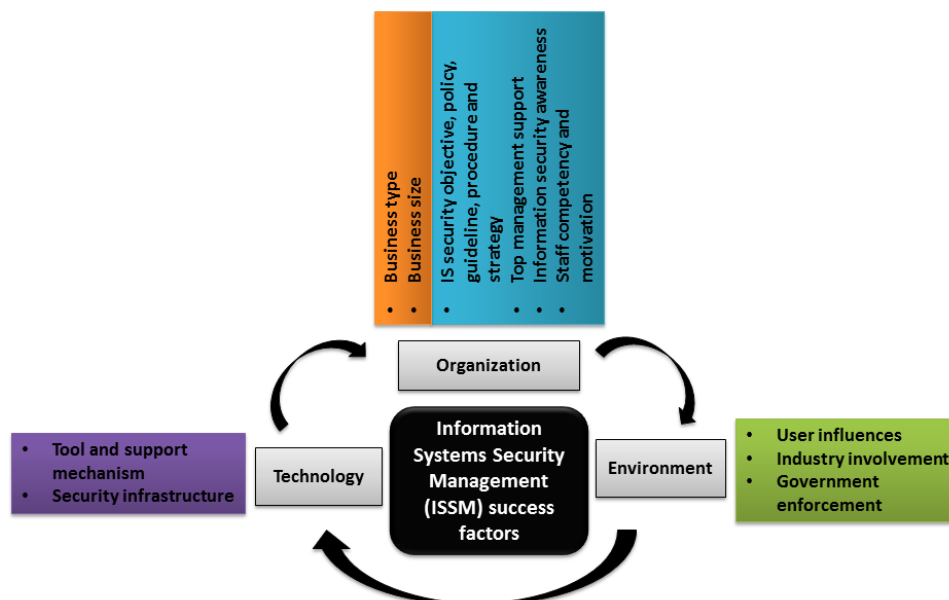


Figure 2.4: ISSM Success Factors

2.3 Information systems security management (ISSM) Maturity

Maturity is the quality or state of being mature or fully developed (Dictionary, 2011). Fraser, Moultrie, and Gregory (2002) in its Capability Maturity Model (Capability Maturity Model (CMM)) defined maturity as the extent to which a process is explicitly defined, managed, measured, and controlled effectively. This research defines the ISSM maturity as the state of which the business has achieved effective ISSM practices. This is a state where the business has successfully connected the socio-technical elements (of TOE) with the presents of business forces (determination to change), to reach its highest ISSM maturity. With the high factor connection and business forces or business dynamics, the business is able to change and adapt the ISSM in the volatile SMI/E business structure. This is because in achieving ISSM maturity, a business is challenged to exercise effective ISSM. Without effective ISSM, a business would not be able to achieve the ideal ISSM level required to safeguard its assets. The importance of having ISSM maturity in a business is not only to assess the ISSM level exercised, but most importantly, it helps businesses to identify any weaknesses of business ISSM.

Many different maturity studies have been carried out due to its importance in a business. One of the earliest maturity studies and a very prominent one, was in 1979 by Philip Crosby on quality management maturity grid (Crosby, 1979). This quality management maturity grid has set forth the maturity grid and has since become the fundamental reference for any maturity studies to define the maturity grid division. This research has conducted the analysis and comparison on four ISSM maturity standards, model and framework, to better understand the ISSM maturity and its important characteristics. Through this analysis and comparison, the researcher could identify the elements of influence to achieve ISSM Maturity in a business. In the security management field, there are security related maturity standards developed, including

the Systems Security Engineering Capability Maturity Model (SSE-CMM) (Carnegie-Mellon, 1999) or currently known as the ISO/IEC21827:2008, Information Security Program Maturity Grid (Stacey, 1996), software security metrics by Murine and Carpenter (1984) and the open information security management maturity model (ISM3) by Aceituno (2006a). All these developed maturity standards have defined the importance of having security practices in all types of business involving IS.

2.3.1 The Information systems security management ISSM Maturity Standards

This research focuses on the ISSM maturity issues. As such, critical analysis is concentrated on the ISSM standards and framework only. The four selected standards which were reviewed are the SSE-CMM (Carnegie-Mellon, 1999), Information Security Program Maturity Grid (Stacey, 1996), software security metrics (Murine & Carpenter, 1984) and the information security management maturity model (ISM3) (Aceituno, 2006a). These four standards and maturity models are significant in ISSM maturity research. The reason of choosing the four security management maturity standards and framework for the discussion in the research is because first, the three models earlier mentioned have addressed many issue in IS security management (Siponen, 2002b). The SSE-CMM has also become a standard under the ISO/IEC section which is now also known as ISO/IEC 21827:2008. As for the ISM3, this framework was discussed in (Dzazali et al., 2009; Lessing, 2008) and currently is part of the maturity model used by many industries for ISSM implementation. The ISM3 highly focuses on process integration which address important issues in business IS.

2.3.1 (a) *Software Security Metrics by Murine and Carpenter (1984)*

The Software Security Metrics (SSM) is one of the earliest information systems security management models developed by Murine and Carpenter in 1984. This maturity model looks at eleven high level security criteria with five milestones, focusing on systems and software information security maturity (Siponen, 2002b). The milestones are based on software lifecycle stages including (i) system security requirements, (ii) software system security requirements, (iii) functional security architecture, (iv) modular security gating and (v) security testing. The definition of each milestone is referred in 2.3

Table 2.3: Software Security Metrics Milestone by Murine and Carpenter (1984)

No	Milestones	Sequence
1	System Security Requirements	Security requirements are defined for both software and hardware
2	Software System Security Requirements	Security requirements are defined for software alone
3	Functional Security Architecture	Security requirements are distributed over the functional software architecture components
4	Modular Security Gating	Entry to modules are defined by access requirements
5	Security Testing	System is tested for illegal entry at all levels

The eleven high level security criteria mentioned are presented in Table 2.4. This model deduces a quantifiable software evaluation from inception through adolescence and into adulthood (Murine & Carpenter, 1984). These security metrics highly focus on the process of software development. As such, there is no clear distinctions of TOE being discussed.

Table 2.4: Software Security Metrics Criteria Definition by Murine and Carpenter (1984)

No	Criteria	Definitions
1	Access Audit	Attributes of software that provide for audit of the access of software and data
2	Access Control	Attributes of software that provide for control of the access of software and data
3	Security Traceability	Security requirement of software system that provide a thread from the security requirement to the implementation with respect to software development and security environment
4	Deceptiveness	Attributes of the software that provide explanation of the implementation of dissimilar function
5	Simplicity	Attributes of software that provide implementation of functions in the most understandable manner
6	Security Complexity	Attributes of software that provide implementation of functions in the least understandable manner
7	Inconsistency	Attributes of software that provide random design and implementation techniques and notation
8	Perturbed Error Tolerance	Attributes of software that provide continuity of operation under randomly controlled conditions
9	Security Completeness	Attributes of software that provide full implementation of security requirements
10	Execution Efficiency	Attributes of software that provide for minimum processing time
11	Storage Efficiency	Attributes of software that provide for minimum storage requirements during operations

2.3.1 (b) Information Security Management Maturity Grid by Stacey (1996)

The maturity grid of Stacey (1996) looks at the risk relationship and how it affects security maturity of an organization. This maturity grid also originated from the Quality Management Maturity Grid by Crosby (1979). The Information Security Management Maturity Grid defines five stages or measurement categories of security maturity in ascending orders of stages. These five stages or measurement categories consisted of objective to evaluate enterprise information security maturity. The stages involved are (i) Stage 1-Uncertainty, (ii) Stage 2-Awakening, (iii) Stage 3-Enlightenment, (iv) Stage 4-Wisdom and (v) Stage 5-Benevolence. The higher the

stages are, the more matured it is. Details of each maturity stages are discussed in Table 2.5.

Table 2.5: Maturity stages in Information security management maturity grid by Stacey (1996)

Maturity stages	Maturity stage descriptions
Stage 1-Uncertainty	Business management has no knowledge and does not recognize information security as a tool to protect business assets. All security issues are addressed after the incidents have taken place.
Stage 2-Awakening	Business management knows that information security is of value towards the business but is not ready to allocate any resources. There is no clear point of contact for information on security incidents.
Stage 3-Enlightenment	Business management understands the importance of information security infrastructure towards the business.
Stage 4-Wisdom	Business management participates in everyday information security exercise with an established security infrastructure.
Stage 5-Benevolence	Business management takes information security seriously as it is essential for the business. It is important for the business to prevent any security incidents with serious monitoring and risk management. In this stage, there is a continuous improvement and security practices.

Each stage consists of management in understanding and attitude, security organization status, incident handling, security economics and security improvement actions. Five measurement categories differentiate each stage, thus improvements according to the measurement categories are suggested to achieve a higher maturity stage. In the Stacey (1996) maturity grid, identification of organization and technological issues are given emphasis. In Stage 5 of the maturity grid, emphasis was given on technological improvement, especially when discussion was focused on serious monitoring and risk management. Unfortunately, there is still no clear discussions on the environmental influences towards achieving each level of maturity.

2.3.1 (c) *Systems Security Engineering Capability Maturity Model (SSE-CMM)(Carnegie-Mellon, 1999) or the ISO/IEC21827:2008*

The SSE-CMM model or currently known as the ISO/IEC21827:2008 is derived from the CMM focused on requirements for security implementation in a system of the Information Technology (IT). Its objective is to improve and assess security-engineering capability of an organization. This model is primarily driven by the business goal and it is a process-specific information assessment. Businesses will be able to use SSE-CMM maturity level specified to assess and improve in-house business process due to its logical sequence in improvement effort. SSE-CMM consists of five capability levels representing the maturity of security-engineering in an organization. The capability maturity levels are depicted in the Figure 2.5.

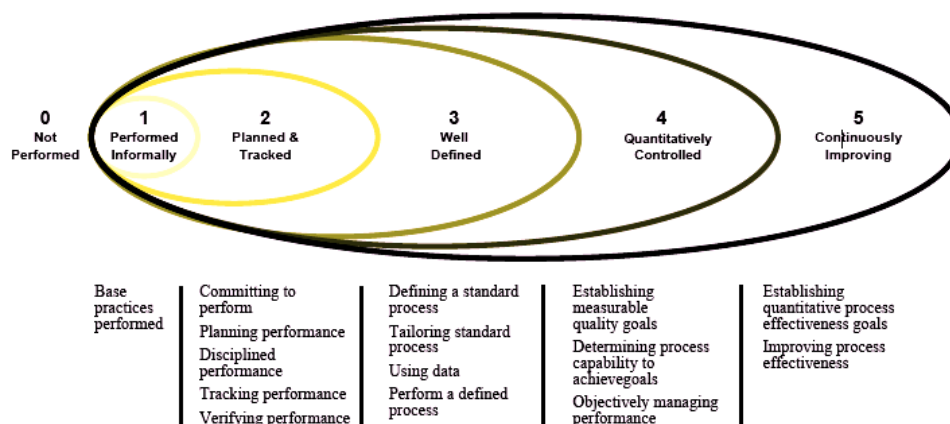


Figure 2.5: Capability level of SSE-CMM by Carnegie Mellon University (1999)

SSE-CMM classifies business which has not performed any common feature in the process area as at level 0. There is no clear description of what is called base practices in the common features of SSE-CMM, so businesses which have somewhat performed what they considered as base practices would be considered as at level 1 maturity. As for levels 2, 3, 4 and 5, these levels require businesses to qualify each common feature for each process area. There are clear descriptions of the common features businesses must meet in their security management

tasks. In order to define and assess which level businesses belong in, they are required to assess the common features and process areas appropriately. The common features are generic practices which are common in each capability level. As for process areas, these consist of the base practices in specific process areas which are referred to as the security-engineering process area as well as the project and organizational process area. Both process areas look into different practices. The security engineering process area focuses on the technological security issues, whereas the project and organizational process area stresses on the human and processes issues.

An example of high abstraction of the common features and process area are depicted in summary as in Figure 2.6. From Figure 2.6, SSE-CMM stresses three important elements in ISSM maturity, which consisted of the TOE. Figure 2.6 shows that issues on (i) technology e.g. the PA01-security control administrations and PA15-control and monitor technical effort; (ii) organization is represented in PA12-ensure quality, PA14-manage project risk and PA21 provide ongoing skill and knowledge; and finally the (iii) environment issues is represented in the PA22-coordinate with suppliers.

In conclusion, the research concluded that technology, elements are related to the security-engineering process, including assessing security risk and threats, monitoring security and recommendation of security. As for organization, the related issues involves the human-related knowledge and awareness, management of processes and its related controls. Finally, the environment issue is the supplier related issues. As such, this research established that in SSE-CMM discussion of maturity, issues that require attention are based on the three earlier mentioned elements.

Table 2.6: ISM3 Maturity Capability Definitions by Aceituno (2006)

No	ISM3 Capability Maturity	Definitions
1	Undefined	There are security processes involved but are not defined
2	Defined	There is a clear documentation of security processes being used in the business
3	Managed	Clear definition of security process. Result is used to fix and improve current processes
4	Controlled	Clearly managed and controlled, with clear milestones where all involved resources are accurately predicted
5	Optimized	Continuously controlled and all fixes and improvement bring resource savings

Each of the above capabilities signifies maturity levels 1-5 of a business as shown in Table 2.7.

At each level, technology issues were mentioned. The environment related issue is as early as level 2 of maturity level, indicating the importance of environmental factors in ISSM maturity.

As for the organization issues, such as business resources, these are mentioned in each maturity level, thus indicating the importance of organization issues in achieving ISSM.

Table 2.7: ISM3 Maturity Level by Aceituno (2006)

ISM3 Maturity Levels	Maturity level description
ISM3 Level 1	Level for organization with low information security targets, low risk involve with little resources. This level provides risk reduction in-term of technical threats.
ISM3 Level 2	Level for organization with normal information security risk targets. Business needs to show good practices to business partners in order to avoid security incidents. This level shows further risk reduction with medium resources investment
ISM3 Level 3	Level for organization with high information security risk targets. This business is dependent on its information systems where moderate to high resources investment is expected. This level shows high risk reduction.
ISM3 Level 4	Level recommended for mature organizations, which are regulatory confined. A high investment on security resource is required where this level shows the highest risk reduction involved.
ISM3 Level 5	Level where continuous improvement and security management innovation is involved. This level is the most experienced level where security management system is optimized and there is a clear reduction of investment.

Based on the examination on the ISM3 documentations and discussions from the standard manual, similar elements to achieving effective ISSM in a business are identified. These elements are also determined as the elements to achieve ISSM maturity. The ISM3 looks into three elements of technology, organizations and environment. Some of the issues addressed under the TOE elements include: (i) technology: define information business, personnel, compliance, access control, priority, durability, information quality and technical related security objectives, (ii) organization: manage budget, people and other resources allocated to information security , and (iii) environment: defines relationships with other organizations, such partners, vendors and contractors.

The earlier security management maturity standards such as the Murine and Carpenter (1984) did not include environment issues in its model discussions. This condition agrees with the

ISSM perspective discussed earlier in Section 2.1, where ISSM research was very much based on the technological issues rather than other business-related issues. Only the later two security management maturity standards and framework agree with the TOE elements, which were found to be involved tremendously to achieve ISSM maturity. Hence, through four standard, model and framework selected, it is seen that the discussion on ISSM evolves where TOE elements have become important issues in addressing any ISSM effective implementation, hence reaching ISSM maturity.

Much ISSM research literature available today discuss effective ISSM as compared to the ISSM maturity in a business. As such, this research embarked to research the importance of TOE in affecting ISSM maturity of a business. The element of TOE involved in ISSM maturity is reflected based on the selected theories and framework. The theoretical assumption of this research is discussed in the immediate Section 2.3.2.

2.3.2 Theoretical perspective of Information Systems Security Management (ISSM) Maturity

Referring to the analysis of the ISSM literatures, ISSM standards and ISSM maturity standards had identified few important elements. The technology issues include compatibility (Fomin & Vries, 2008; Hu et al., 2007), complexity (Werlinger et al., 2009), and relative advantage (Al-Awadi & Saidani, 2010; Kankanhalli et al., 2003), usage (Werlinger et al., 2009) and technology availability (Tsohou et al., 2010). In the organization elements, two main categories were identified which are (i) physical and (ii) logical. Elements under each of these categories include (under item (i)) business characteristics such as business size (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978), business type (Yildirim

et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) and business length (Prananto et al., 2003a; Prananto, McKay, & Marshall, 2003b). As for items under the logical component, they involve (ii) human resources (Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010) and management support (Monfelt et al., 2011; Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010; Ozkan & Karabacak, 2010). Finally, under environment, elements include are the supplier (Kraemer et al., 2009) and government regulations (Farn et al., 2004). TOE attributes identified provide an overview of what the items are that influence ISSM of a business. Through this identification, it helps the researcher to explain whether the same TOE influences are involved in the ISSM maturity of a business.

In order to identify the TOE items in ISSM maturity, this research also analysed literature discussing ISSM maturity in real business situations. This is the first step to observe similar items in ISSM effectiveness mentioned are involved. However, analyses on ISSM maturity showed that ISSM articles are primarily oriented in the ISSM effectiveness, rather than the ISSM maturity. Current research scenario on ISSM maturity mostly discussed ISSM maturity as part of the assessment activity conducted in the research investigation (Zuccato, 2007). Nevertheless, from the comparison conducted between mentioned research, similar TOE are being discussed. Nonetheless, it is highly required by a business to understand the ISSM maturity concept so that the business can exercise the best and suitable ISSM for their business, and directly achieve ISSM maturity. Elements for security management discussed in many ISSM maturity standards and frameworks are very much based on the process involved rather emphasizing on the content and context (Siponen, 2002a).

The identification of ISSM maturity elements through current literature faced some obstacles

due to the limited discussion on ISSM maturity. As such, this research has used the same elements of TOE presented by articles in ISSM research and the ISSM standards, models and framework to further discuss issues which influence the ISSM maturity based on the identified TOE elements. However, the elements gathered from the Section 2.2 and Section 2.3, may not be exhaustive. Hence, the research has selected a few related theories, framework and IS factors to become the research foundation in order to address ISSM maturity issues in the SMI/E.

Theories are used to provide the foundation of any studies (Siponen et al., 2008). There are many reasons as to why theories were used in this research. As mentioned, the previous discussion on ISSM maturity elements in Section 2.2 and Section 2.3, may not be exhaustive. It is through having selected IS theories as a foundation, that thorough issues are expected to be covered because theories provide basic understanding and act as the research lens for this research. The other important reason as to why selected theories were used in this research, is to take up the challenge of Siponen et al. (2008), which had mentioned that IS security research is chronically underdeveloped.

Businesses such as the SMI/Es, which are conducting e-commerce, have to understand the concept of ISSM, thus appropriating them to their business. As such, ISSM cannot be confined to issues in ISSM research studies and the ISSM standards only, but it has to look into the security management in a larger scope based on the TOE elements (Hsu et al., 2012). The current ISSM research asserted that ISSM is an administrative innovation. In order to achieve maturity, this administrative innovation has to be accepted and adopted by the business. Hence, the theory of TOE (Tornatzky et al., 1990) and the DOI (Rogers, 1995) were assessed. Findings from the ISSM literature and standards previously were appropriated based on these two theo-

ries. Besides these theories, the researcher concluded the importance of organizational factors (Ein-Dor & Segev, 1978), and a variable from IS Success Model (DeLone & McLean, 2003, 1992) which is the technology usage as much of the ISSM literature discussed the importance of these elements. The details of elements identified and discussed above are presented in Table 2.8 showing the relationship of elements to the appropriate IS theories discussed. New elements were also included which completed the whole theoretical framework of this research.

Table 2.8: Relationship of elements with the IS theory

Elements identified	Elements from ISSM literatures and standards	Theories related
Technology	(i) compatibility (Hsu et al., 2012; Fomin & Vries, 2008; Hu et al., 2007) (ii) complexity (Werlinger et al., 2009) (iii) relative advantage (Hsu et al., 2012; Al-Awadi & Saidani, 2010; Kankanhalli et al., 2003) (iv) usage (Werlinger et al., 2009) (v) technology availability (hsu2012, Tsohou et al., 2010)	(i) Technology, Organization and Environment framework (TOE) (Tornatzky et al., 1990) (ii) Diffusion of Innovation (DOI) (Rogers, 1995) (iii) IS Success Model (DeLone & McLean, 2003, 1992) (iv) IS Success Model (DeLone & McLean, 2003, 1992) (v) Technology, Organization and Environment framework (TOE) (Tornatzky et al., 1990)
Organization	(i) business size (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) (ii) business type (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) (iii) business length (Prananto et al., 2003a, 2003b) (iv) human resource (Hsu et al., 2012; Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010) (v) management support ((Hsu et al., 2012; Monfelt et al., 2011; Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010; Ozkan & Karabacak, 2010)	(i) organization factors (Ein-Dor & Segev, 1978) (ii) Technology, Organization and Environment framework (TOE) (Tornatzky et al., 1990) (iv) Technology, Organization and Environment framework (TOE) (Tornatzky et al., 1990) (v) organization factors (Ein-Dor & Segev, 1978)
Environment	(i) supplier (Kraemer et al., 2009) (ii) government regulations (Hsu et al., 2012; Farn et al., 2004)	(i) Technology, Organization and Environment framework (TOE) (Tornatzky et al., 1990) (ii) Technology, Organization and Environment framework (TOE) (Tornatzky et al., 1990)

Ein-Dor and Segev (1978) asserted that to develop successful Management Information Systems (MIS), organizational factors are the utmost factors to consider. This statement holds true where organizational factors highly influence ISSM effectiveness and showed that all elements identified play an important role in influencing effective and successful ISSM in a business (Werlinger et al., 2009; Barlette & Fomin, 2008; Fomin & Vries, 2008; Kankanhalli et al., 2003). Organization factors consist of business types, business size and top management support. These three factors inevitably guarantee ISSM success. The ISSM maturity concept involves innovative processes which oversee necessary diffusion of security management practices in a business. As asserted by Rogers (1995) and Tornatzky et al. (1990), process adoption requires communication and a definite social system to agree on and accept changes. It involves attributes that influence and support the social system. Hence, to become mature, successful adoption and diffusion of security management practices are vital (Melenovsky & Sinur, 2006). Decisions to adopt innovative processes in security management depend upon three main criteria, which are technology context, organization context and environment context (Tornatzky et al., 1990). All elements identified highly influenced the ISSM as discussed in the articles referred. This research has chosen identified theories as these theories show high importance in ISSM effectiveness hence relates positively towards the ISSM maturity. These theories help to provide perspective of the relationship of each attribute to investigate the factors influencing ISSM maturity. In the articles discussed, all these attributes were identified independently without the relating with IS theories, many referred authors successfully identified attributes influencing ISSM independently, hence it is difficult for the research to understand the relationship of these independent factors towards ISSM maturity. A such, this research coordinates the independent identified elements and relates them to chosen theories to better predict the ISSM factors contributing to security maturity of a business.

Attribution of elements in the TOE framework and DOI theory to the ISSM maturity research are seen to be highly related. Technology characteristics (Monfelt et al., 2011), availability, complexity (Ozkan & Karabacak, 2010; Werlinger et al., 2009) and compatibility (Kraemer et al., 2009) influence the security management practice in a business. Maturity is also related to time (Prananto et al., 2003a, 2003b). Besides time, two significant items deemed to influence ISSM maturity are usage and user satisfaction (DeLone & McLean, 2003, 1992). As ISSM maturity requires continuous involvement of users, usage and user satisfaction are to be considered in this research. These two attributes form part of the IS success model as posited by DeLone and McLean (1992). The theoretical view represents how each variable of selected theories relates with each other, which embody a mature ISSM of a business. As such, four new elements, which are considered to be highly influential, were added to the elements from ISSM literature and standards. The complete elements involved are as represented in the ISSM maturity theoretical model as depicted in Figure 2.7.

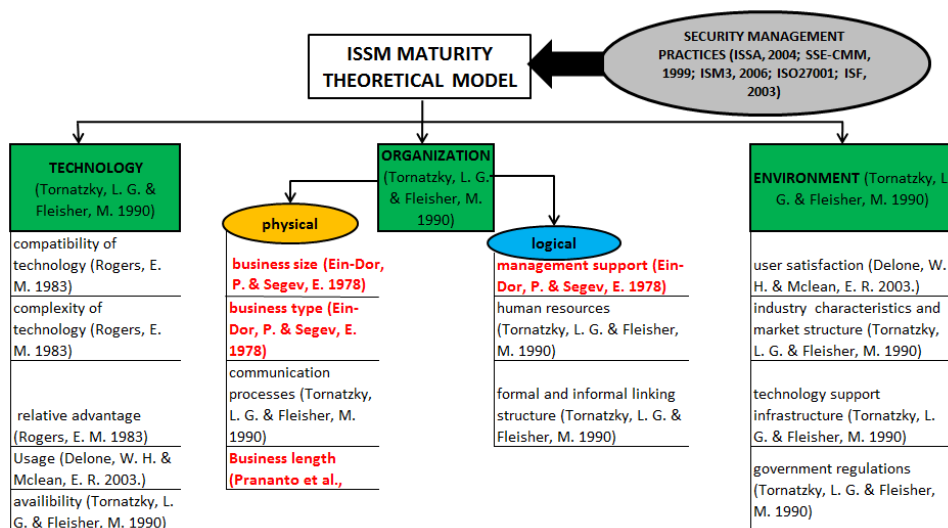


Figure 2.7: ISSM maturity theoretical model

2.3.2 (a) Definition of Attributes in Technology, Organization and Environment

The attributes of TOE are define in the Table 2.9 to better understand the relationship of these attributes hence provide a clear representation for the purpose of research conceptual framework development in Chapter 3.

Table 2.9: Definition of Attributes in Technology, Organization and Environment

NO	TOE Attributes	Definition
1	Compatibility of technology	Capability of the technology to perform harmoniously to support specific task (Werlinger et al., 2009)
2	Complexity of technology	The richness of a technology to support a business task (Werlinger et al., 2009)
3	Relative advantage	Ability to offer advantages relative to existing comparable products (Al-Awadi & Saidani, 2010)
4	Usage	How technology is used and leveraged in a business (Ozkan & Karabacak, 2010)
5	Availability	The technology position whereby technology is always available to support specific task (Ozkan & Karabacak, 2010)
6	Business size	Size of the organization usually is reflected by the number of the staff in the business (Kankanhalli et al., 2003)
7	Business type	Type of business the organization is involved with e.g. financial institution, public sectors and manufacturing (Kankanhalli et al., 2003)
8	Communication process	Processes involve in the business to communicate knowledge and technology usage (Ling, 2001)
9	Business length	The length of time organization is involved in the specific trading (Prananto et al., 2003a)
10	Top management support	Top management behaviour and action towards business information system security management effort. It is highly related to the top management action towards (i) IS security-related meetings, (ii) IS security-related decisions, (iii) monitoring IS security-related activities and (iv) support on IS security-related functions (Kankanhalli et al., 2003; Thong, Yap, & Raman, 1996)
11	Human resources	Human related issues in the security related exercise (Hsu et al., 2012)
12	Formal and informal linking structure	Formal structure refers to the authority who could make decisions and the degree of autonomy and flexibility that this individual have to initiate new ideas e.g. formalization or decentralization and as for informal linking structure it refers to degree to which organizational norms support and direct behaviors e.g. top management support which is usually associated with the innovation process (R. Russell, 1990)
13	User satisfaction	User behaviour due owing to the specific service provided by a business (DeLone & McLean, 2003)
14	Industry characteristics and market structure	Current market status depending on the type the business is involved in (Alfawaz, 2011)
15	Technology support infrastructure	Support infrastructure provided by supplier or vendor (Yildirim et al., 2011)
16	Government regulations	Government legislation regulated in a country (Hsu et al., 2012)

Relatively, through the comparison between ISSM standards, ISSM research literature and the

IS theories and framework, TOE become the main contributing elements. This research predicted the same issues of TOE in ISSM maturity in practical scenarios involving a business. In Zuccato (2007), holistic ISSM for an e-commerce business involved TOE. The holistic ISSM was assessed using SSE-CMM, and it showed the TOE elements being highly involved in ensuring effective ISSM. A recent research by Hsu et al. (2012) also showed how TOE influenced ISSM. This article also defined ISSM method, model and process developed as an innovation, where this innovation is referred to as an administrative innovation, hence benefit the business to achieve ISSM maturity. This is because an administrative innovation represents any new ideas and practices that are lacking in adoption when they are carried out. This will become the regular practice of the organization. Hsu et al. (2012) also mentioned that this innovation can potentially be conducted in different ways applicable to the organization, hence promotes organization change which in this research context discussion it will contribute towards business ISSM maturity. Hsu et al. (2012) asserted the importance of the factor relationship and other change issues, substantial to the meaning of innovation discussed in their article. It also highlights that for organization change, factors identified for business to reach intended ISSM maturity may not be assessed via static relationship. However it may require an in-depth research so the phenomena could be understood clearly. Besides discussion by Zuccato (2007); Hsu et al. (2012), Dzazali et al. (2009) in their discussion on ISSM in the Malaysian public organizations, asserted the presence of TOE elements in maturity assessment and also mentioned the influence of TOE elements towards an organization. The comparison between ISSM standards and framework with ISSM research literatures state issue of concerns are depicted in Table 2.10.

Table 2.10: ISSM Issues of Importance

ISSM Maturity factors	Issues of importance	References
Organizational factors [INDEPENDENT FACTORS]	Business size	(Werlinger et al., 2009; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978)
	Business type	Werlinger et al. (2009); Chang and Ho (2006); Kankanhalli et al. (2003); Ein-Dor and Segev (1978)
	Top management support	Hsu et al. (2012); Werlinger et al. (2009); Chang and Ho (2006); Kankanhalli et al. (2003); Ein-Dor and Segev (1978)
Business Length [INDEPENDENT FACTORS]	Length of time in business	Dictionaries (2011); Prananto et al. (2003a, 2003b)
Technology [MEDIATING FACTORS]	(SM structure)compatibility of technology, complexity of technology, relative advantage, usage, information and system quality, availability	Hsu et al. (2012); Monfelt et al. (2011); Ozkan and Karabacak (2010); Werlinger et al. (2009); Kraemer et al. (2009); Dzazali et al. (2009); SIRIM (2007); Aceituno (2006a); Dzazali (2006); ISSA (2004); ISF (2003); Carnegie-Mellon (1999); Stacey (1996); Murine and Carpenter (1984)
Organization [MEDIATING FACTORS]	(SM Value, SM Purpose, SM Utilization) communication processes, formal and informal linking structure, human resources	Hsu et al. (2012); Yildirim et al. (2011); Tsohou et al. (2010); Da Veiga and Eloff (2010); Dzazali et al. (2009); SIRIM (2007); Albrechtsen (2007); Aceituno (2006a); Dzazali (2006); ISSA (2004); ISF (2003); Carnegie-Mellon (1999); Stacey (1996); Murine and Carpenter (1984)
Environment [MEDIATING FACTORS]	(SM Support, SM Stimuli) user satisfaction, industry characteristics and market structure, technology support infrastructure, government regulations	Hsu et al. (2012); Gillies (2011); Alfawaz (2011); Yildirim et al. (2011); Dzazali et al. (2009); SIRIM (2007); Aceituno (2006a); Dzazali (2006); ISSA (2004); ISF (2003); Carnegie-Mellon (1999); Stacey (1996); Murine and Carpenter (1984)

The issue of importance segregates the organization factors and business length from the TOE. As asserted by Yildirim et al. (2011); Chang and Ho (2006); Kankanhalli et al. (2003); Ein-Dor and Segev (1978), in ISSM, organization factors are independent factors that influence the ISSM of a business. Same goes with the business length, where the time of business (Prananto et al., 2003a, 2003b) operation influenced the maturity of a business independently. Remaining issues as discussed in the next section are categorized in TOE as each of the elements are also addressed by the standards and framework. These issues are seen as mediating factors. This is

because all issues relates highly on how it is employed in a business. All the issues addressed have high relations with the business characteristic including the business type, size and management support, plus business length (time) in the market. To achieve the ISSM maturity, the SM practices is seen to be the mediating factors. This is because without the SM practices, business would not achieve ISSM maturity. The classification of issues which fall under each of the TOE elements are derived based on the requirement and issues from by the ISSM standards and framework. Through three standards and framework which were being discussed earlier, we derived that under each TOE elements, the classification similarly address item mentioned in the ISSM standards, which this research has grouped as SM practices. Under technology, SM task involved the inclusion of the technology usage and structure, organization involves the business purpose, value and utilization of SM, and finally the environment which consisted of support and stimuli surrounding the SM in a business environment. The independent and mediating factors for ISSM Maturity are also described in the same Table 2.10.

2.4 The Study: Malaysia SMI/E with e-commerce

ISSM is widely used by many businesses (Hsu et al., 2012; Gillies, 2011; Alfawaz, 2011; Yildirim et al., 2011; Abu-Musa, 2010; Al-Awadi & Saidani, 2010; Ozkan & Karabacak, 2010; Dzazali et al., 2009; Werlinger et al., 2009; Kraemer et al., 2009; Barlette & Fomin, 2008; Fomin & Vries, 2008; Yeo et al., 2007; Albrechtsen, 2007; Zuccato, 2007; Hu et al., 2007; Yeh & Chang, 2007; Dzazali, 2006). Based on the literature referred to, most of the discussions involved big and hierarchical organizations, who own many types of IS in their businesses. As such, many developed standards were designed to fit this type of business rather than the SMI/E with e-commerce. Based on this situation, the SMI/E has to appropriate the current standards and framework in their businesses accordingly. This task in not straightforward or easy as it involves time and resources to coordinate this effort. The Internet technology has

changed the way how SMI/Es conduct their daily business processes. With e-commerce efforts these businesses are susceptible to security risk and they need support in safeguarding business assets. The increase in the world Internet users from Asia shows the strong need of having secure business transactions from the SMI/E with e-commerce. The online census by the Internet world statistics show the latest world Internet usage as of March 2011, has reach to 2,095,006,005 people, where 44% of the world's Internet users are from Asia (Stats, 2011). In Malaysia, the Internet usage is at 19,082,000 people with 65.8% penetration as of December, 2013 as reported by the The World Bank. A report from the Internet world statistics shows strong increase among the Internet users in Malaysia from 2000 to date.

2.4.1 Malaysian SMI/E

In Malaysia, the SMI/E is considered as one of the important annual revenue generators consisting of 47.3% of the total Gross Domestic Product (GDP) (Aris, 2006; Bank Negara, 2005). According to Bank Negara (2005), about 99.2% of establishments in Malaysia consisted of SMI/Es, one of the largest countries in Asia having the SMI/E establishments apart from Japan, Korea, Philippines, Thailand and Indonesia. SMI/E is classified into three different groups, which are micro, small and medium. SMI/E is considered as one of the important business entities in the Malaysian economy as the SMI/E helps generate new employment, create new income distribution and plays as a training ground for entrepreneurs before investing on a larger scale of business (Burhanuddin, Arif, Azizah, & Prabuwono, 2009). Burhanuddin et al. (2009) asserted that SMI/E can stimulate private ownerships, increase entrepreneurial skills and become an incubator for developing domestic enterprises into large corporations. Although the SMI/Es have shown many advantages towards a country such as Malaysia, this business is still small compared to other types of businesses in Malaysia, such as the large types of businesses

including the Government Link Companies (GLC) and the International conglomerates. The SMI/E is also very much influenced by the technology, especially the Internet. This SMI/E showed fair level of acceptance in the technology and e-commerce usage (Ainin & Noor Ismawati, 2003) and e-commerce readiness (Ramayah, Yan, & Sulaiman, 2005). Hence, it is very important that this business context is given emphasis as it can increase the Malaysian annual turnover.

2.4.2 E-commerce scenario in Malaysia

In Malaysia, e-commerce took its place back from 1995 (Paynter & Lim, 2001). By 2000, many changes had happened in the Malaysian online business. In the year 2000, Bank Negara Malaysia (BNM) formally allowed local commercial banks to provide online banking services (Andam, 2003; Sohail, 2003). The Malaysian online market has seen much evolution from physical trade to online trade starting from the year 2000. The raise of e-commerce website is also highly dependent on the product provided as asserted by Andam (2003). In Malaysia, the e-commerce business sees the raise of the phenomenal e-commerce websites, which include the Air Asia; the first economical flight ticketing business in Malaysia. Besides, business that provides telecommunication product and service such as Maxis is also successful in its online transactions efforts. There are businesses such as online ticketing, online retail stores, online bidding systems and other businesses. Alam and Ahsan (2007) concludes in his research that the Internet also acts as a medium for commercial use in the manufacturing arena. In the tourism industry Malaysia, Mohamad and Ismail (2009) affirmed the e-commerce usage has influenced business performance, hence it is important for the tourism business to implement e-commerce for business sustainability. The Internet is seen as a marketing platform where businesses could tell the rest of the world about their the nature of their businesses, which

makes it very interesting to the small businesses such as the SMI/E. Besides, it is not costly and is very simple to be carried out. E-commerce has since become a potential revenue generator to the country (Ainin & Noor Ismawati, 2003). Based to this reason, the Malaysian government is currently giving serious support towards e-commerce businesses especially in the SMI/E business for global promotions and revenue generation. Although there are many advantages of e-commerce towards different business sectors in Malaysia, nevertheless business in Malaysia still shows low e-commerce adoption due to various issues including TOE issues (Mohamad & Ismail, 2009; Alam & Ahsan, 2007; Andam, 2003). Issues include technology adoption, managerial support and policies and legislation (Mohamad & Ismail, 2009) are some of the main issues under the TOE scopes.

E-commerce has always been known to provide less expensive ways to search and buy products compared to the traditional retailer. Sage (2009) also reported that, based on Forrester Research's five-year e-commerce forecast in USA, e-commerce is expected to make a comeback in the year 2010 with predicted growth of 13% in the forecast. This will certainly impact the world's e-commerce scenario, including the Malaysian e-commerce market. While facing all these crises, the e-commerce has to withstand and evolve to become a more dynamic, global and highly profitable business. E-commerce pioneers have become e-commerce giants and are dominant within the e-commerce scope, such as Yahoo!, Amazon.com and Ebay (Economist, 2003).

According to the Malaysia Communication Multimedia Commission (MCMC), in 2008, there was a significant increase of use of the Internet in the financial activities as compared to the previous year. There was also a moving trend to use the Internet for online stock trading and

e-government services from the year 2006 to 2008. This statistic shows healthy improvement of Internet usage, thus marking a good identification of the importance of being online. Besides the increased of usage in Malaysia, the same trend was observed in the Association of South-east Asian Nations (ASEAN). An average of 3.1% purchases per person was made in Asia Pacific (APAC) alone in the second quarter of 2008 (MasterCard, 2008). The same statistic shows an average of USD 601.90 total online spending over the past three months in APAC. According to the Internet Stats (Stats, 2011), the estimated number of population in Asia in 2010 is 3,879,740,877 persons, consisting of 56% of the world population. If the estimated number of population in APAC in the year 2008 is half, predicted to be about 1.5 billion, the total online spending of APAC alone is tremendous. It is also predicted that 47% of respondents are likely to make an online purchases in the next six months. This statistic by MasterCard was conducted for the second quarter of 2008. Counting that the number of average online spending in APAC has increased due to the diagonal increase of the Internet usage, the total online spending in years to come will be immense. The APAC statistics covers countries including Japan, Singapore, Australia, Korea, India and China.

As for Malaysia, online spending statistics, the Malaysia local newspaper reported in 2010 itself, Malaysian has spent total of RM 1.8 billion on online purchases. The newspaper also reported that the figure is expected to almost triple in three years, according to a Nielsen Company study. Malaysians spend more on local website with transactions worth RM825mil, compared with foreign websites which only recorded RM627mil in receipts, as reported by (TheStar, 2011). The Wong (2013) also reported in 2012, there are 65% majority of Malaysia internet users buying products online, where purchases include from clothing and accessories to toys and baby products. Many Malaysians also prefer to shop at famous shopping platforms includ-

ing the Groupon, eBay and trusted retail websites. The same report also shows that it only takes 1-2 hours for 29% of the total number of internet purchasers in Malaysia to transact online, which proves that online purchasing is not time consuming. Based on these statistics, we could conclude that the e-commerce business is significant and acts as an important platform for businesses to venture into. This is because with the proliferation of technology and the Internet, consumers are highly dependent on this technology to get update and feedback which provides the concluding to online purchase.

2.4.3 The need for ISSM Maturity Model for the Small Businesses

There are immense profits and advantages of online businesses based on the online spending statistical result by MasterCard and other related academic literature such as (Mohamad & Ismail, 2009; Alam & Ahsan, 2007; Andam, 2003) and other substantial online reports Wong (2013); TheStar (2011). Report from MasterCard also shows that one of the most important reasons of not wanting to do online shopping is the security concern. Besides security concern, there are two other reasons, which are the preference of physical purchasing and additional online handing charges Wong (2013); MasterCard (2008). However, security concerns is the top concern in APAC countries including India, Thailand, Hong Kong and China MasterCard (2008). As Malaysia is included in the APAC countries list, security concern has been becoming one of the crucial concerns of business and users, thus deterring many customers from purchasing online. Security has become a major hindrance which was highlighted and discussed by (Mansor & Amri, 2010; Ainin & Noor Ismawati, 2003; Zakaria & Hashim, 2003; Paynter & Lim, 2001) for businesses in Malaysia. (Alam & Ahsan, 2007) also asserted the security/confidentiality factor as a major inhibitor of e-commerce adoption by the business in Malaysia. The security issues may include issues such as trust towards the banks of transactions, clear

and understandable instructions, security of Internet transaction and the length of Internet experience as asserted by Sohail (2003). As security has become a major factor across different types of industries in Malaysian businesses, similar issues are found to be critical issues to the SMI/E in Malaysia (Mansor & Amri, 2010; Zakaria & Hashim, 2003; Ainin & Noor Ismawati, 2003) as this SMI/E has few resources and little experience in security matters.

As asserted in the previous discussions, standards currently are designed based on the hierarchical business, where emphasis on e-commerce in small business is rarely the case. In addition to that, these small businesses which are involved with e-commerce face the same risks as those faced by the hierarchical businesses because perpetrators do not distinguish big or small business. Due to this reason, a simple and practical ISSM solution is required to assist these businesses to achieve the intended ISSM to secure business. As the fourth wave of ISSM perspective focuses on security governance in a business, a practical method is required to address this issue. The ISSM maturity framework is seen to be the best solution as it provides the level of security management implementation and security management exercise required, compared to other ISSM standards available in the market. The ISSM maturity framework provides tools to assess the security management level in a business. Businesses could also performed self-assessment on their security management performance.

2.5 Summary

The purpose of the literature review is to understand the ISSM and its importance in the SMI/E, especially to the SMI/Es which are conducting e-commerce. This literature review is also conducted to seek factors which are related to the ISSM effectiveness, leading to the ISSM maturity. Besides, it is also important for this research to conduct this literature review to understand

the ISSM maturity concepts and practices currently used in to achieved ISSM maturity by businesses. Past researches were reviewed and analysed to help investigate the issues of ISSM. Current standard and framework are also analysed to help determine the socio-technical factors involved, and those which are vital to achieve ISSM maturity. Through the investigation, the researcher is able to identify factors influencing ISSM effectiveness which led to the ISSM maturity of a business. The literature analysis also revealed that ISSM is important in business including SMI/E involved in the e-commerce.

The review continues with the understanding of ISSM maturity towards a business. The ISSM maturity concept and practices are analysed to find the advantages towards these businesses. Unfortunately, there are very small empirical literatures pertaining to ISSM maturity in the e-commerce. Many of these ISSM maturity frameworks were design to address issues in the hierarchical business, thus limited sources were available to address the small business requirement in this field. As the ISSM perspective of the fourth wave focuses on the security management governance, ISSM maturity concept has become one of the most popular ISSM implementations in many businesses. Regrettably, there is no simple models or solutions that address the SMI/E with e-commerce concern appropriately. The literature then continues to analyse the relationship of ISSM success and effectiveness with ISSM maturity factors. It is revealed through the literature review that the socio-technical factors could predict the ISSM maturity of a business. A theoretical representation is then designed to assist this research.

Finally, the analysis also discovered that in Malaysia, the SMI/Es contribute to the annual income positively and e-commerce have become one of the tools to increase productivity of these businesses. As such, ISSM is highly required in these businesses. Although there are limited

articles explaining the real situation of ISSM in e-commerce in Malaysia, the Internet and e-commerce has become one of the most popular tools for business and communication currently. The high usage of Internet in Malaysia increases the concern of securing business online to ensure the business and its assets are appropriately protected.

CHAPTER 3

RESEARCH FRAMEWORK

3.1 Introduction

This chapter discusses the research conceptual framework for the study. The framework proposes the main dimension of ISSM for the SMI/E business, based on the findings gathered from the literature review in Chapter 2. The conceptual framework is important and acts as a guide in a research, in which propositions summarize explanations and predictions (Webster & Watson, 2002). This conceptual framework serves to guide this study in the research investigation processes, especially in the development of research instruments for both quantitative and qualitative data collection discussed in Chapter 4. The conceptual framework also determines types of the data analysis approach required for analysis purpose. In this chapter, the first discussion will look into the issues of the theoretical grounding the conceptual framework. Here, the discussion will focus on the issues of aspects, premises and assumptions of the study. Secondly, the variables underlying the framework will be discussed and considered. The discussion will also define the relationship between the values of the defined aspects and the premises. Next, we will determine the relationship involves in the conceptual framework, and finally, design and develop the conceptual framework based on the theoretical/empirical underpinnings of the relationship. This chapter will conclude with the concluding remark and where the summary is presented. Determining maturity factors in ISSM is important as it provides helpful indication of the essential security management practices required in a business. The maturity indication will be able to provide these businesses with the current business ISSM status, and further identify improvement criteria for the business, hence be successful in their

secured e-commerce business. Consequently, from this determination, e-commerce business could invest in the required and specific ISSM practices, feasible with business objectives. Thus, only the required resources are used and utilized without dissipation. Besides that, the maturity factor determination will be a good benchmark for the SMI/E to determine the most suitable ISSM for each business.

3.2 The Information Systems Security Management (ISSM) Maturity Conceptual Framework

In the context of ISSM maturity study, the research must clearly consider what determines ISSM maturity of a defined business. ISSM maturity essentially defines the full development of security management (SM) of a business. Full development here does not only refer to implementation of ISSM but the exercise and the effectiveness of the ISSM of a specific business context through a period of time. Hence, in order to build the ISSM research conceptual framework, three important aspects are determined to be important from the literature reviews, which are the technology, organization and environment (TOE). However, through the standards analysis from the literature, these three aspects cannot exist independently as business are dynamic in nature. Standards highlight the position of TOE for example in Carnegie-Mellon (1999), to assess business ISSM maturity, the business must address combinations of TOE issues in the process area determined. Generally the attributes of the TOE have already been identified in Chapter 2 as referred in 2.8. Table 2.8 shows the attributes of TOE and the related theories which highlighted the determined attributes through the literature review. The attributes are classified generally under TOE without clear relationships between these attributes. However, from the literature review, the research predicted a simple relationship between TOE in achieving ISSM maturity. As ISSM maturity is influence by TOE, simple direct relationships are

depicted in Figure 3.1.

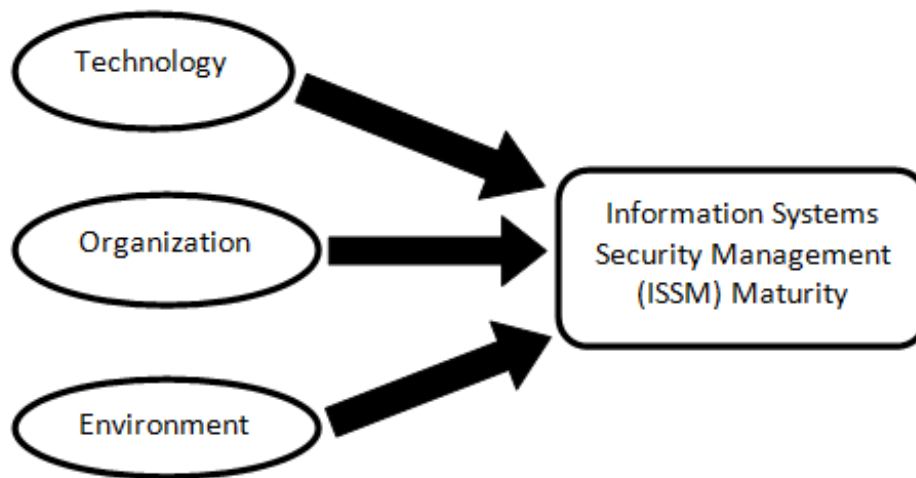


Figure 3.1: Relationship of TOE elements to ISSM Maturity

3.2.1 The ISSM Maturity Independent, Mediating and Dependent Factors

3.2.1 (a) The ISSM Maturity Independent Factors

Conversely, this simple relationship in Figure 3.1 cannot provide a clear relationship of the identified factors to explain the ISSM maturity phenomena in the SMI/E. Literature review shows that TOE elements influence the ISSM maturity as referred in Table 2.10 page 53. The independent factors identified in the literature review are derived with the organization factors (which are the business type, size and top management support) (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) and business length (Prananto et al., 2003a, 2003b). These factors are identified to independently influence ISSM maturity. The business length, business type and business size in this research is considered as formative constructs as changes in the formative measures can cause changes in the underlying construct (Petter, Straub, & Rai, 2007; Diamantopoulos & Sigauw, 2006; Jarvis, MacKenzie, & Podsakoff, 2003). This means if the business type, size and length is address with other

measures/indicators the construct will not bring any meaning to the whole framework. In the independent factors, the top management support cannot directly be addressed by one indicator, hence this factors required representation. In this research, the top management support is represented as any issues on this matter is related to (i) IS security-related meetings, (ii) IS security-related decisions, (iii) monitoring IS security-related activities and (iv) support on IS security-related functions as discussed in Chapter 2. The top management support is a reflective construct requires few indicator to address top management support issues. As asserted by Petter et al. (2007); MacCallum and Browne (1993) a reflective constructs must have observed measures that are affected by an underlying unobservable construct. The remaining issues under the TOE mediates the independent factors to achieve ISSM maturity. This condition is discussed in Chapter 2 where the categorization is depicted in Table 2.10. For instance, the organization factors have direct and positive relations towards ISSM maturity, however to achieve ISSM maturity, organization factors are not enough. The business has to exercise SM practices and policies to mature in the business ISSM exercise. Hence, this research predicted that in order for business to reach its ISSM maturity, mediating factors are required to stimulate the businesses. The independent factors are depicted in Figure 3.2.

3.2.1 (b) The ISSM Maturity Mediating Factors

As mentioned in Chapter 2, a review of 3 selected standards shows remaining items under each TOE elements are classified similarly to the item mentioned in the ISSM standards. In this research, it is grouped as SM practices. The TOE elements includes technology usage and structure, organization involves the business purpose, value and utilization of SM, and finally the environment which consists of support and stimuli. All these mediating factors represent the SM practices happening in a business. For example: (i) support-from supplies and tech-

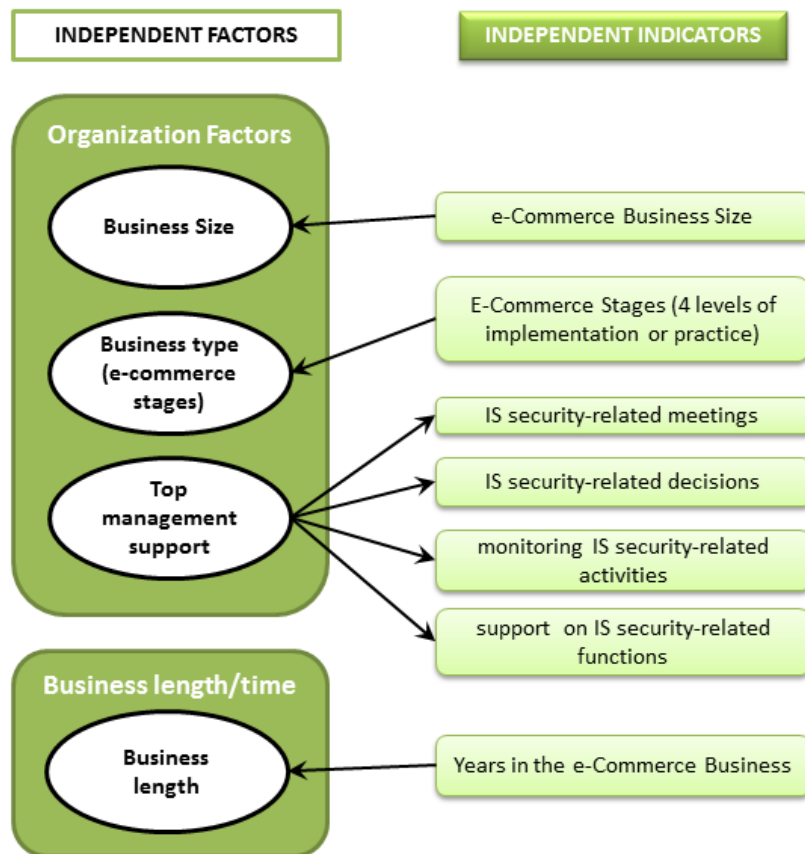


Figure 3.2: Independent factors for ISSM Maturity

nology updates, (ii) usage- types and level of SM being exercised, carried out or implemented as part of workflow in a business, (iii) value- the ISSM perception of the CEO/owners for the business, (iv) purpose – the main aim of having ISSM and (v) communication structure- technology usage, status and implementation involved in a business. Table 2.10 in Chapter 2 also describes the TOE classification of the independent and mediating factors influencing ISSM Maturity in this research. Hence, as referred to in Table 2.10 descriptions, the mediating factors are depicted in Figure 3.3 below.

The representation of mediating factors as in Figure 3.3 shows the research relates the ISSM theoretical attributes with the aspect of SM to build the research framework. The very right of the figure show ISSM theoretical attributes derived from the literature review, standard compar-

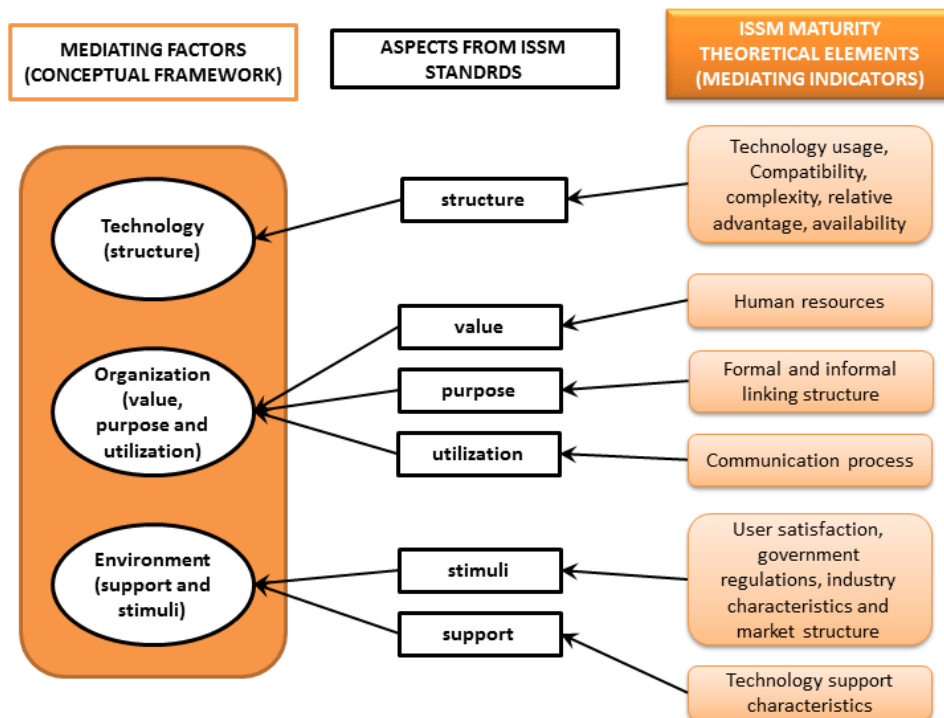


Figure 3.3: Mediating factors for ISSM Maturity

isons and theory discussions. These attributes reflect the issues of importance encompassing discussions made in Chapter 2. The issues of importance as described in Table 2.10 is then organized and premised based on the SM standards task. This is done because this research assumed that to achieve the ISSM Maturity, SM practice has to mediate the independent factors. Without SM practices, which is usually based on ISSM standards, a business will not achieve the optimum ISSM mature status. Sequentially, these SM aspects become the themes to represent the important elements of TOE. Seven aspects have been derived based from the SM standards comparison in Chapter 2. There are (i) usage, (ii) structure, (iii) value, (iv) purpose, (v) utilization, (vi) support and (vii) stimuli. All these aspects are representing attributes that the researcher needs to investigate to determine the ISSM maturity of the business. The researcher predicts that to achieve ISSM maturity a business, it must be ensured that the socio-technical factors (TOE) have factor inter-relation with high business forces or dynamics where it relates in optimum. Independently, these factors will not affect the business ISSM maturity.

3.2.1 (c) The ISSM Maturity Dependent Factor

Following the simple relationship determine in Figure 3.1 and the determination of mediating factors as Figure 3.3, this research depicts the independent and mediating factors representation towards the ISSM Maturity as presented in Figure 3.5. In this figure, there are independent segment depicted as Figure 3.2 , mediation segment as as Figure 3.3 and dependent segment as Figure 3.4. The independent segment consists of four independent factors (business size, business type, top management support and business length), three mediation factors (technology, organization and environment) and finally the dependent factor which is the ISSM Maturity. The dependent factor refers to the ISSM maturity which is represented by two important variables which are the security measurement presence and the security management awareness and risk towards business.

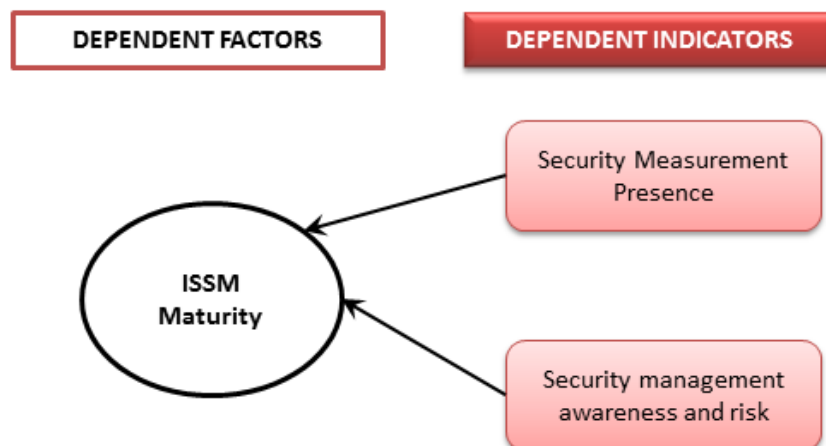


Figure 3.4: Dependent factors for ISSM Maturity

Figure 3.5 clearly shows the factors influencing ISSM Maturity. Now it is important for the research to design the relationship between these factors based on the discussion from Chapter 2. These relationships are hypothetical as they are highly based on literature review of selected

articles, standards and theories conducted in the previous chapter. Based on literature review, assumptions were deduced, hence constructing the hypotheses.

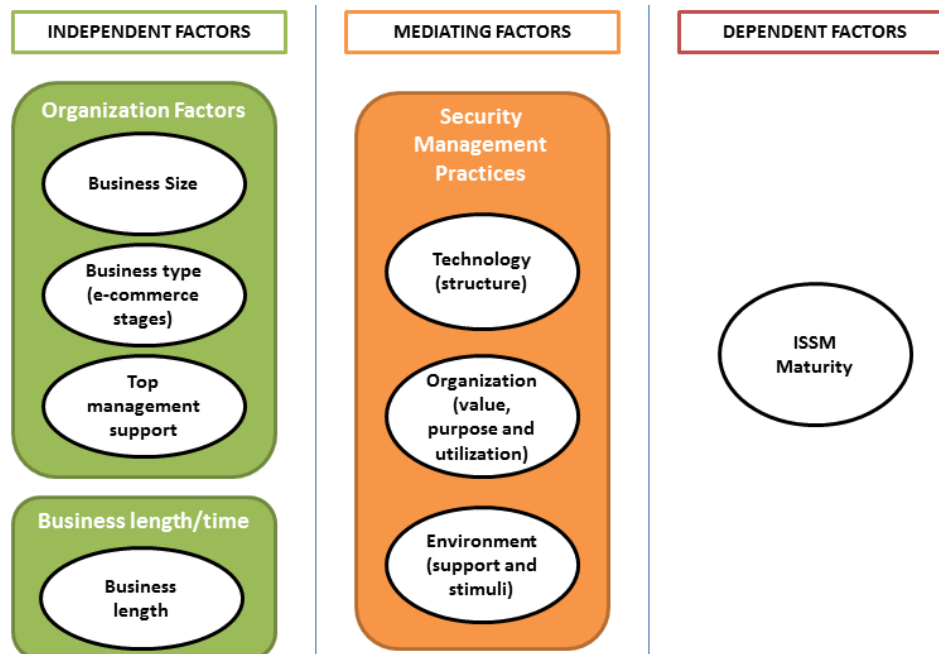


Figure 3.5: Independent and mediating factors for ISSM Maturity

3.2.2 Research Hypotheses

Many big organizations do not practice security management due to various reasons. Straub (1990) asserts that big organizations which have been in business for several years may have problems like legacy and awareness issues in implementing security management. It is common for big businesses to have old IS system using legacy technology which is no longer current with the available IS technology. Also, these legacy systems may have problems in upgrading due to compatibility issues. However, it is still widely used in the business task and process. Here, we assume that the longer the business, the SM may involve through SM practice due to the technology difference and complexity. Besides, Prananto et al. (2003a, 2003b) mentioned that for e-commerce to mature, time plays an important role as business developed and practice better improvement towards the business through time. Thus, we assume that

business length has to have a positive relationship to the SM practices, hence ISSM maturity is achieved. Therefore, our first hypothesis defines:

H1a- Business length is related to Technology factors of security management practices;

H1b- Business length is related to Organization factors of security management practices; and

H1c- Business length is related to Environment factors of security management practices.

Werlinger et al. (2009); Kraemer et al. (2009); Barlette and Fomin (2008); Fomin and Vries (2008); Zuccato (2007); Chang and Ho (2006); Zhuang and Lederer (2004) asserted in their research, the business size, business type and top management support are major influence in ISSM implementation and effectiveness. Literature review has also concluded that without organization factors (three factors mentioned above), a business will not achieve the desired ISSM required as there business size is too small for ISSM implementation, the business type is not a critically business type (non-financial related business, minimal online transactions process in executing business task) and that the top management is not aware of the consequence of not practicing ISSM effectively (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003). Similarly, these factors should influence ISSM maturity as a business must be successful in its SM practices before it becomes mature. For the context of this research, the researcher assumed that business size, business type and the top management support factors influence SM practices, hence influence ISSM Maturity. As such the second (H2a-H2c), third (H3a-H3c) and fourth (H4a-H4c) hypotheses are developed based on this discussion. The hypotheses are:

H2a- Business size is related to Technology factors of security management practices;

H2b- Business size is related to Organization factors of security management practices; and

H2c- Business size is related to Environment factors of security management practices.

H3a- Business type or e-Commerce stage is related to Technology factors of security management practices;

H3b- Business type or e-Commerce stage is related to Organization factors of security management practices; and

H3c- Business type or e-Commerce stage is related to Environment factors of security management practices.

H4a- Top management support is related to Technology factors of security management practices;

H4b- Top management support is related to Organization factors of security management practices; and

H4c- Top management support is related to Environment factors of security management practices.

From the discussion in Chapter 2, the ISSM standards and model selected show a high relationship towards ISSM Maturity. This is because aspects in SM Practices are aspects found in the ISSM standards. To achieve effective ISSM, a business must adhere to the standard recommendations which are mentioned according to some of the aspects derived through the researcher's understanding of the standards comparisons. The respective ISSM maturity framework (Aceituno, 2006a; Carnegie-Mellon, 1999; Stacey, 1996; Murine & Carpenter, 1984) clearly shows that SM practices are related to the ISSM maturity. The ISSM standards and model asserted that without security management practices, an organization will not achieve ISSM maturity at any point of the business. For example in Stacey (1996), it is mentioned that the aspect of SM consists of management of understanding and attitude, security orga-

nization status, incident handling, security economics and security improvement actions representing the usage, structure, value, purpose, support and stimuli. It is also mentioned by Carnegie-Mellon (1999) that the same aspect of SM is found in the standards for example security control administrations, control and monitor technical effort (under usage, utilization and structure), ensure quality and coordinate with suppliers (represent support and stimuli) and also provision of ongoing skills and knowledge (representing value and purpose). All these aspects are required towards the ISSM maturity of the business. Hence, this research deduces the fifth hypotheses as:

H5a- Technology factors are related to ISSM maturity;

H5b- Organization factors are related to ISSM maturity; and

H5c- Environment factors are related to ISSM maturity.

Based on the first hypothesis discussion, it has mentioned that the length of time in the business towards ISSM maturity is important. In Prananto et al. (2003a, 2003b), time influences the e-commerce maturity of SMI/Es in Australia. As e-commerce advances, the security management in e-commerce will undergo changes, hence improvement is achieved, thus the level of maturity will be achieved. Similar to the scenario above, for a business to achieve its ISSM maturity, business length/time factor play a role to achieve ISSM maturity. Hence the sixth hypothesis is derived as:

H6- Business length is related to ISSM Maturity

The organization factors determine its security management practices in order to achieve ISSM maturity. Standards and the ISSM maturity standards and framework discussed in Chapter 2 emphasized the important organization factors to foster effective information security, thus

achieving maturity (ISO/IEC, 2008; Aceituno, 2006a; ISF, 2003; Carnegie-Mellon, 1999; Murine & Carpenter, 1984). Business types, business size and top management supports are factors that highly influence a business to adhere to the ISSM standards. This is because with these characteristics, the business will understand the type of SM practices required. With appropriate security measure, it will lower the business risks, especially the SMI/E businesses involved in e-commerce. Thus, the researcher has concluded that for a business to achieve ISSM maturity, organization factors (which include business types, business size and top management support) directly affect ISSM maturity with appropriate SM practices. *H7- Business Size is related to ISSM Maturity*

H8- Business Type or E-commerce stage is related to ISSM Maturity

H9- Top management support is related to ISSM Maturity

Closely following to the discussion in Chapter 2, this study has derived a conceptual framework for this research. The relationships of these factors are based on the literature review assumption as discussed above. The conceptual research framework for the ISSM Maturity is depicted in Figure 3.6.

Based on this relationship, the researcher will be able to design the research method to carry out research investigations. The determination of all the independent and mediating factors and dependent factor will be assessed through the quantitative investigation. In understanding the relationship of all these factors, the researcher will conduct a qualitative investigation. The in-depth qualitative investigation is important as it will provide further understanding and information to address the ISSM maturity phenomena in the SMI/Es. The researcher will be able to determine and demonstrate factors relationship and its dynamics in the selected SMI/Es.

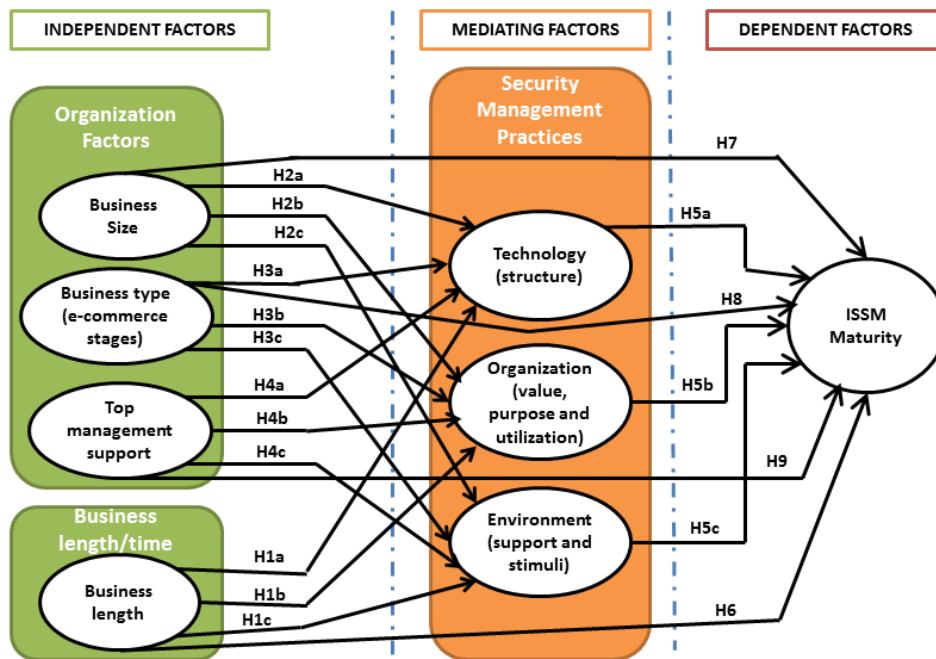


Figure 3.6: Research Conceptual Framework for ISSM Maturity

The researcher has also predicted an inter-relation of identified factors and issues on business dynamics which will influence the ISSM maturity in a business.

3.3 Summary

This chapter concludes the research conceptual framework designed to assist the research in carrying out its research investigation. The conceptual framework is predicted using selected IS theories, framework and model, as represented in the theoretical model of ISSM maturity in Chapter 2. The relationship as depicted in Figure 3.6 consisted of attributes in Table 2.10. The Table 2.10 was derived based on the discussion in Chapter 2, representing the socio-technical factors effecting ISSM Maturity. This chapter concluded nine hypotheses derived based on the assumption from Chapter 2. Sequentially from Chapter 3, Chapter 4 will discuss the research method conducted in details based on the conceptual framework designed from this chapter. The research framework will provide a blueprint for the research methodology to carry out

research investigation accordingly. Analysis of the results from the data collection will be presented in Chapter 5. Following that, a conclusion and discussion of the findings will be carried out in the final chapter.

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Introduction

The research methodology adopted in this research is the mixed-method research. This method employs more than one research method in a research (Greene, Caracelli, & Graham, 1989; Mingers, 2001), which are the quantitative and qualitative methods. The main purpose of selecting the mixed-method research is to enable the research to use multiple approaches to research the phenomena using multiple data collection techniques (Trauth & Jessup, 2000), and hence provide richness of data, in order to understand the phenomena (Petter & Gallivan, 2004).

A methodology is a structured set of guidelines or activities to assist the undertaking of a research or intervention (Mingers & Brocklesby, 1997). A mixed methodology has the ability to provide a holistic approach in dealing with the richness of the real world (Mingers & Brocklesby, 1997). It also allows and assists the researcher to use different interventions throughout the various stages of the research. A mix methodology involves five different approaches, which are triangulation, complementary, development, initiation and expansion. This research uses the complementary approaches with the purpose to seek elaboration, enhancement, illustration and clarification of the results from one method with the results from the other methods, (measure overlapping but different facets of a phenomenon, yielding an enriched, elaborated understanding of that phenomenon) (Greene et al., 1989).

The task to select the most appropriate method is an important research requirement. The first

criterion when choosing the mix methodology research approaches is due to the need for the research to understand the different dimensions of the real situation of the phenomena. This is important because there were limited reading on these issues, especially involving the SMI/E with e-commerce. As research requires the involvement of the CEO, higher management and the owner of the business, a diverse method is the best way to capture the respondent's experience and insightful views of the issues. A single quantitative method would only provide the factors involved in ISSM Maturity. However by using mix methodology research will be able to capture in-depth ISSM views from the participating CEOs of selected companies. The limited number of CEOs of SMI/Es in e-commerce also brings us to limited access towards data. Thus, a diverse intervention has to be strategically deployed to ensure full use of reachable respondents. The complementary mixed-method is chosen as it fulfils the research objectives and purposes. Results from quantitative investigation in phase 1 are complemented by qualitative investigation of phase 2. Through this method, the research is able to acquire enriched and elaborated understanding of the studied phenomena.

Through the complementary mixed-method, the researcher is obliged to determine the sequence of investigation carried out. This research has chosen to conduct the sequential mixed-method (complementary) as it is less complicated and the researcher is comfortable in conducting both methods for this research. Besides, this sequential research is the most suitable design to address the issues analytically. In the sequential mixed-method (complementary) design, the research will collect and analyse the quantitative data first, followed by the qualitative data in two consecutive phases within one research (Ivankova, Creswell, & Stick, 2006). In the sequential explanatory design, the second qualitative phase was built based on the first quantitative phase. These two phases are connected in the intermediate stage of the research. The rationale for this

approach is that the quantitative data and their subsequent analysis provide a general understanding of the research problem (Ivankova et al., 2006). In sequential explanatory design, the qualitative data and their analysis is refined, and will be able to explain the statistical results, by exploring participants' views in more depth (Creswell & Clark, 2007; Tashakkori & Teddlie, 1998). Figure 4.1 depicts the ISSM maturity research method.

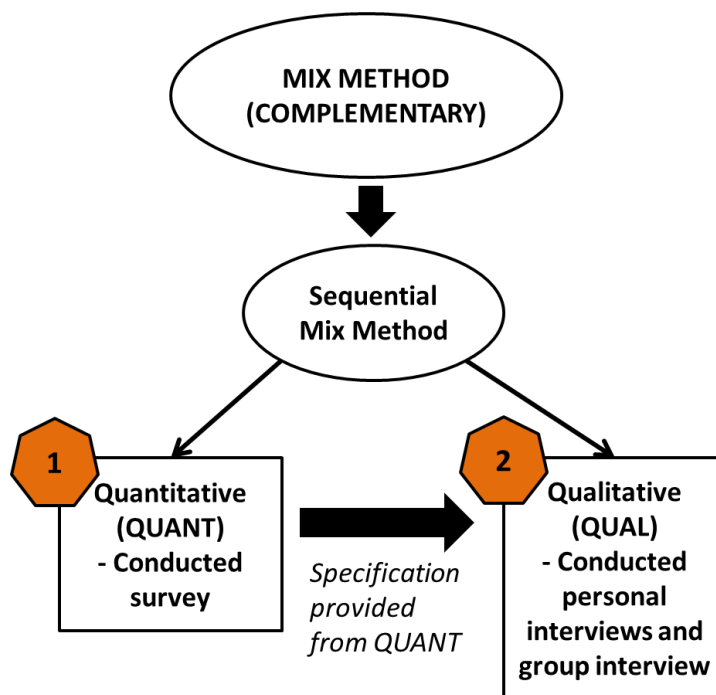


Figure 4.1: ISSM maturity research method

The complementary approach is the best method to address the current research phenomena as complementary approach purpose seeks to elaborate, enhance, illustrate and clarify of results from one method with the results from other method. It is the same aim of the researcher to address and research the ISSM maturity phenomena in the SMI/E e-commerce in Malaysia. There other mixed-method investigations such as mentioned by Greene et al. (1989) which are the (i) triangulation, (ii) development, (iii) initiation and (iv) expansion have different purposes which are are not appropriate to help the researcher in addressing the research questions and objectives. The triangulation purpose concentrates on finding validity of constructs by using different

method of investigation. Triangulation seek to converge, corroborate and correspond of result from different methods, which this is not the main focus of the research. As for the development approach, this method seeks to use result from one method to develop or inform other methods to increase validity of constructs. The initiation approach is used to increase breadth and depth of inquiry result, where it seeks to discover paradox and contradictions from one method with questions or results from other methods. Finally the expansion approach is conducted to increase the scope of inquiry, to extend the breadth and range of inquiry using different methods for different inquiry components. Hence from the discussion of the mixed-method approaches (besides the complementary approach), the researcher has chosen the complementary approach as the method to conduct this research, which is the closest research method that can help to answer the research questions and objective.

4.2 Procedural Issues in the Mixed-Methods Sequential Explanatory Design

As the researcher selected a mixed-method research methodology, there are a few important aspects of mixed-method approaches that require consideration. The issue of priority (Creswell & Clark, 2007; Ivankova et al., 2006), implementation (Creswell & Clark, 2007; Ivankova et al., 2006; Greene et al., 1989), and integration (Creswell & Clark, 2007; Ivankova et al., 2006; Greene et al., 1989; Tashakkori & Teddlie, 1998) of the quantitative and qualitative approaches must be understood and dealt with appropriately. This is because the researcher needs to establish whether quantitative or qualitative (or both) methods had more emphasis than the other. These three important issues could assist the researcher to understand the sequence of the method and the analysis of data. It also helps to determine at which point of the research the mixing of both methods actually occurs.

4.2.1 Priority

This research prioritizes the quantitative research as compared to the qualitative. As this research requires to develop the ISSM maturity model, it is important for the researcher to identify the factors influencing the ISSM maturity first. As asserted by Kaplan and Duchon (1988), the goal of the whole research will determine whether the qualitative research is given more priority as compared to the quantitative research. In this case the quantitative research is priority as the researcher need to identify ISSM factors before understand the relationship of factors to develop the ISSM maturity model. In Morgan (1998), it was asserted that a smaller quantitative research precedes the qualitative research which serves to guide data collection by informing theoretical sampling or establishing preliminary results to be pursued in-depth. There is no specific theoretical perspective which could explain the phenomena appropriately. The researcher is required to predict the conceptual framework based on collection of appropriate theory to answer the research goal (Creswell & Clark, 2007).

4.2.2 Implementation

Implementation in mixed-method research refers to the sequence used by the researcher to collect data (Creswell & Clark, 2007; Ivankova et al., 2006). In this research, the quantitative data collection is conducted first, followed by the qualitative data collection. The goal of the quantitative approach was to determine the ISSM maturity factors in Malaysian SMI/E with e-commerce. Besides that, through this method, the researcher will be able to select participants for the next qualitative phase. The qualitative phase explores in-depth issues on ISSM maturity. The quantitative results gathered from the first phase help provide a general understanding of the factors relationships. As for the analysis of the qualitative phase, it explained further the relationships between factors. As for the qualitative results, it complements the result gathered

in the first phase, thus enriches the result analysed from the quantitative phase. Conclusively, the quantitative investigation addresses research question 1 which directly answers objective 1 and part of objective 2 of the research. The qualitative investigation strengthens the findings of quantitative investigation by answering the research 2 and the objective 2 of this research.

4.2.3 Integration

Integration refers to the stage where the process of mixing quantitative and qualitative methods during the process of the research inquiry occurs (Creswell & Clark, 2007; Ivankova et al., 2006; Greene et al., 1989). The integration happens during the intermediate stage, during the data collection process, data interpretation and discussion. Here, the researcher connects two approaches using the participants' selections. The researcher will select participants for the qualitative follow-up, based on the results gathered after the quantitative phase (Creswell & Clark, 2007). The integration also occurred through the development of the qualitative data collection protocol. The qualitative interview questions were formulated based on the results gathered from the quantitative phase. The researcher has also mixed the quantitative and qualitative approaches at the research design stage by developing quantitative and qualitative research questions. The quantitative and qualitative results are integrated during the interpretation and reflection of the outcomes for the entire research (Creswell & Clark, 2007). As a result of the analysis integration, the objective 3 and the research question 3 is answered. Hence, it is important for this research to carry out the mixed-method research as it is required to answer all three objectives determined in this research.

4.3 Introduction of the research

The research involves quantitative and qualitative data collection provided using the business contacts available in three organizations, two of which involved in this research have official collaborations, through a Memorandum of Understanding (MoU) and Memorandum of Agreement (MoA) between the researcher's university with the Organization A and the researcher's university with the Organization B. The main objective of involving three organizations is particularly due to many expected problems which often occur in research involving information security of a business as asserted by (Kotulic & Clark, 2004). One common and expected problem in the field research is making contact and creating relationships. By bonding the relationship through official collaboration, the researcher will be able to have smooth and ethical access towards the respondents' data. Hence, this will increase the reliability of the data gathered. The collaboration also promised active participation and assistance to reach respondents, thus creating research productivity. Relationships with two organizations (with which the research have official collaboration) were good and active during this research. However, the organization has no authority to control feedback from their business contacts available in their databases. This is because each company has its own business policies in participating in an academic research. Besides cooperation and assistance, it is of utmost importance for this research to generate official collaborations due to the sensitivity of the issues being researched, and where it involves the organizations' business practices.

4.4 The Selection of research

This research has carried out a purposive sampling technique in terms of respondents for the research. Besides, a mixed-method research technique requires the researcher to be creative in gathering appropriate respondents because Myers and Newman (2007) mentioned many prob-

lems and pitfalls in qualitative interviews, especially on the issues of having good connection with the participants, lack of trust, level of entry and elite bias. Through research collaboration, contacts and networking were created. Hence, it is easier for the researcher to gather responses from business participants. With this positive relationship and understanding, trust is easily built. The entry level of contact problem is also another main concern of this research. This is because the research conducted quantitative and qualitative investigation on the highest business level only. In a common field research scenario, most researchers create relationships with the lower level of the officers in a specific organization. This is again why collaboration is highly required. Through collaboration, the researcher will have access to the champion in the organization; hence ensuring that the research effectively. The elite bias issue is no longer an issue in this research as the research requires the most appropriate person in charge to define and describe the situation of the business in the issues of ISSM implementations, and ISSM maturity faced by the business.

4.5 The Selected research

This section describes three involved organizations which have provided the business contacts to be come the respondents of this research. These business contacts are compiled in the involved Organization A, B and C business contact databases.

4.5.1 Organization A

The Organization A is a statutory body linked to the Ministry of Trade and Industry Ministry of International Trade and Industry (MITI) in Malaysia. This organization was established in the year 1962, as a joint project between the United Nations Special Fund and the Malaysian Federal Government. Organization A has passed through many phases of organizational changes

until the most recent change in February 2008, this body is officially known as Organization A, a statutory body under the MITI remaining as a corporation under the Incorporated Act 1966 (Amended in 2008).

The mission of organization A is to provide high impact service towards businesses in Malaysia to achieve their performance excellence through any type of business innovation. This body is committed to provide value-added information pertaining to productivity, quality, competitiveness and best practices to the required businesses through their research activities. Organization A is also dedicated to assist in developing highly knowledgeable human capital and organizational excellence through their robust training, system development and best practices. Organization A invites innovative and creative cultures among their business participants via smart partnership programmes. Organization A is also active in providing quality publications for the reference of business partners and researchers, as part of their objective to transform the business practice in Malaysia to be more innovative, which are in line with the Prime Minister's objective, which is to create a productive and innovative businesses and prepare these businesses towards the global competition.

The Organization A consists of the Board of Directors. The Director General is the head of the office. There are eight departments in in the organization, where five are the departments involved in the core business services provided by Organization A to their users. The remaining departments oversee the internal needs of the business, for example the human resources department, management and service department, finally the strategic planning and corporate communication departments.

The department which is involved with this research is a department involved with electronic service solutions for service innovation. The head of the group from Organization A, has agreed to champion this research as they have similar research interests, which is to understand the issues businesses are facing in e-commerce which include the ISSM. In this research collaboration, Organization A agreed to share their available database, based on their previous research which they have conducted with e-commerce businesses in Malaysia. The databases they have are from their access to the Ministry of International Trade and Industry, Malaysia. Organization A also agreed to assist the research in the survey distribution using their mailing system. By doing such a task, Organization A had hoped that the survey returns would be more effective as they had already created a good rapport between these businesses compared to the researcher. The researcher of this research was responsible for the creation of the survey instrument and research design to carry out the research. The researcher was also responsible for data analysis and reporting research findings for the benefit of both parties. Research findings were reported to Organization A, once the research analysis was completed. With this collaboration, the data collected were more reliable and the data collection process would be more effective due to the high level of trust among the business contacts towards Organization A.

4.5.2 Organization B

Organization B is a non-government organization established in September 2003. Organization B champions the right in business owners and professionals among specific entrepreneurs in Malaysia. This association comprises members from new and experienced entrepreneurs and professionals in Malaysia. The main aim of Organization B is to create synergy and employ strategies to facilitate a continuous and successful development of the business owners. Organization B is also determined to promote a culture of business excellence among its members,

thus emphasizes on making significant impacts in the dynamic and challenging global market and economy by leveraging their expertise and knowledge among members. It is the responsibility of the senior members to share and promote sound business education by introducing solid fundamentals of a business and insightful business knowledge with their vast practical experience towards the members. It is also a requirement for new business members who are experts in the technology and new media to introduce this idea to the rest of the members for the benefit of all in the Organization B.

Organization B is also playing an active role in voicing up their concerns and issues to the authoritative body in order to improve the current support delivery system provided by the government to support entrepreneurs like them. The body is dedicated to have an active role in championing the efforts of government in creating policies to support their business to be in line with the globalization era. This non-profit organization's vision specifically caters to Bumiputera (the Malay race and the indigenous people of Malaysia) entrepreneurs. This organization encourages dynamic networks between entrepreneurs and professionals and promotes technology adoption amongst its members for the benefit of their businesses.

The initiation of contact to this association was created due to the snowballing process which the researcher has conducted from the initial research investigation. The initial meeting was conducted between the researcher and the head of the bureau of learning and development, where a small group interview was suggested to be conducted for the sequence of the research. The opportunity to conduct a sequence to the earlier research investigation was expected, because the researcher has tried to bridge a few themes with the conceptual framework which was mentioned through the previous research investigation. The small group interview involved

16 CEOs from the service and product businesses from the SMI/Es. All the participants have agreed to take part in the interview conducted in this research. Organization B signed a formal document of understanding due to the highly sensitive issues which will be discussed in this research investigation. By having the understanding, both parties have gained each other's trust and hence a reliable research environment will be created due to the element of trust among all involved parties.

4.5.3 Organization C

The last database was provided by Organization C. No formal relationship was created as the database of SMI/E contacts is available online and anyone is free to download the information from Organization C's secured website.

Organization C is a body entrusted by the national SMI/E council to carry the role of formulating overall policies and strategies for SMI/Es and coordinating programmes across all related ministries and agencies. Organization C was transformed in October 2009 and today has become the central point of reference for information and advisory services for all SMI/Es in Malaysia. The business vision of Organization C is to become the premier organization for the development of progressive SMI/Es to enhance wealth creation and the social well-being of the nation. Organization C's business mission is to promote the development of competitiveness, innovative and resilient SMI/Es through effective coordination and provision of business support. There are five important functions Organization C has to deliver, which are coordination of policies and programmes, centre of advisory and information, management of data, dissemination of information and research on SMI/Es, provide business support and finally the secretariat to the national SMI/E Council. This body specifically oversees the SMI/Es, thus

supports them for business improvement.

4.6 Phase One: Quantitative Research Investigations

This research embarks on a quantitative method as the first research investigation. The quantitative investigation was carried out with the objective to identify the possible ISSM maturity factors. Through the quantitative data analysis, the researcher is also able to predict the relationship between independent factors, mediating factors and the dependent factors. These factors were determined based on the conceptual framework in Chapter 3. The quantitative analysis will address the first research objective of this research, thus answer the research questions one and two.

4.6.1 Population and Sample

A questionnaire survey was carried out to selected SMI/Es. This research carried out a purposive sampling procedure based on the criteria defined in the scope of research as stated in Chapter 1. During the selection process, the researcher also ensured that only active e-commerce business owners remain in the list. Although the database is from a trusted source, each contact in the database is checked to ensure that the business address and contact information are still the same for survey mailing purposes. The population of the sample was based on three databases provided by three organizations discussed earlier. Each organization owns about 200 or more business contacts and information, making the population of the research. However, as the research scope defined focuses on SMI/E with define criteria as mentioned in Chapter 1, the businesses were selected to further conduct the research investigations. The selected businesses becomes the research sample size. The first database consisted of business

contacts from the semi-government sector, based on which companies are in charge of business productivity in Malaysia. The second database is from the non-government organization body based in Klang Valley and the final database is from the semi-government agency which oversees and supports SMI/E, where the related business contacts are available via the business website. The population size for each set is listed in Table 4.1 below. Table 4.1 also shows the sample size of the survey conducted.

Table 4.1: Sample size and unit of analysis

	Population size	Sample Size
Respondents Organization A	250	45
Respondents Organization B	200	55
Respondents Organization C	300	29
Total Respondents	750	129

Table 4.2 discusses the research investigation one, which involved the quantitative investigation and its purpose. Based on Table 4.1, the sample size is small due to the purposive sampling conducted by this research.

Table 4.2: Research Investigation 1: Quantitative Investigation

Research Investigation 1 : Quantitative Investigation	
Investigation Objective:	1. Identify and determine factors governing ISSM maturity in SMI/Es in e-commerce. 2. Evaluate the relationships between the ISSM maturity factors.
Research questions being addressed:	RQ1 and RQ2
Expected link between data and proposition:	<ul style="list-style-type: none"> • Identify the factors of ISSM maturity of SMI/E with e-commerce in Malaysia. • Evaluate the relationship of ISSM maturity factors in SMI/E
Methods used:	Survey. A purposive sampling was conducted to determine respondents of survey
Unit of Analysis:	The Chief Executive Officer (CEO) or owner of the SMI/E companies incorporated in Malaysia with any type of e-commerce presence.
Scope for unit of analysis:	SMI/Es with e-commerce in their business process. Besides practicing e-commerce, the selected businesses have to implement at least minimal security practices to support their businesses, especially in terms of securing their online transactions.
Data access:	Three organizations: <ul style="list-style-type: none"> • Organization A: A semi-government agency involved in business productivity in Malaysia. • Organization B: A non-government organization (non-profit making body) • Organization C: A semi-government agency involved in the ac-SMI/E development in Malaysia.
Population, N:	Please refer Table 3.1
Sample size, s:	Please refer Table 3.1
Analysis method:	Structural Equation Modelling using PLS technique
Criteria interpreting findings:	ISSM Factors and hypothesis relationship define in Chapter 3

4.6.2 Establishing contacts

In the attempt to establish initial contacts with the research respondents, the researcher has leveraged an indirect relationship with the respondents through having two different agreements, except for the respondents from the third organization. The respondents' information is accessible through an online search from organization C's website. As the third database is available freely via the organization C's website, it is not required for the researcher to request for permission to use the contact information in the company website. It is sufficient for the researcher to establish initial contacts direct to the selected businesses using telephone. This task was conducted before deploying the survey to request for permission from selected busi-

nesses to send survey documents and invite the CEO or owner of the business to participate in the ISSM maturity research.

The first organization's (Organization A) initial contact was made through an introductory meeting set-up between the researcher and the semi-government body. The opportunity surfaced after a short discussion between the researcher and a consultant from the semi-government research team, during a two-day conference held in Selangor, Malaysia. The initial meeting was set up right after the discussion. In the first meeting, the research group in the semi-government agency expressed their interest in collaborating due to the similar research interest between both parties. A following meeting was held to discuss the research responsibilities of each party. In this second meeting, the semi-government agency expressed their intention to create a MoA to ensure research ownership, and to maintain confidentiality. An official MoA was signed in July 2010, and the research works commenced right after.

The second organization (Organization B) access was made from a successful snowballing procedure. This successful snowballing process led to the second research collaboration involved during this research. During an interview conducted using a contact from the first database, a CEO, also the business owner of a SMI/E company who had shown high interest in the research conducted. The interest was raised as the Non-profit organization (NGO) she is involved with, is currently interested to learn about the members' performance in e-commerce usage, security management issues and acceptance. As such, a follow up discussion was conducted between the researcher and the NGO team. Through the discussion via emails and phone calls, the NGO decided to collaborate and created a MoU between both parties. The research was conducted directly after the MoU was signed in July 2011.

4.6.3 Research Measurements

4.6.3 (a) Development of the quantitative research instrument

A questionnaire was used as a quantitative research instrument (refer Appendix A for the survey instrument). The development of questionnaire was based on the literature analysis done in the Chapter 2 and the relationship discussed in the research conceptual framework in Chapter 3. Through the literature analysis, a few issues were determined to have a significant relation towards the ISSM maturity, thus becoming the main elements. Hence, the research instrument is classified according to classification in Table 2.10 discussed in Chapter 2. All questions posted in the questionnaire were based on the classification of Table 2.10, which is organized in reflected issues.

In the questionnaire (in Appendix A), Questions 1, 2 and 3 are designed to collect demographic data and address the independent factors (business size, business length and business type-please refer to Figure 3.2 in Chapter 3). However, the top management support (in Figure 3.2) is not addressed as part of Questions 1, 2 or 3 as the top management support is a factor of a reflective construct rather than a direct form of question (such as the Questions 1, 2 and 3). The mediating factors are in reflective constructs. These mediating factors are spread-out in 10 different sections, starting from Question 6 to Question 13 (Refer Appendix A). The 8 different elements include (i) purpose of having security measurement, (ii) value of security towards e-Commerce, (iii) security usage, (iv) security communication structure, (v) support and enabler for security implementation, (vi) barriers to effective security, (vii) security implementation influences and (viii) security responsibility and current structure. Finally, the ISSM maturity reflective indicators predicted are reflected in Questions 4 and 5 under (i) presence of secu-

rity measurement in e-commerce and (ii) awareness level on security risk and management the company. The segmentation is designed to encompass relevant indicators discussing each topic mentioned above. However, there are indicators referred to top management support included in one of the segments. The researcher tried not to design a definite and rigid classification labelling as it will restrained the instrument answering, hence preventing it from further instrument bias. There are negative and positive types of questions in different sections to ensure that participants are aware and careful in answering the questionnaire.

4.6.3 (b) Measures of elements

The answer scale varies throughout the questionnaire. The first scale in Question 1, 2 and 3 involves definitive answers. The answers address the condition of business characteristics appropriate with questions being asked. For the purpose of data analysis, answers to each question are allocated with a scale to ease data identifying during data entry. The second scale reflects Questions 4 and Question 5 for ISSM Maturity. In this section, the scale involves "Yes, No and Not Applicable" as the answers. This section requires a definite answer from the respondents as the researcher needs to know whether each business has implemented each of the ISSM accordingly. The remaining questions from Question 6 to Question 13, the researcher employed the 6-point Likert scale answers, ranging from 1=strongly agree to 5= strongly disagree to 6= Don't know.

The decision to use a different types of answer scale is influenced by the objective of each question. In Question 4 and Question 5, the researcher's objective is to find out the type of security management practice and its availability in the business. These security management practices mainly range from basic security management practices to a complex level of security manage-

ment practice appropriate to the context of the research. In Questions 6 to Questions 13, the researcher needs to understand participants' practice and perceptions of security management in their businesses. The "yes/no" answers are not appropriate to describe the participants' practice and perceptions as a binary answer is too rigid in describing the actual situation. Although Likert-scale answers are still considered to be rigid compared to the qualitative interview answers, this ratings helps participants to choose the best appropriate situation of their respective business. The different types of scale also increase the instrument reliability as this criterion increases the awareness of the participants to be extra careful in answering the questions. Through the inconsistent pattern of question structure, it prevents participants from circling answers following the previous section style, thus preventing acquiescence bias as asserted by Lavrakas (2008); Podsakoff, MacKenzie, Lee, and Podsakoff (2003).

4.6.3 (c) Validation from expert

The instrument validation was conducted by experts in the field of ISSM and the academic research. The objective of the expert validation is to increase reliability and consistency of the research instrument. Through expert review, the content of the questionnaire were reviewed and further revised. All experts were chosen based on their expertise in ISSM research issues. They consisted of three ISSM practical experts and two academic research experts. The research instrument was also reviewed by a consultant from the Organization A's research team to ensure appropriateness of questions addressed to the targeted respondents. List of experts and the reviewer involved are described in Table 4.3 below.

Table 4.3: Experts and Reviewer Background involved in Content Validation

No	Experts/ Reviewer	Profession	Background
1	Expt1	Senior Government officer	A PhD holder and a security management specialist from a government agency focusing on information security management for the government sector. Currently holds the position as the Public Sector ICT Consultant (senior ranking) in a government agency.
2	Expt2	Professional Practitioner	Graduate and a practical practitioner. Works in a renowned Malaysia Security Management Company and an owner of a security management consultancy firm. Previously worked in a USA security management company based in Malaysia for more than 5 years.
3	Expt3	Professional Practitioner and Academician	An owner of few security patents. A PhD Graduate and a practical practitioner in a Malaysia renowned consultancy firm in the field of security management. Recently joined a private university as an academician.
4	Expt4	Academician	An Associate Professor and PhD holder who specializes in information security management field focused in security culture.
5	Expt5	Academician	A PhD holder who specializes in information systems and an expert in quantitative data analysis.
6	Reviewer	Senior Government officer	A senior consultant and a senior government officer of a government mandated body with more than 15 years of experience working with businesses in Malaysia on business productivity issues.

A test and review script was circulated to the experts as an assisting tool with their validation. The purpose of the script is to guide the experts on necessary validation. Besides, this script also explains the objective of the research and expected outcome out of the data collection using the questionnaire. Most reviews from the experts have been highlighted in the sample questionnaire given to each expert via email. Only three out of the six validations were conducted face-to-face as these three experts had requested to do so. The whole process of the expert validation took approximately three months. All these experts were contacted one month before the validation exercise. All experts agreed to participate in the research validation process, prior to sending the questionnaire and validation script via email. Most of the communication between

the researcher and the experts were based on emails for fast responses. The revisions on the questionnaire as suggested by the experts were incorporated and completed a week before it was ready for the pilot test. The revised copy was informed to the experts and made available as required by the experts.

4.6.4 Pilot test (analysis and improvement)

In the pilot test, the researcher conducted the test using the initial database given by the first database. The test was conducted using eleven selected CEOs from organization A's database. These businesses are the SMI/E selected for the purpose of this research. This test was conducted with the purpose of testing the questionnaire using the respondents (selected businesses from database provided by organization A) of the research. Using this method, the researcher will be able to identify the issues and problems of the instrument design. No major reports were received after the return of six questionnaires from the eleven selected SMI/Es. The pilot test was conducted for a month. The only major problem conducting this test was the willingness of the participants to participate. Besides, participants had to be reminded to reply the questionnaire in the allocated time given as they were busy with their daily business responsibilities. Analysis was strictly on the content of the questions, style and level of question apprehension. There were no statistical analyses that could be conducted, as the reply rate was low. The objective of the pilot test was to test the appropriateness of the questionnaire instrument within its context.

4.6.5 Conducting the actual questionnaire

The actual questionnaire survey was conducted immediately after all reviews and corrections on the questionnaire were completed. Reviews were mainly on the terminologies and security terms used by the researcher. The researcher was requested to use laymen words to explain security scenario to ensure respondents had no problems in answering the questions. The questionnaire was mailed to respondents from the organization A's and C's database, using the mailing facilities provided by organization A. Returns of questionnaires from the respondents were collected using the organization A's business mailbox or via fax. Maximum responses were received from the first round of questionnaire, in between five to eight weeks. In the case of no reply, the researcher sent an e-mail reminder followed with the telephone reminder to ensure participants have received the mailed questionnaire. An analysis was carried out from the first questionnaire immediately after the 8 weeks of questionnaire period.

The second round of questionnaires was distributed using organization B's database. The questionnaires were distributed using emails and some were sent by hand to 55 respondents. The hardcopy questionnaire responses were collected during a short meeting conducted in the Faculty of Computer Science and Information Technology, University of Malaya. The questionnaire responses were received within 3 weeks from when it was first sent. The number of returns from each phase of survey are as in Table 4.4.

Table 4.4: Sample size and unit of analysis

	Population size	Sample Size	Returns
Respondents Organization A	250	45	20
Respondents Organization B	200	55	28
Respondents Organization C	300	29	3
Total Respondents	750	129	51

According to Table 4.4, the total returns of the questionnaire are 51 from a total of 129 respondent identified earlier. Although 51 replies were received, only 49 questionnaires were usable as three replies were incomplete. The substantial decrease of population size to the sample size was discussed earlier due to the purposive sampling conducted in this research. As for the total returns, the research gained only approximately 50% returns, mainly due to the business policy restrictions on security management information sharing on the business. During the phone conversations conducted by the researcher (during the telephone reminder conversations), many business CEO and owners expressed their discomfort in participating in this research questionnaire, as the researcher had requested for business current security management practices. The low return rate agrees with assertion from Kotulic and Clark (2004) that information security research is one of the most intrusive types of organization research. Thus, businesses may refuse to participate as there is a general mistrust of any *outsider* attempting to gain data about the security measures in the business. Although the researcher has tried establishing contact using internal networking strategy, businesses associated to organization A and B especially were reluctant to disclose current business SM practices to outsiders. There were many challenges in persuading these organizations to participate in this academic research, especially as the topic of the research looks at the security management of a business (Kotulic & Clark, 2004).

4.7 Qualitative Research Investigations

The sequential investigation involved in this research applied the qualitative method to investigate further the possible ISSM maturity. A qualitative research emerges due to the demand to research the social environment of a specific phenomenon (Myers & Newman, 2007). In this second investigation, the researcher investigated the opinions and beliefs of ISSM maturity of the SMI/E CEOs and owners who have meticulously implemented e-commerce for business benefit, by using the semi-structured interview. Two types of interviewing style were adopted (i) is the personal face-to-face interview and (ii) is the group interviewing with the business owners. The selected CEOs (based on the survey responses in quantitative investigation) were identified according to their willingness to participate given in the questionnaire responses received earlier. The purpose of this qualitative investigation is to understand the underlying relationships of the factors in stimulating ISSM maturity in SMI/Es involved with e-commerce. Through the second phase of research investigation, deeper understanding could be gathered according to the CEOs' experiences and perspectives on the issues of ISSM Maturity in Malaysia SMI/Es. The interviews were set-up in the situation which were most comfortable and appropriate for the respondents.

As asserted by Denzin and Lincoln (2005),

Qualitative research research things in their natural settings, attempting to make sense of, or interpret, phenomena in terms of the meanings people bring to them. Qualitative researchers believe that rich descriptions of the social world are valuable, whereas quantitative researchers, with their etic, nomothetic commitments, are less concerned with such detail pp. 3

4.7.1 Research procedure

In any empirical investigation, uniformity in data collection contributes greatly to the rigour of the method and validity of the result (Miles & Huberman, 1994). In this phase, the one-to-one and group interviews were based on the semi-structured interview script based on Figure 4.3. The research procedure looked at three important phases involved in the qualitative analysis. Similar to the quantitative investigation, the qualitative method also has to identify the selected case and establish contacts, design the research instrument, validate the instrument, and finally conduct a pilot test before the actual interviews takes place. In this phase, the research issues and description are represented in Table 4.5.

Table 4.5: Research Investigation 2: Qualitative Investigation

Research Investigation 2: Qualitative Method	
Investigation Objective:	2. Evaluate the relationships between the ISSM maturity factors.
Research questions being address:	RQ2
Expected link between data and proposition:	• Evaluate ISSM maturity factor relationship
Methods used:	Semi-structured one-to-one interview and semi-structured group interview
Unit of Analysis:	Chief Executive Officer (CEO) and business owner of the SMI/SME companies whom voluntarily agreed on the interview session (based from previous quantitative data collection).
Scope for unit of analysis:	Selected voluntary SMI/E companies who practice e-commerce business.
Data access:	Similar with quantitative data access.
Population, N:	Based on quantitative input
Sample size, s:	23 companies
Analysis method:	Description of each of the interview as case and themes and sub-themes identified from each of the case
Criteria interpreting findings:	Themes determinations, where themes coexist during interview. Themes expanded from quantitative result.

4.7.2 Selection of cases and establishing contacts

Selections of interviews were based on the previous responses gathered from the quantitative research investigation, which were based on the CEOs' willingness to participate. The selection was directly made based on the responses given by the CEOs indicated in a designated column in the questionnaire. Statistical results analysed from the quantitative data collection had no influence in deciding the second phase's respondents. The researcher gathered all responses and further carried out telephone conversations with the CEOs to discuss the continuation of this research. Selected CEOs represented different types of businesses from product to service of the micro SMI/E. Most of these CEOs indicated their willingness to participate due to their high involvement in ISSM in their businesses especially in their e-commerce activities. Through the telephone conversations, the researcher was able to confirm the CEOs' decision on the interview participation. In the telephone conversation, the researcher also asked about current business SM practices to ensure that CEOs involved in this interview are aware of the research focus. Once the CEOs had indicated their willingness to participate, the researcher would email the interview details as a reminder to these participants. Meetings are set during the telephone conversations or through the emails sent. Through this exercise, one-to-one interviews were initiated.

As for the group interview, respondents were from the organization B's survey replies. As such, the representative from organization B has helped in gathering the contacts of the CEOs who were willing to participate in the qualitative investigations. The researcher then proposed a schedule and the venues for the purpose of this second round of qualitative investigations. All selected CEOs have indicated strong involvement in online business or e-commerce based on their business histories. Before setting up the group interview, the details on the interview

were emailed to the person in charge in the organization to disseminate the information accordingly. All CEOs were requested to read and understand how the interview would be conducted before they could provide their positive response towards the time and venue of the interview proposed. The interviews were only targeted to the business owners, CEO and the higher management of the businesses. The reason is because the research requires the in-depth views of the business processes and procedures of the businesses with regards to the ISSM effort. Additionally, the interviewees must be fluent with the business objectives and business policies to ensure the group interviews run smoothly.

4.7.3 Research measurements

4.7.3 (a) Development of interview guide

In the qualitative method, semi-structured interviews were carried out. The semi-structured interview approach was chosen due to its simplicity and straightforward procedure. It is the most common and one of the most important data gathering tools in qualitative research (Myers & Newman, 2007). As asserted by Rubin and Rubin (2011), qualitative interviews permit the researcher to see what is normally not on view and observe what cannot or seldom be seen. It is also important that in collecting in-depth social explanations and arguments, the research give emphasis on the depth and complexity in data (Alfawaz, 2011; Baskerville & Myers, 2009). Through the interview, it is believed that this technique could provide a deeper understanding of the studied phenomena.

The qualitative research investigation was facilitated by a semi-structured interview script to collect the in-depth data required for this research. The procedure involved seven personal interviews and three groups of CEOs in two different sets of research set-up. All questions

were open-ended and were formulated based on the previous literature and quantitative analysis. The interview protocol extracted results from the quantitative analysis, and then developed the interview protocol based on the quantitative results. The researcher also strengthens the interview protocol by comparison with the literature review previously conducted and discussed in Chapter 2. The open-ended structure permits the participants to provide details to help the researcher understand the vastness of the phenomena. The interview protocol was divided into two main parts. The first part is the demographics (refer to Figure 4.2), which is to gather information of the participant and the business. The first part of the interview also holds the purpose to “break-the-ice” between the interviewer and interviewee; in short to establish a sensible relationship and trust to ensure the effectiveness of the interview session. The demographic questions elicit information on the business size, business type, security understanding level, length of e-commerce in the market, annual income and age of the CEO.

Business size: <input type="checkbox"/> Less than 10 staff <input type="checkbox"/> 10 to 20 staff <input type="checkbox"/> more than 20 staff	Length of your e-commerce in the market: <input type="checkbox"/> Less than 5 years <input type="checkbox"/> 5 to 10 years <input type="checkbox"/> more than 10 years
Business type: <input type="checkbox"/> services (professional/educational) <input type="checkbox"/> product <input type="checkbox"/> services (domestic/utilities)	Annual profit from your e-commerce business: <input type="checkbox"/> Less than RM24000/year <input type="checkbox"/> RM24000 to RM72000/year <input type="checkbox"/> more than RM72000/year
Your security management understanding: <input type="checkbox"/> excellent or above average (have self-implemented a type of security implementation) <input type="checkbox"/> moderate/average (have learn and know basic security implementation in e-commerce) <input type="checkbox"/> novice/below average (have heard about it but never had a formal training on security management)	Your age: <input type="checkbox"/> 25 to 30 <input type="checkbox"/> 30 to 40 <input type="checkbox"/> 41 to 50 <input type="checkbox"/> 51 and above

Figure 4.2: Interview Protocol- Demographics Questions

The second part is the key area questions. It is a collection of specific questions to address the ISSM maturity issues. The objective of these five key areas is to identify any possible and additional factors which could possibly lead to ISSM maturity of SMI/E with e-commerce. All five key areas were derived from the quantitative results which were based on to carry out the

qualitative investigations. The five key areas were favourable reception, usage, business returns, acceptance and current ISSM procedure. These key areas were derived from the literature analysis and the conceptual research framework based on the SM practices. Here, the research seek to understand the relationships between constructs determined, by trying to understand the SM practices involved in the business. In order to better understand the SM practices in each of the business, the researcher leveraged the conceptual framework of TOE to derived with the appropriate issues for the interview. The interview protocol key areas can be referred to in Figure 4.3.

4.7.3 (b) The pilot test

The pilot test was carried out with four CEOs, using the interview protocol. All comments by the participating CEOs were taken note of. This pre-test was conducted to review the interview protocol and highlight any questions which were not clear to cover all issues addressed in the ISSM maturity. The pilot research objective is also to ensure that the intended data were indeed reflected by the data collected through this pilot test. By having this procedure, the researcher will revise the interview protocol accordingly, hence appropriate data will be collected. It will also increase the researcher's focus on the studied issue. Further revision is conducted before the actual interviews. There were no major comments on the interview protocol from the CEOs but rather the researcher was cautioned by the way these four CEOs answered the interview. This is because each CEO is constrained with his own business policies and procedures, hence a variety of answers were collected from this pilot test. The interview protocol may not follow the sequential issues listed, as the flow of the interview is highly based on the responses from the CEOs. Nonetheless, the interview protocol is the main source of reference which stimulated the interview. The researcher identified a few weaknesses in the questions, thus probe text was improved for clarity.

Research Questions (RQ)	RQ2-What are the underlying relationships of the factors in stimulating ISSM maturity in SMI/E involved with e-commerce?
Interview Questions (IQ)	<p>What is your opinion on security management for e-commerce?</p> <p>KEY AREA</p> <p>FAVOURABLE RECEPTION</p> <p>a) How is ISSM being practice in your e-commerce company?</p> <p>Probe</p> <ul style="list-style-type: none"> • Where is it practised? Why is it being used, for what purpose? Who used it, who is the stakeholder? Who/what influence you of having ISSM? • From what source do you appropriate the security management concept? <p>USAGE (INCULCATE)</p> <p>b) How has the usage/infusion of ISSM change your e-commerce business?</p> <p>Probe</p> <ul style="list-style-type: none"> • In what ways? Where and How far has it improve in house process? • Has it affect your staff/business process • Are you as the CEO feel more comfortable after the security adoption compared to before the implementation? • What else has change? Users? <p>BUSINESS RETURNS</p> <p>c) How do you see ISSM adoption and adaption towards your e-commerce business returns (economically/socially)? What else you think ISSM could be utilized to maximize your ROI?</p> <p>Probe</p> <ul style="list-style-type: none"> • In terms of business process? Salient return on IT investment? • Effective service delivery • Increased trusted by users <p>ACCEPTATION (accepting with approval)</p> <p>d) Why does ISSM has a slow take-off in the e-commerce context?</p> <p>Probe</p> <ul style="list-style-type: none"> • Problems in implementation? • Issues not addressed? • Not support? • Back-burner issue • Other issues? <p>CURRENT ISSM PROCEDURE (standards and best practices)</p> <p>e) Why does the current standards or best practices on ISSM are minimally utilized by the e-commerce business as it could contribute to an effective security management for the e-commerce?</p> <p>Probe</p> <ul style="list-style-type: none"> • Problems in understanding? • No knowledge? Lengthy standards • Need practical framework • Issues are not addressed appropriately

Figure 4.3: Interview Protocol

4.7.4 Conducting the actual interview

The actual interview was conducted in two series. First, the one-to-one interview and the second was the group interview. All participants were provided with the interview introduction email. They were requested to read the information provided in the email before the interview

session. A consent form also accompanied the interview's brief introduction.

There were seven one-to-one interviews conducted and three group interviews. The one-to-one interviews were carried out first, followed by the group interview as the management of one-to-one interview is much simpler than the group interview. The seven one-to-one interviews were conducted in the business premise or any place deemed to be most convenient for the participants, for example, having the interview in a convenient coffee shop or private recitation club around Klang Valley. Most of the interviews were conducted in the morning, around 10:00 AM to 12:00 PM. As for the group interviews, the number of groups and time slots were determined by the researcher. There were three group interviews arranged by organization B. The number of CEOs in each group ranged between 5-7. The group interviews were conducted at the researcher's premise as proposed by organization B. The decision to use the researcher premises was made by the participating CEOs because all CEOs were comfortable to have the Faculty of Computer Science and Information technology, University of Malaya as a host. The CEOs also believed that it is more conducive to conduct the interviews in a research premise rather in their business meeting rooms or private recreational clubs, to prevent any disturbance. The one-to-one interviews were conducted between 50 minutes to an hour, while the group interviews were conducted approximately 1 to 1 hour and a half hours. The researcher started the interview with a brief introduction on the research followed with documentation management highlights such as the consent forms and data recording required for the investigation. In the one-to-one interviews, the interviews were recorded using a tape recorder and a smart recording device (e.g. smart phone or MP3 recording devices). As for the group interviews, the researcher had received consents from all group members to conduct video recordings via camera-recorder and voice recording using a tape recorder. Video recordings for all three group interviews ses-

sion were conducted to ensure all discussions were captured. The group interviews were also assisted by a research assistant to assist in written data collection. As the length of the group interviews were predicted to be a little longer than one hour, the researcher had provided light refreshments, coffee and tea to ensure the group interviews went smoothly, where participating CEOs could enjoy coffee and tea during the session, hence feel more comfortable to participate in the discussions.

4.8 Analysis strategy

A mixed-method research generates data from two different research approaches. Hence, a clear analysis strategy has to be designed to accommodate the complexity during the analysis stage.

4.8.1 Visual representation

A suggestion by Ivankova et al. (2006) is to develop a visual representation of the analysis strategy which will be carried out in any mixed-method research. The visual representation concept has been used by many earlier researchers (Creswell & Clark, 2007; Ivankova et al., 2006; Tashakkori & Teddlie, 1998). This visual representation helps the researcher to visualize the sequence of data collection and prioritize between the quantitative and the qualitative methods. The visual representation also provides guidance as to where the integration of the mixed-method could be made in the research. Using the visual representation, the researcher could decide when and where adjustments could be made in the mixed-method research, thus the researcher could also determine whether research acquires augmenting information to complete the whole research process. In this research, the research prioritizes the quantitative

approach. Quantitative terms are written in capital letters to show their priority. The visual representation of the research as in Figure 4.4, portrays the sequence of the approaches with detailed procedures relevant to each phase.

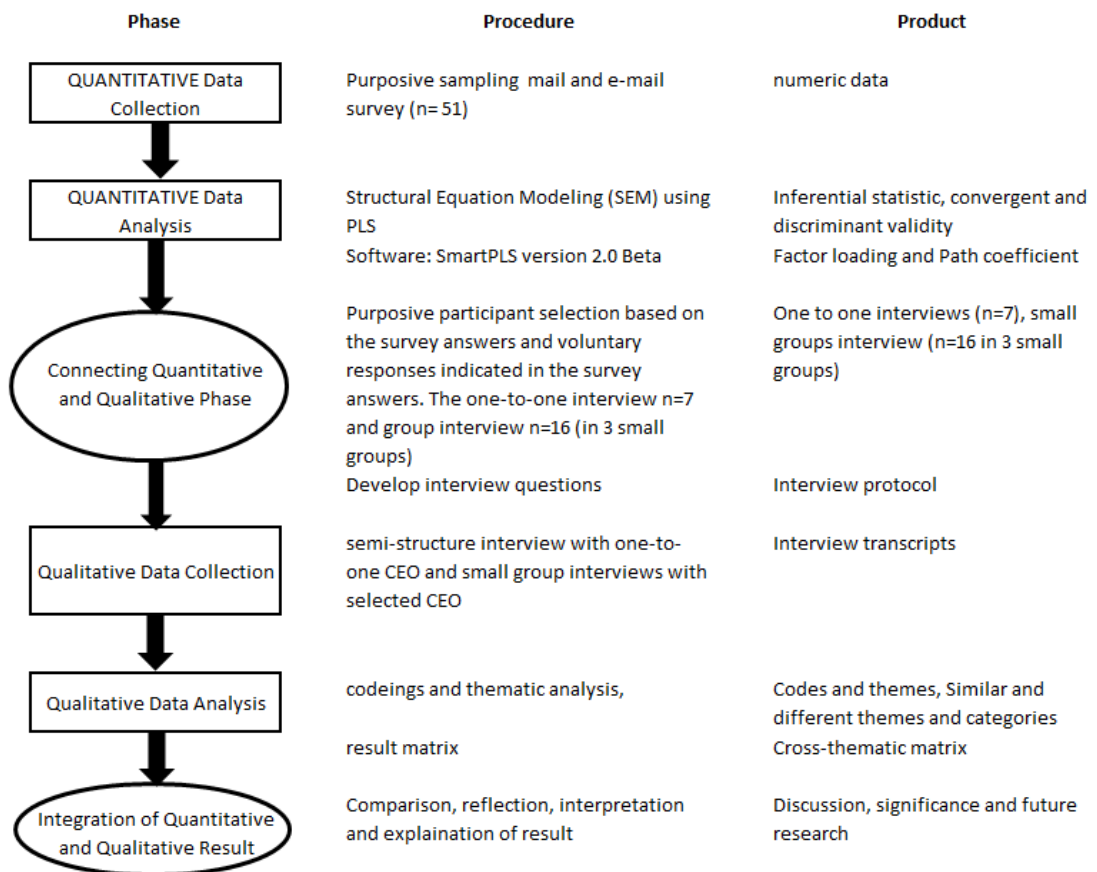


Figure 4.4: Visual representation of the ISSM Maturity Research

The integration of quantitative and qualitative methods happens in between both approaches in sequence. This research leverages on the ten rules to building visual representation of mixed-method research as suggested by Ivankova et al. (2006) presented in Table 4.6.

Table 4.6: Rules to Drawing Visual Models for Mixed-Methods Designs adopted from Ivankova et. al., 2006

No	Rules to Drawing Visual Models for Mixed-Methods Designs
1	Give a title to the visual model.
2	Choose either horizontal or vertical layout for the model.
3	Draw boxes for quantitative and qualitative stages of data collection, data analysis, and interpretation of the research results.
4	Use capitalized or lower-case letters to designate priority of quantitative and qualitative data collection and analysis.
5	Use single-headed arrows to show the flow of procedures in the design.
6	Specify procedures for each quantitative and qualitative data collection and analysis stage.
7	Specify expected products or outcomes of each quantitative and qualitative data collection and analysis procedure.
8	Use concise language for describing procedures and products.
9	Make your model simple.
10	Size your model to a one-page limit.

4.8.2 Analytic strategy for research

The general analytic strategy revolves around two approaches, the quantitative analysis approach and qualitative analysis approach. In this research, the analysis was conducted sequentially. The strategy also must accommodate the integration of two results and thus answers the research objectives of this research.

4.8.2 (a) *Quantitative analytic strategy: Structural Equation Modelling (SEM) using Partial Least Square (PLS) technique in quantitative data analysis*

The quantitative data analysis was conducted to address the first research objectives and partially answers the second research objectives. The quantitative analysis was conducted using Partial Least Square (PLS) technique. The PLS technique is an alternative technique under the Structural Equation Method (SEM). This technique was first discussed in 1975 by Wold (1974). The PLS technique has been frequently discussed in many IS papers and the acceptance of this method is very promising (Urbach & Ahlemann, 2010). This technique was chosen due to

many reasons. Firstly, based on the research respondents, a small sample was collected, thus is very unlikely to meet homogeneity and normality requirements (Hair, 1998). PLS does not require multivariate normality assumption on the data (Hair, Ringle, & Sarstedt, 2011; Henseler & Chin, 2010; Urbach & Ahlemann, 2010; Kankanhalli et al., 2003; Hair, 1998), especially when the responses are expected to be small, which is very much expected in this research scenario. PLS also emphasises on sample size that is based on the power analysis on the portion of the model with the largest number of predictors, with minimal recommendations of 30 to 100 cases (Urbach & Ahlemann, 2010). Secondly, this research involved two types of data, nominal (e.g., business type, business size) and ordinal data (e.g., the security management practices). Finally, the data collected in this quantitative investigation involved manifest (observable/formative) variable or latent (unobservable/reflective) variables, where the analysis of both relationships can only be done in PLS (Hair, Anderson, & Black, 2010; Urbach & Ahlemann, 2010). As this research examines the socio-technical factors and their relationship involved in ISSM maturity, it is expected that the data collected measure latent elements in which the conceptual relationship involved formative and reflective constructs. PLS has the ability to handle both types of constructs of the analysis (Hair et al., 2011; Henseler & Chin, 2010; Urbach & Ahlemann, 2010), thus making the analysis activity robust. As this research focuses on predicting the ISSM maturity model based on selected IS theories, PLS is the best suited analysis technique for this compared to the SEM (Urbach & Ahlemann, 2010).

This research conducts the quantitative data analysis with SmartPLS software version 2.0 Beta (Ringle, Wende, & Will, 2005). PLS was chosen due to the strength it has over traditional statistical methods (e.g. using SPSS). It is best used for prediction and theory development. PLS has the ability to test measurement models and structural models simultaneously as opposed to other techniques. The measurement model refers to the relationship between constructs

and measures (outer model), whereas the structural model refers to the theoretical relationship among constructs (inner model) (Kankanhalli et al., 2003). Also, PLS was chosen as the statistical analysis tool as it addresses the issues this research has based on the reasons given above.

4.8.2 (b) Overview of quantitative analysis

The quantitative analysis was conducted to identify the relationship between manifest variable with latent variable, and to test whether the hypothesis drawn in Chapter 3 is fulfilled or otherwise. In the conceptual framework discussed in chapter 3, three formative and a reflective constructs were identified as the independent elements of this research (refer Figure 3.2). To address all constructs formulated in the Figure 3.2, three formative constructs (business length, size, and type) measurement and the reflective construct (top management support) measurement were designed and presented in Figure 4.5. These measurement were developed based on the issues discussed in Chapter 2 and was represented in the Table 2.10. The top management support reflective construct measurements which are determined by nine items, whereby it addressed the issues on top management support related to (i) IS security-related meetings, (ii) IS security-related decisions, (iii) monitoring IS security-related activities and (iv) support on IS security-related functions) (Kankanhalli et al., 2003), which are questioned in the questionnaire (refer Appendix B, Table B.1 in page 231).

As for latent variable or unobservable elements, these consist of SM practices involving the technology, organization and environment attributes. These factors mediates a business to achieve ISSM maturity. Figure 4.6, Figure 4.7 and Figure 4.8 show some examples of the latent variable of mediating factors from SM practices. The remaining measurements for each latent variable are shown in the Appendix B Table B.2. The measurements for each SM prac-

No	Construct	Indicator construct	Code
1	Organizational size (formative)	size of your e-commerce company	ORGs
2	Business length (formative)	length being in the e-commerce business	BIZI
3	e-Commerce stage (formative)	stage of e-commerce adoption	ecS
4	Top management Support (TopMS) (reflective)	1. New implementation of security tools and techniques has to be approved by the highest management	TM1
		2. New implementation of security tools and techniques received strong support from the management	TM2
		3. Budgets are allocated for security implementation in a year	TM3
		4. Security training is staff Key Performance Index (KPI)	TM4
		5. Security knowledge sharing is encouraged by the management	TM5
		6. Security knowledge sharing is conducted every month	TM6
		7. Training required by critical staff is conducted once a year	TM7
		8. The management encourage security implementation	TM8
		9. The management is responsible for security implementation	TM9

Figure 4.5: Independent construct

tices were developed based on the issues discussed by Hsu et al. (2012); Monfelt et al. (2011); Yildirim et al. (2011); Gillies (2011); Alfawaz (2011); Tsohou et al. (2010); Da Veiga and Eloff (2010); Ozkan and Karabacak (2010); Werlinger et al. (2009); Kraemer et al. (2009); Dzazali et al. (2009); SIRIM (2007); Aceituno (2006a); Dzazali (2006); ISSA (2004); ISF (2003); Carnegie-Mellon (1999); Stacey (1996); Murine and Carpenter (1984). Further information are available in Chapter 2 represented in the Table 2.10. The operational definition is discussed in following subchapter.

Finally, the ISSM maturity is represented by 30 possible ISSM maturity indicators in the e-commerce business which was discussed by SIRIM (2007); Aceituno (2006a); Dzazali (2006); ISSA (2004); ISF (2003); Carnegie-Mellon (1999); Stacey (1996); Murine and Carpenter (1984). All considered variables reflects the SM exercised and practices required for business to achieve the ISSM maturity. ISSM maturity is the dependent factor of this research. Figure 4.9 shows some example of the elements. Direct and indirect relationships between elements are tested considering based on 0.05% level of significant presented in the path coefficients report. Concurrent with the conceptual modelling, hypotheses are tested to find relevancy. Subse-

No	TECHNOLOGY CONSTRUCT	Indicator construct	Code
9	Technology/Communication Structure	14. Information on security tools and techniques are shared using the Intranet	SMUS1
		15. Information on new security tools and techniques are circulated using internal e-mail	SMUS2
		16. Issues on security tools and techniques are discussed formally	SMUS3
		17. Issues on security tools and techniques are discussed informally	SMUS4
		20. Security tools and techniques are practiced by all staff	SMUS7
		21. Information on security tools and techniques used for a specific task are circulated to all via the Intranet	SMUS8
		22. Security tools and techniques practices are the responsibility of the staff	SMUS9
		23. Security tools and techniques updates inform formally in meeting	SMUS10
		24. Security tools and techniques updates inform informally by word of mouth	SMUS11
		25. New security tools and techniques demonstration is formally done and tested before full deployment	SMUS12
		26. New security tools and techniques demonstration are conducted in meetings	SMUS13

Figure 4.6: Technology Construct (Communication structure elements)

No	ORGANIZATION CONSTRUCT	Indicator construct	Code
4	Security Management Purpose	1. Security tools (technologies) important for the company	SMPur1
		2. Security techniques (procedures and policies) important to the company	SMPur2
		3. Security is main concern in deploying the e-commerce business	SMPur3
		4. Security is the main issue emphasized by management	SMPur4
5	Security Management Value	1. Security implementation help increase business reputation	SMVal1
		2. Security control implemented has increase users trust	SMVal2
		3. Security control practices has increase the company efficiency	SMVal3
		4. Security control practices has increase e-commerce availability	SMVal4
6	Security Management Utilization	1. The security tools and techniques are used to secure website	SMUU1
		2. The security tools and techniques are used in the e-commerce solutions to provide new and better services	SMUU2
		3. The security tools and techniques adopted help deter and prevent users from system misused	SMUU3
		4. The usage of security tools and techniques is a way to promote business	SMUU4

Figure 4.7: Organization Constructs (Purpose, Usage and Utilization elements)

quently, the result will be used for the qualitative research investigation in the second research investigation phase involving semi-structured interview (one-to-one and group interviews).

4.8.2 (c) Definition of Operational Elements for Quantitative Analysis

Operational elements are variable involved in researching ISSM maturity. Following Figure 3.5, there are three formative variables (business length, business size and business type/e-

No	ENVIRONEMENT CONSTRUCT	Indicator construct	Code
7	Security Management Practices Support	6. Incentives are given to staff fluent with company policy	SMS6
		7. Malaysia government plays an effective role in security management by allocating special consultancy body	SMS7
		8. Standards and best practices available are appropriate to assist e-commerce to implement security practices	SMS8
		9. Technology provided by local vendors is enough to implement security management	SMS9
		10. Communication technology provided by local providers are compatible with security implementation	SMS10
8	Security Management Practices Stimuli	1. Technology influence the security implementation in company	SMI1
		2. Technology suppliers provide excellent support to implement security	SMI2
		3. The company received funding from the government to implement security	SMI3
		5. Even though the company consist of small staff, security is perceived as important	SMI5
		6. Business competitors implemented security practices thus it is important for the company to do so	SMI6
		7. In order to compete in the e-commerce world, security gives important value towards e-commerce business	SMI7
		8. Confidentiality, data integrity, users authentication and availability are important factors in e-commerce business	SMI8

Figure 4.8: Environment constructs (Support and Stimuli elements)

No	Construct	Indicator construct	Code
10	ISSM Maturity Consideration (reflective)	1.The company uses user log-in and password for system applications	SMPos1
		2. The company uses SSL (Secure Socket Layer) certificate to secure web transaction	SMPos2
		3. The company designs policy, e.g. for change of password every six months	SMPos3
		4. The company designs a policy for validation purposes, e.g. when customers register to our website	SMPos4
		5. The company stores all user data and the system applications in secure servers	SMPos5
		6. The company stores all back-up data in a physical location equipped with physical security	SMPos6
		7. The company posts business terms and conditions on the website for everyone to read	SMPos7
		8. The company designs the e-commerce site considering applicable security measures	SMPos8

Figure 4.9: ISSM maturity dependent construct

commerce stages) and remaining are reflective variables (top management support, technology, organization, environment (under SM practices) and ISSM maturity). Based on Figure3.3, the technology, organization and environment constructs in the SM practices consisted of elements related to each construct. Under the technology or communication structure, the ISSM standards discussed the importance of security control and monitoring (Carnegie-Mellon, 1999). This includes technology usage, technology compatibility, complexity, relative advantage and availability (Hsu et al., 2012; Monfelt et al., 2011; Ozkan & Karabacak, 2010; Werlinger et al.,

2009; Kraemer et al., 2009; SIRIM, 2007; Aceituno, 2006a; ISSA, 2004; ISF, 2003; Carnegie-Mellon, 1999; Stacey, 1996; Murine & Carpenter, 1984). Hence it is important for the quantitative investigation to understand processes involved in practising security management and how it is being used.

As for the organization constructs, three elements were defined following Figure 3.3. The purpose of SM practice defines the aim and intention of security management seen or perceived by the SMI/E business. Thus, it looks at formal linking structure or informal linking in the business that promotes the SM practices. This includes how business perceived policies and procedures which formalize the business process (Hsu et al., 2012; Gillies, 2011). This is an example of formal linking structure involved in a business (Tornatzky et al., 1990). The value elements referred under SM practice relates highly between business with human resources. This is because, humans reflect highly towards how business perceived SM practices, hence creating value and advantage to the business. Utilization in SM practices defines the communication process involving security practices involved to carry out business tasks (Hsu et al., 2012; Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010). It assessed how business utilizes the security tools and technique towards the business. Here the researcher could assess the importance of ISSM towards a business. The security management utilization looks at what and why it is used.

Support in the SM practices refer to technology support characteristics. These involved the attributes of supplier and vendor technology supports (Hsu et al., 2012; Gillies, 2011; Alfawaz, 2011; Yildirim et al., 2011). It is important as in the SMI/E e-commerce, technology becomes the major environment influence in the ISSM maturity. Stimuli in the SM practices refer to user satisfaction, government regulations, industry characteristics and market structures. All these

attributes are considered as stimuli as they influenced the business to practice ISSM. User satisfaction signifies the satisfactory level of users in business e-commerce practices which highly relates with security matters (especially if it involves money transactions). The government regulation regulates ISSM standards in every e-commerce effort of a business. Hence, it is one of the important stimulus as it pushes a business to follow the legislation by authoritative body. Finally, the industry characteristics and market structure define the industry requirements and market orientations in current online businesses. Currently, the industry and market require businesses to be competitive. As such, the SMI/Es have to be flexible in exercising new business alternative such as the e-commerce to remain competitive (Tornatzky et al., 1990).

The ISSM Maturity defines the positions of businesses in achieving ISSM maturity. To determine whether a business has reached ISSM maturity, assessment questions are developed looking into security management presence and business awareness of security management. It is important to know security management presence of a business, be it from the implementation of security tools and techniques to the security awareness of a business; such will provide approximate ideas about the level of maturity a business currently has (Aceituno, 2006b; Carnegie-Mellon, 1999). The research conceptual framework as in Figure 3.6 was translated in the SmartPLS software to conduct the quantitative analysis Figure 4.10 is the research conceptual framework in SmartPLS worksheet before any evaluation had been conducted.

4.8.2 (d) Qualitative analytic strategy

In the qualitative analytic strategy, the researcher used thematic coding and pattern matching in analysing data. It is a classification of system or methodology which looks at categories, which in this research are the technology, organization and environment elements. The researcher

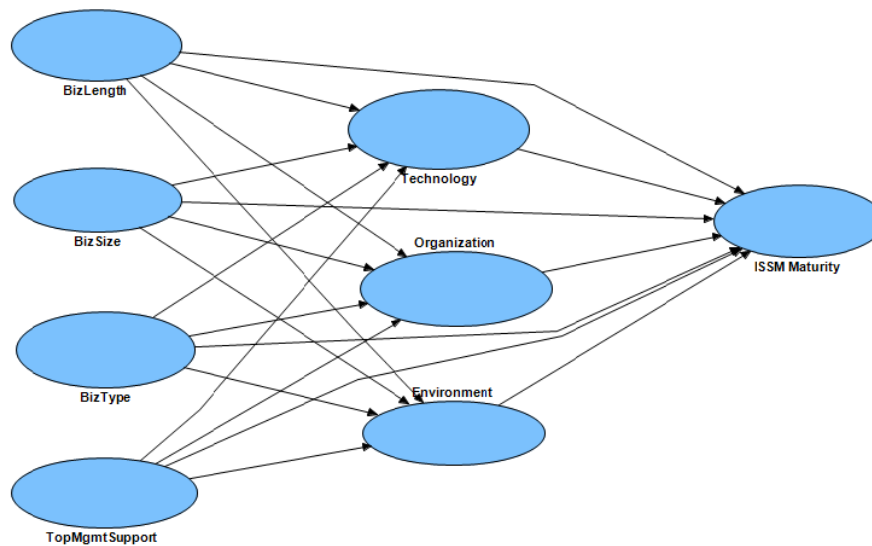


Figure 4.10: ISSM Maturity conceptual relationship model in SmartPLS

becomes the main tool of interpreting data. The researcher analysed and interpreted the data through the researcher's understanding (Miles & Huberman, 1994). Other than the technique used, qualitative analysis also employs three important processes, as asserted by Miles and Huberman (1994), in its data categorization:-

- a) Data reduction: data were selected, simplified and transformed into understandable information to address the issues in the research;
- b) Data display: summaries, diagrams and text-matrices are designed to seek meanings of the data analysed; and
- c) Conclusion: data were compared and contrasted between each participant where patterns were identified to address the research questions of the research.

These three processes of qualitative analysis help the researcher to categorize the data better and logically. The data reduction techniques example is displayed in Figure 4.11.

In data reduction, the scenario in each interview transcription was reduced to issues and items

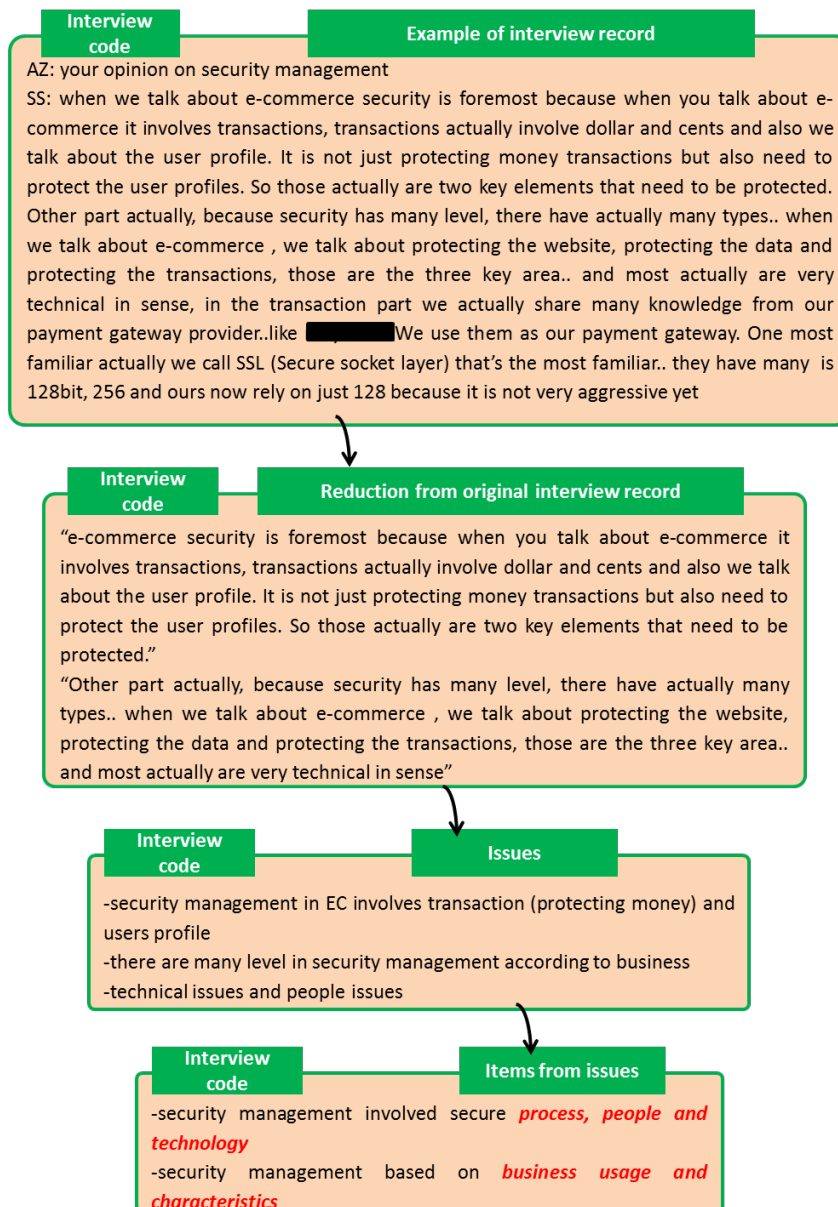


Figure 4.11: Data reduction process

of issues as presented in the last two boxes in the Figure 4.11. These will create the themes and sub-themes for the research. The example shown above is only one example of many yellow-sticky-notes being used to address issues of importance in ISSM maturity. All of this work was done manually with the usage of sticky-notes and multiple coloured pens for emphasis and differentiation of the different businesses involved. A huge piece of paper was used to paste all the identified items of issues (written on the sticky-notes). From this gathering, the researcher then tries to find patterns in the issues gathered. Once a pattern was detected, the items are grouped

together to become a sub-theme. The same process was conducted until all issues are grouped into identified patterns. The data are then displayed in Figure 4.12, which represent part of the interview record. The full transcriptions can be found in Appendix D. Figure 4.12 contained eight main themes with nineteen sub-themes, addressing multiple issues in each sub-theme. It includes quotes from the interviews and references to the participants being interviewed. Before the data is summarised, a data cleaning is conducted to check on the spellings and other associated errors. For the purpose of qualitative analysis discussion, quotes which are used to address discussions in Chapter 5, which were transcribed in Bahasa Malaysia were translated and mentioned in the discussion to maintain the standard of the research reporting.

No	Themes	Subthemes	Issues	Quotes	Reference	Relationship to theories
1	Organization	Business type/ structure	Business need/ requirement/ business mission/ business objective	<p>AZ: ...other influence in you implementing security... GX: I think in mine, because most of my customer are multinationals and also principle are. I deal with vendors supplier from overseas</p> <p>HS: ... I used to do a lot of work with international authorities, so manage to make a lot of contact with European authorities, and they sometimes pass me some cases to investigate...</p> <p>AHS: security tools apa yang ada yeh... consideration dier lah...satu needs... AZ: so keperluan company nih important lah... AHS: mcm company nih needs two cost, we will not go with the most expensive ones or nor e will use the cheapest ones.</p> <p>US: I see a need for that, like i said based on the maturity of the company. Because security is important. I realized that cuma depending on the level of the company punya resources dier focus dier.. tu semualah kan. So if you have the tool it should be based on certain number of website ker network ker, but if you have standards that people can use, to assess their security level, it would be good laa</p> <p>SS: ...no.. security must suit business objective... that is why they have many choices.. you have to understand exactly, what type of security that you need and what type of data you need to protect, so as I say just now.. it cannot rely on SSL.. but few other things we have to implement all together</p> <p>GX: also the nature of my business.. i think we deal with intellectual property, consulting and training. SO that nature of business is something that we need to protect</p> <p>KY: well, Firstly as I think as an owner of a business, coming from that perspective,</p>	<p>I5_NZA-GX Row: 65-66</p> <p>I2_HS-TB Row: 63</p> <p>I7_AHS-PTS Row: 281-283</p> <p>I6_DL-US Row: 161</p> <p>I4_MD-SS Row: 94 and 96</p> <p>I5_NZA-GX Row: 70</p> <p>I1_KY-SW Row: 20</p>	organization -formal linking structure

Figure 4.12: Qualitative analysis data display

The real identity of a business is not exposed rather initials or identifications are developed for analysis purposes. All participants are coded for confidentiality purpose. Codes used are I5-NZA-GX (for one-to-one interview) and FG2 (group interview) (as an example). The interview code represents the interview number-CEO-company name; and the group interview code represents group number. Participants and their organizations will remain anonymous.

The data are then read by the defined data headings as presented in Figure 4.13. As for the conclusion, the data were compared and contrasted as discussed in Chapter 5 in the interview analysis results.

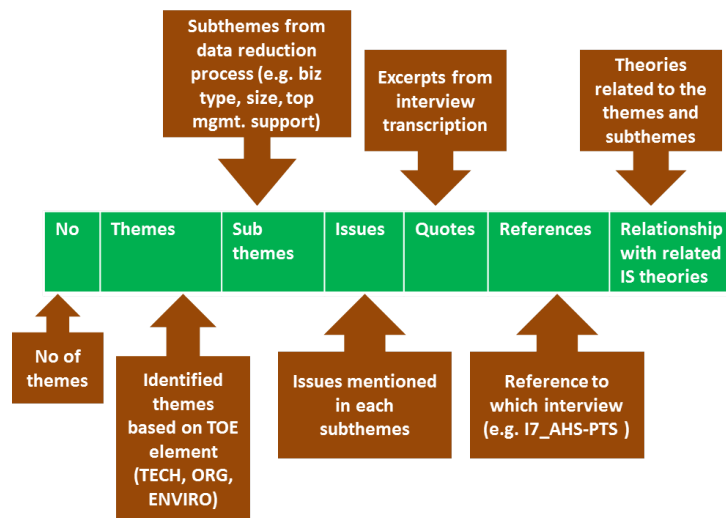


Figure 4.13: Qualitative analysis table representations

4.9 Conclusion

The research methodology and data collection methods conducted in this research are discussed in this chapter. This chapter justifies the choice of mixed-method techniques conducted based on the complexity and the multitude of the phenomena being researched. Hence, it is useful to conduct the quantitative data analysis, firstly because the research requires aggregation on the constructs of the phenomena and secondly, an in-depth qualitative exploration provides understanding through the relation of the constructs based on a “true-scenario”. The selections of the research are very much based on purposive sampling. Due to the high requirements of the research, the data collected have to be re-analysed and cleaned before it could be used to run the fieldwork. Organization A and organization B provided the required data, whereas organization C data had to be re-analysed and cleaned before the data collection started. The whole

process of getting two organizations to be involved in this research, through a formal research collaboration, took more than four months from the whole research schedule. This delayed the data collection process from the earlier schedule. An active sampling strategy was created to secure collaborations between identified organizations, hence ensure smooth and collaborative research investigations being conducted for the benefit of both parties. In this chapter, the researcher has justified and outlined the data collection strategy and analysis techniques and the respondents involved to achieve the objectives of the research. Chapter 5 presents the findings of the research eliciting and synthesising the current ISSM Maturity constructs in the chosen context, and its relationships towards the phenomena.

CHAPTER 5

DATA ANALYSIS AND FINDINGS

5.1 Introduction

This chapter presents the analysis of the mixed-method data collection involved in this research. There are two main sections involved in this discussion. The first section provides discussion on the analysis of factors of ISSM maturity in SMI/Es with e-commerce referred as RQ1 box in the analysis path and the factor relationship in the RQ2 box of the analysis path. The discussions are based on the analysis from quantitative data followed by the qualitative data analysis. Then the analysis results is integrated. Finally RQ3 is answered in the design of the ISSM maturity model as depicted in Figure 5.1. The first round of data analysis involved quantitative and qualitative data, conducted separately and sequentially following the analysis path below. The second round of analysis will then focus on the integration of quantitative and qualitative analysis to answer separate research questions, has resulted from the first section.

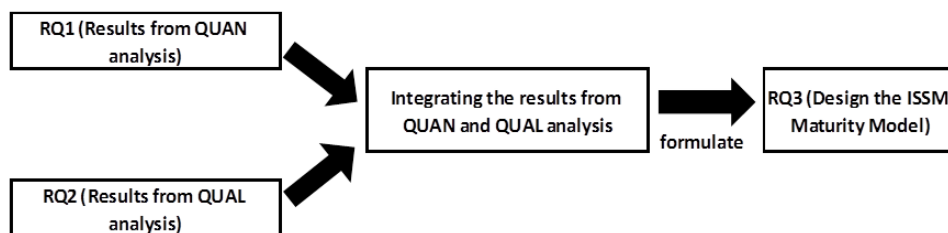


Figure 5.1: Analysis paths to formulate ISSM Maturity Framework

The quantitative analysis was carried out based on SEM using the PLS technique, to analyse the significance of the data collected. The qualitative data were coded where the relationships were derived following the comparison of coded data. The factors influencing ISSM maturity

are organized according to the theoretical maturity model and the relationship of these factors are analysed based on the research conceptual framework as in Figure 3.6

5.2 Quantitative Investigation Analysis

Using the conceptual relationship model as in Figure 4.10, the quantitative analysis was carried out. In PLS, analysis model validation is the first step of carrying out model parameter estimates. The purpose of the model validation is to determine whether the measurement models as well as the structural model fulfil the quality criteria for empirical work, whereby it involved a process of systematically evaluating whether the hypotheses expressed by the structural model are supported by the data (Hair et al., 2011; Urbach & Ahlemann, 2010; Haenlein & Kaplan, 2004). This partial model structure assessment involved a two-step processes including (1) the assessment of the measurement models and (2) the assessment of the structural model. The measurement model assessment involved the formative and reflective model assessment. Once the model validation was successfully carried out, then the assessment of structural model can be carried out. The results of the structural model analysis were evaluated and used to test the research hypothesis (Urbach & Ahlemann, 2010).

5.2.1 Model Validation in PLS: Reflective, Formative Model and Structural Model

In the model validation a two-step processes was carried out. The researcher started the process with the reflective measurement model assessment where it involved the outer/items loadings, internal consistency reliability (Cronbach's Alpha and composite reliability), convergent validity (AVE) and discriminant validity (Hair et al., 2011; Urbach & Ahlemann, 2010). In the PLS analysis, the significant of each item or variable is measured using the items loadings and

cross loadings in the reflective measurement model test. Although some scholars mentioned on the importance of conducting factorial validity with Exploratory Factor Analysis (EFA) (using SPSS or SAS) (Urbach & Ahlemann, 2010; Gefen & Straub, 2005), the factorial validity has been conducted by the PLS where results are as the loadings items and cross loading scores. Also, in many social science studies, the EFA may contribute to problem, for example, the algorithms used do not incorporate semantic knowledge about the variables when grouping occurs (Kock & Verville, 2012; Hair et al., 2010; B. Thompson, 2004). Hence, different items or variables may be found to belong to the same factor due to the strong inter-correlation, yet refer to different underlying construct (Kock & Verville, 2012; B. Thompson, 2004). It is also mentioned in D. Russell (2002, p. 1637), that researcher has to be careful in determining number of factor through EFA as "the default method of extracting factors with eigenvalues ≥ 0.1 is clearly not accurate". The same author also suggested to consider SEM as a method of quantitative analysis. The second step of the model validation is on the formative measurement model, consisting of measurement to assessed the formative indicator and the construct levels.

5.2.1 (a) Model Validation- Reflective Measurement Model: Outer Loadings

The next reflective PLS measurement model is to check its outer loadings. The outer loadings score is presented in the outer loading results as Table C.1 in Appendix C. The variable loading score must be above 0.707 (Hair Jr, Hult, Ringle, & Sarstedt, 2013). If the loading reading is below 0.707, variables must be dropped from the analysis model before conducting further tests. The dropped variables show that the variables are considered as not reliable and valid. The variables correlation within its own factor is also measured to assess its significant, where variable loading score must be highest in its own factor compared to the remaining factors. The result of this test is shown in Appendix C- Table C.2. The result is represented in Figures below, where items/variables constituted the appropriate factor are shown accordingly. Figure

5.2 represents the items/variables loading for independent factors, Figure 5.3 represents the TOE factors variables influencing ISSM maturity and finally, Figure 5.4 represents the variable loading scores for the ISSM maturity factor. All items load highest in its factors and are above 0.707 as recommended by Hair Jr et al. (2013).

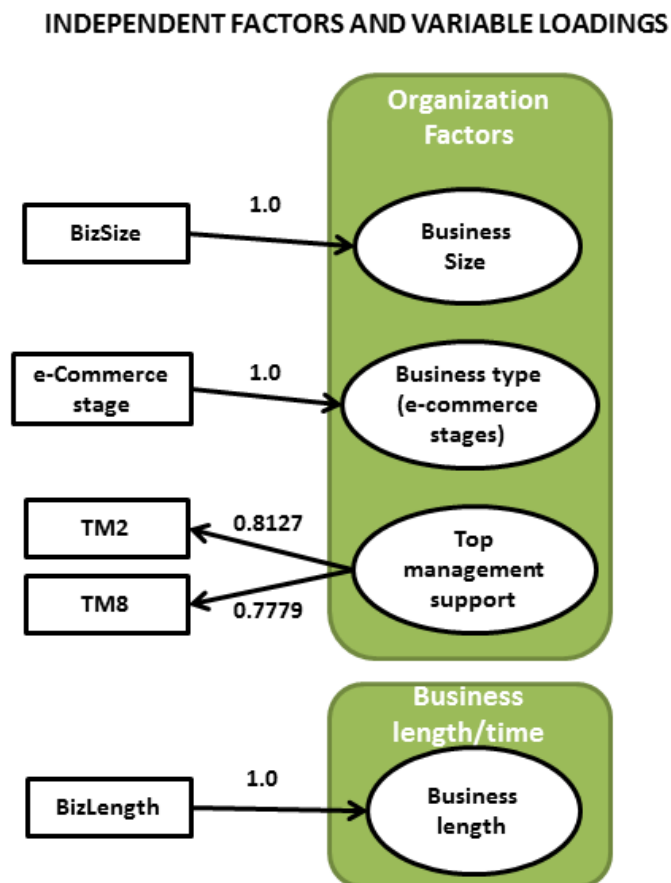


Figure 5.2: Independent Factors and Variables Loading

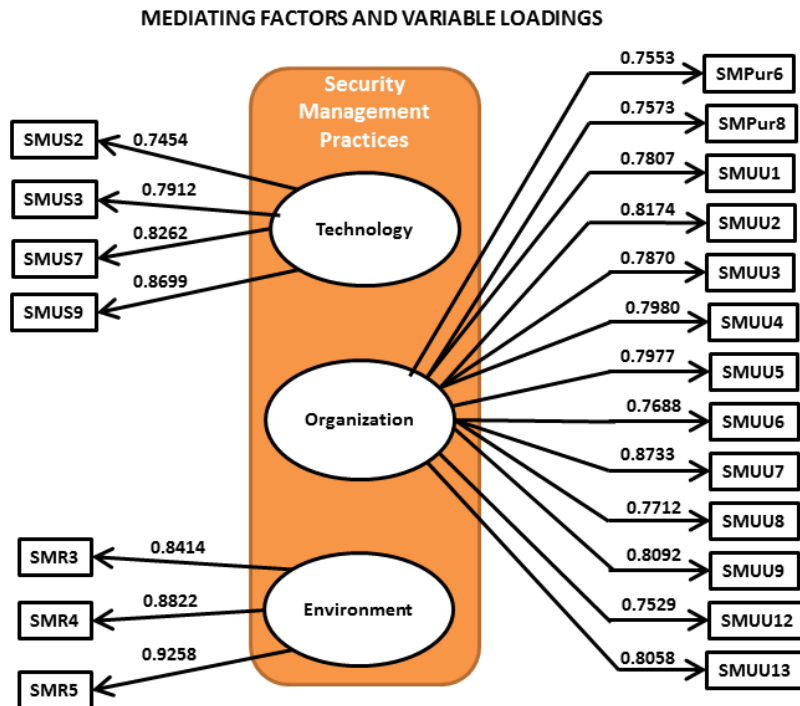


Figure 5.3: Technology, Organization and Environment (TOE) Factors and Variables Loading

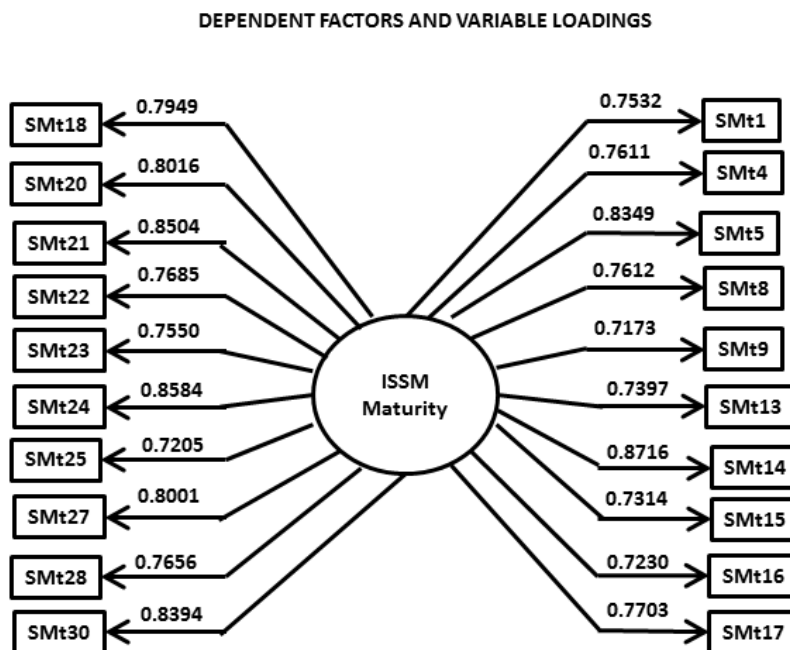


Figure 5.4: Dependent Factor and Variables Loading

5.2.1 (b) *Model Validation- Reflective Measurement Model: Internal Consistency Reliability (Cronbach's Alpha and Composite Reliability)*

The internal consistency reliability assessment involved the Cronbach's alpha and composite reliability test. Irrespective of which coefficient is used to assess the internal consistency, Nunnally and Bernstein (1994) asserted that all coefficient scores above 0.7 are necessary for exploratory research and all scores above 0.8 or 0.9 are in a more advanced stages of research. Conversely, scores below 0.6 indicate a lack of reliability. In Table 5.1, the evaluation of measurement shows the composite reliability and the Cronbach's alpha of the PLS analysis. In this test, the construct is considered reliable because the value of the composite reliability and the Cronbach's alpha is more than 0.80. These show that the composite reliability and the Cronbach's alpha reading have high reliability of internal consistency of the latent elements. This is because the score of latent elements composite reliability and Cronbach's alpha is higher than the threshold value recommended which is 0.6. The output of the composite reliability test shows a value of above 0.80 for all its constructs. The same output is given from the Cronbach's alpha value, which is all above 0.80 for all the constructs. Thus all constructs are considered reliable for this research. As displayed in Table 5.1, all constructs show composite reliability and a Cronbach's alpha reading of above 0.8, indicating high internal reliability (Urbach & Ahlemann, 2010).

Table 5.1: Composite Reliability and Cronbach's Alpha for ISSM maturity factors

	Composite Reliability	Cronbachs Alpha
Environment	0.914427	0.859115
ISSM Maturity	0.96917	0.966354
Organization	0.967919	0.96584
Technology	0.883417	0.824325
TopMgmt Support	0.891514	0.838537

5.2.1 (c) Model Validation- Reflective Measurement Model: Convergent Validity

The convergent validity assessment is where it involved the assessment on the degree to which individual items reflected a construct converge in comparison to items measuring different constructs (Urbach & Ahlemann, 2010). The convergent validity is assessed using the average variance extracted (AVE) criterion. The AVE score must be at least 0.5 to be able to explain more than half of the variance of its indicators, in which it explained sufficient convergent validity. This criterion was proposed by Fornell and Larcker (1981). Table 5.2 shows the AVE of each construct threshold is above 0.6, whereby all constructs had sufficient convergent validity.

Table 5.2: Average Variance Extracted (AVE) for ISSM maturity factors

	AVE
Environment	0.781899
ISSM Maturity	0.612067
Organization	0.650543
Technology	0.655442
TopMgmtSupport	0.813551

5.2.1 (d) Model Validation- Reflective Measurement Model: Discriminant Validity-Cross Loadings

Finally, the discriminant validity test assessed whether the items do not unintentionally measure something otherwise. In the SEM using PLS, the discriminant validity test was conducted using two measurements. Firstly, the measurement is conducted using cross-loading as asserted by Chin (1998a), whereby the result must show that each indicator's loading is higher for its designated construct compared to other constructs, where the loading score must load highest with its assigned items and it cannot be interchangeable between other constructs (Urbach & Ahlemann, 2010). The result is shown in the Appendix C in Table C.2 as the Cross Loadings analysis table. The second measurement involved the average variance extracted (AVE)

criterion by Fornell and Larcker (1981), whereby the AVE reading of each latent variable is higher compared to the latent variable's highest squared correlation than other latent elements (Urbach & Ahlemann, 2010). The result is shown in the Appendix C in Table 5.3. In Table 5.3, the result presented the latent variables correlation which signified that the latent variables have good discriminant validity value.

Table 5.3: Latent Variable Correlations

	BizLength	BizSize	BizType	Environ	ISSM Maturity	Org	Techno	TopMgmt Support
BizLength	1.00000							
BizSize	0.34169	1.00000						
BizType	0.20703	0.00834	1.00000					
Environ	0.03888	0.00262	0.09869	0.78190				
ISSM Maturity	0.07204	0.01028	0.26636	0.30603	0.61207			
Org	0.00000	0.01672	0.01984	0.64928	0.24483	0.65054		
Techno	0.00001	0.00069	0.02995	0.48606	0.14247	0.49669	0.65544	
TopMgmt Support	0.00013	0.00085	0.06089	0.67485	0.31309	0.56436	0.60050	0.81355

Note: Diagonals representing the AVE while the off-diagonals represent the squared correlations

From the model validation measurement, the researcher could summarized that the reflective measurement model is reliable and valid. The result of the reflective model validation is concluded in the Table 5.4. Consequently the assessment on the formative measurement model could be carried out based on the result from the reflective measurement carried out.

Table 5.4: Reflective Model Validation Results

Validity Type	Criterion	Description on analysis	Results
Factor validity	Outer Loadings and Cross Loadings	In the PLS analysis, the significant of each item or variable is measured using the items loadings and cross loadings in the reflective measurement model test. The variable loading score must be above 0.707 (Hair Jr et al., 2013). The loading reading is below 0.707, variables must be dropped from the analysis model before conducting further tests.	The dropped variables show that the variables are considered as not reliable and valid. The variables correlation within its own factor is also measured to assess its significant, where variable loading score must be highest in its own factor compared to the remaining factors. The result of this test is shown in Appendix C- Table C.1 and Table C.2.
Internal consistency reliability	Cronbach's alpha (CA) and Composite reliability (CR)	Irrespective of which coefficient is used to assess the internal consistency, Nunnally and Bernstein (1994) asserted that all coefficient scores above 0.7 are necessary for exploratory research and all scores above 0.8 or 0.9 are in a more advanced stages of research. Conversely, score below 0.6 indicate lack of reliability.	The results showed that the constructs are considered reliable because the value of the composite reliability and the Cronbach's alpha from the analysis is more than 0.80 as presented in Table 5.1. The results showed that the composite reliability and the Cronbach's alpha reading have high reliability of internal consistency of the latent elements. Hence this shows that the data has high internal reliability
Convergent validity	Average variance extracted (AVE)	The convergent validity is assessed using the average variance extracted (AVE) criterion by Fornell and Larcker (1981). The AVE scores must be least 0.5 to be able to explain more than half of the variance of its indicators, in which it will explained sufficient convergent validity.	The AVE results presented in Table 5.2, showed the AVE of each construct threshold is above 0.6, whereby all constructs had sufficient convergent validity.
Discriminant validity	Cross-loadings	The measurement is conducted using cross-loading as asserted by Chin (1998a). The results must show that each indicator's loading is higher for its designated construct compared to other constructs, where the loading scores must load highest with the assigned items and cannot be interchangeable between other constructs (Urbach & Ahlemann, 2010).	The results showed the constructs only consisted of items with loading higher in the group, compared to the remaining constructs. The result is shown in the Appendix C Table C.2.
Discriminant validity	Fornell-Larcker criterion	The analysis was conducted based on the average variance extracted (AVE) criterion by Fornell and Larcker (1981). The AVE readings of each latent variable is higher compared to the latent variable's highest squared correlation than other latent elements (Urbach & Ahlemann, 2010).	The results were shown in the Appendix C Table 5.3. Table 5.3 presented the latent variables correlation which signifies that the latent variables have good discriminant validity values.

5.2.1 (e) *Model Validation- Formative Measurement Model: Indicator Validity*

The indicator validity is part of the formative measurement model. This VIF test is conducted to understand how much an indicator's or item's variance is explained by other indicator of the same construct (Urbach & Ahlemann, 2010). The researcher had conducted a test on variance inflation factor (VIF) assessment to calculate the degree of multicollinearity among the formative indicators calculating the (Cassel, Hackl, & Westlund, 2000). The indicator validity test is to examine the multicollinearity of the indicators. This test is conducted using SPSS through linear regression. Here, linear regression between formative indicators of a specific formative construct (independent variables) and any other indicator of the dependent variable were tested. The result should yield values of commonly accepted threshold of 10. Any value of VIF which is below 10 is accepted as valid constructs. The results of the VIF is represented in Figure 5.5. Results on VIF in both figures showed all values are way below the accepted threshold of 10. Hence indicate construct validity for the formative indicators tested. The regression involved independent factors of formative construct (which include the Business size, Business type/e-Commerce stages and Business Length) with the dependent indicators of ISSM Maturity.

The linear regression output comes from SPSS analysis where the dependent variables of ISSM Maturity (SMPos) and three independent variables of business length (BIZI), business size (ORGs) and business type/ e-commerce stages (ecS). All VIF score are above 1 and are well below than threshold value of 10.

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	58.712	3.707		15.837	.000		
	BIZI	.000	1.614	.000	.000	1.000	.638	1.568
	ORGs	1.767	2.052	.157	.861	.395	.532	1.881
	ecS	-6.690	1.499	-.679	-4.463	.000	.766	1.306

a. Dependent Variable: SMPos

Figure 5.5: The Variance Inflation Factor (VIF) assessment for Indicator validity

5.2.1 (f) *Model Validation- Formative Measurement Model: Construct Validity*

The construct validity test for formative construct is the final test in the model validity. The construct validity test is assessed based on the statistical significance of the outer weights, not the loadings of all the constructs. The outer weight readings can be obtained through bootstrapping technique discussed by (Efron & Tibshirani, 1993) which is available in SmartPLS. Results for our ISSM maturity analysis indicated that all formative indicators have no outer weights value. This is because, only one formative indicator existed to each independent construct. The research does not require many formative constructs to represent business size, business length and business type/e-commerce stages. It is clear that for each independent constructs mentioned above only an indicator is sufficient to represent the respected independent constructs. Hence, this construct validity assessment is not appropriate for application in this ISSM maturity model validity test. Figure 5.6 presented the result of the outer weight result for construct validity discussions.

Outer Weights (Mean, STDEV, T-Values)

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	Standard Error (STERR)	T Statistics (O/STERR)
BIZI -> BIZI	1.000000	1.000000	0.000000		
ORGs -> ORGs	1.000000	1.000000	0.000000		
ecS -> ecS	1.000000	1.000000	0.000000		

Figure 5.6: The Outer Weight Results for Construct Validity

The results of the formative measurement model assessment are discussed in Table 5.5.

Table 5.5: Formative Model Validation Results

Validity Type	Criterion	Description on analysis	Results
Indicator validity	Variance inflation factor (VIF)	This is to examine the multicollinearity of the indicators. This test is conducted using SPSS through linear regression between formative indicators of the independent variables and any other indicator of the dependent variable. The commonly accepted threshold value is 10. All value of VIF which is below 10 is accepted as valid constructs	Results on VIF in both figures showed all values are way below the accepted threshold of 10. Hence indicate construct validity for the formative indicators tested.
Construct Validity	Outer Weight	The construct validity test is assessed based on the statistical significance of the outer weights, not the loadings of all the constructs. The outer weight readings can be obtained through bootstrapping technique discussed by (Efron & Tibshirani, 1993) which is available in SmartPLS.	Results indicated that all formative indicators have no outer weights value as only one formative indicator existed to an independent constructs. Only an indicator can represent the respected independent constructs as direct indicator is able to explain the independent constructs. Hence, there is no reading for outer weight in ISSM maturity.

5.2.1 (g) PLS Structural Model

The second phase of PLS analysis is the structural model assessment. Once the measurement model has satisfied all important tests conducted in the PLS measurement model above, the hypotheses of this research can be tested using the structural model. The structural model is assessed based on the amount of variance of endogenous latent elements (R^2) of the model. The R^2 value shows the significance of the relationship of a latent variable's explained variance to its total variance (Urbach & Ahlemann, 2010). Table 5.6 shows the R^2 value of the PLS analysis.

Table 5.6: R² Value for ISSM Maturity in SMI/E e-Commerce Malaysia

	R ²
Environment	0.575073
ISSM Maturity	0.509325
Organization	0.604746
Technology	0.527085

The PLS results show an R² values for technology factors at 0.5271, ISSM maturity at 0.5093, environment factors value at 0.5751 and organization value at 0.6048. The analysis concluded an R² value of 0.5093 for ISSM maturity. This means 50.93% of the construct indicators used to assess ISSM maturity is demonstrated by determined constructs defined in this research. Business length, business size, business type or e-commerce stage, top management support and the three important security management practices consisting of technology, organization and environment factors have represented this research well. According to Chin (1998b), R² values around 0.333 to 0.67 have average explanatory power. While R² values with more than 0.67, show strong explanatory power. From the results shown in Table 5.6, the ISSM maturity R² values in this research show average to substantial explanatory power. This means that there are substantial amount of issues covered in this research and this research has successfully addressed the ISSM maturity phenomena in an average to substantial manner. In a social science research, it is common to have the R² score between 0.50 and 0.80 as it is complex to address social science issues in a straight-forward relationship as the collected data were from the field investigation which are prone to many potential biases (Ghozali, 2008). The other reason of being able to identified only 50.93% is that, the researcher did not consider the culture issues, which may have influenced the ISSM maturity of the business. Although culture can be referred as part of the organization factors, the researcher does not give emphasis on the culture issues as the SM standards comparison did not give much emphasis on this matter. The SM

standard comparison mainly indicated the importance of usage, purpose and value of ISSM implementation towards business. As such, research could address this issue in the research future work; hence become part of the ISSM model improvement.

The path coefficient value (T-value) indicates the magnitude of relationship between two latent elements in the model. The cut-off value for T-value score is significant at significant at $p=0.05$ (value at ≥ 1.96), $p=0.1$ (value at ≥ 1.645) and at $p=0.2$ (value at ≥ 1.282) to have a certain impact within the model. In addition to the T-value, the path coefficient reading should also be substantial when it exceeds $p=0.05$, $p=0.1$ and $p=0.2$ levels. In order to test the significance, a re-sampling technique is required using the bootstrapping technique (based on 1000 samples selection) available in the SmartPLS. The hypotheses showed relationship between two factors. The hypotheses are not supported if the significant cut-off value is lower than $p=0.2$, where the T-value is lesser than 1.282. The negative and positive values of β determine whether the hypotheses are positively related or negatively related. The T-Value of the hypotheses relationship is presented in Table 5.7. The same table also presented the decision on each hypothesis.

Table 5.7: Result of Hypothesis

Hypotheses relationship	Hypotheses	Beta (β)	Standard Deviation (STDEV)	T-Statistics (IO/STERRI)	Decision
BizLength -> Technology	H1a	-0.0833	0.1893	0.4401	Not supported
BizLength -> Organization	H1b	-0.2814	0.1306	2.1546***	Supported
BizLength -> Environment	H1c	-0.2624	0.1123	2.3356***	Supported
BizSize -> Technology	H2a	0.1267	0.1300	0.9744	Not supported
BizSize -> Organization	H2b	0.3546	0.1380	2.5704***	Supported
BizSize -> Environment	H2c	0.1581	0.1075	1.4703*	Supported
BizType -> Technology	H3a	0.0125	0.1115	0.1121	Not supported
BizType -> Organization	H3b	0.1533	0.1107	1.3850*	Supported
BizType -> Environment	H3c	-0.0510	0.1001	0.5101	Not supported
TopMgmtSupport -> Technology	H4a	0.7310	0.1272	5.7484***	Supported
TopMgmtSupport -> Organization	H4b	0.7844	0.1304	6.0142***	Supported
TopMgmtSupport -> Environment	H4c	0.7176	0.1485	4.8311***	Supported
Technology -> ISSM Maturity	H5a	-0.1653	0.1645	1.0050	Not supported
Organization -> ISSM Maturity	H5b	0.3576	0.2527	1.4148*	Supported
Environment -> ISSM Maturity	H5c	0.0509	0.2300	0.2213	Not supported
BizLength -> ISSM Maturity	H6	-0.0250	0.1550	0.1612	Not supported
BizSize -> ISSM Maturity	H7	-0.0762	0.1443	0.5279	Not supported
BizType -> ISSM Maturity	H8	-0.4097	0.1266	3.2358***	Supported
TopMgmtSupport -> ISSM Maturity	H9	0.2583	0.1847	1.3986*	Supported

Note: *** significant at $p > 0.05$ (1.96), ** significant at $p > 0.1$ (1.645) and * significant at $p > 0.2$ (1.282)

The results showed eleven supported hypotheses. All eleven supported hypotheses showed the T-value reading at $p = 0.05$ and $p = 0.2$. This showed that the path coefficient value for these eleven hypotheses are significant at $p = 0.05$ and $p = 0.2$. The remaining paths were not significant as the as the T-value indicated is lower than $p = 0.05$. The researcher also identified positive and negative relationship of the hypotheses, indicated that factors can relate negatively or positively in the ISSM maturity. The supported hypotheses are the H1b, H1c, H2b, H2c, H3b, H4a, H4b and H4c, H5b, H8 and H9. The supported hypotheses are presented in the Table 5.8.

Hence, explained the significant relationship between factors identified in the earlier stage of the quantitative analysis.

Table 5.8: Hypothesis decision

H	Hypothesis	Decisions
H1a	Business length is related to technology factors in the SM practices	Not supported
H1b	Business length is related to organization factors in the SM practices	Supported
H1c	Business length is related environment factors in the SM practices	Supported
H2a	Business size is related to technology factors in the SM practices	Not supported
H2b	Business size is related to organization factors in the SM practices	Supported
H2c	Business size is related to environment factors in the SM practices	Supported
H3a	Business type is related to technology factors in the SM practices	Not supported
H3b	Business type is related to organization factors in the SM practices	Supported
H3c	Business type is related to environment factors in the SM practices	Not supported
H4a	Top management support is related to technology factors in the SM practices	Supported
H4b	Top management support is related to organization factors in the SM practices	Supported
H4c	Top management support is related to environment factors in the SM practices	Supported
H5a	Technology factors in the SM practices is related to ISSM Maturity	Not supported
H5b	Organization factors in the SM practices is related to ISSM Maturity	Supported
H5c	Environment factors in the SM practices is related to ISSM Maturity	Not supported
H6	Business length is related to ISSM Maturity	Not supported
H7	Business size is related to ISSM Maturity	Not supported
H8	Business type is related to ISSM Maturity	Supported
H9	Top management support is related to ISSM Maturity	Supported

The conceptual framework designed was assessed, and the result is presented as in Figure 5.7. In this figure, the value of each relationship is depicted, and for a significant relationship the researcher has indicated the value with "*" sign to show the level of significant.

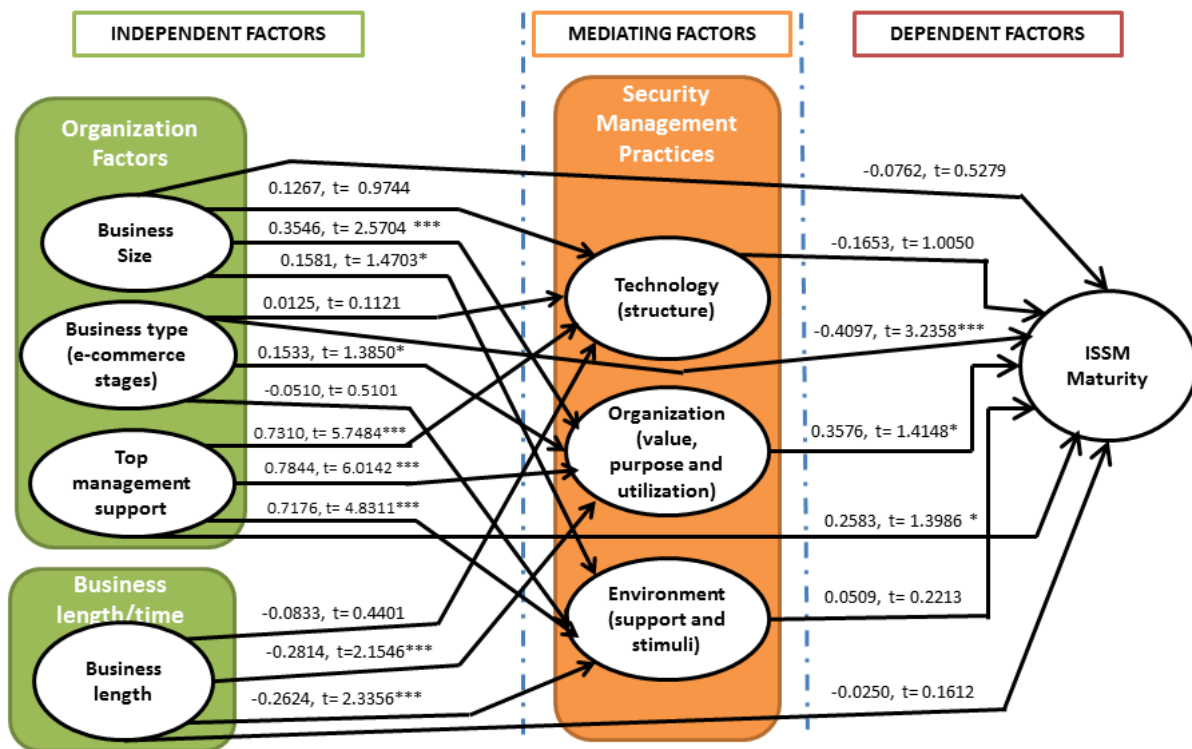


Figure 5.7: The ISSM maturity result from the quantitative analysis

5.2.2 Quantitative Results Analysis

The predicted model was empirically tested. Factors which influenced ISSM maturity were identified and PLS analysis concluded the indicators influencing ISSM maturity. The conceptual framework design in Chapter 3 was also tested and the results are represented in Table 5.7. Key discussions are presented below, according to the PLS analysis results. The discussion should be able to mainly address the first research question which is:

RQ1) What are the factors that influence the SMI/Es in e-commerce to reach ISSM maturity?

Through the results from the PLS measurement model, it is concluded that business length, business type or e-Commerce stage, business size, top management support, technology factors and organization factors and the environment factors show substantial relationship towards ISSM Maturity reflected in the R^2 results of 50.93% presented in Table 5.6. Appropriate with

the theory from Ein-Dor and Segev (1978) and the discussion from Prananto et al. (2003a, 2003b) business type, organization size and business length showed similar influence in ISSM maturity of a business. Results from the Table C.2 showed the significant variables associated to each factors (independent, TOE and dependent factors). Hence, these results indicated that the independent constructs are valid and significant.

The top management support indicated significant result in top management support towards implementing new security tools and techniques (TM2), and encouragement in practising security implementation (TM8). These factors influenced the business to achieve ISSM maturity. As for the technology variables, the analysis had shown high significant on the variables of the technology and communication structure involved in the business. These variables showed the importance of technology usage and technology availability in achieving ISSM maturity of a business. The significant technology variables are:

- 1) Usage of email is required to exchange information on new security tools and infrastructure (SMUS2);
- 2) Security information has to be communicated formally in the business (SMUS3); and
- 3) Security tools have to be practised by all staff (SMUS7) and is part of staff responsibility towards the business (SMUS9).

In the organization factors, items identified significantly influence ISSM maturity are:

- 1) Data integrity and system availability are business objective (SMPur6 and SMPur8);
- 2) Security tools and techniques are used to safeguard business assets (SMUU6), website (SMUU1), mitigate risk and threats (SMUU12), and prevent from system misused (SMUU3);
- 3) Security tools and techniques are adopted to follow business trend (SMUU13);

- 4) Security tools and techniques are used to provide new and better services (SMUU2), and promote business (SMUU4);
- 5) Security tools and techniques are used to compete with competitors (SMUU5) and fulfil user requests (SMUU7);
- 6) Security tools and techniques are used to comply with government legislation (SMUU8) and security standards (SMUU9).

Finally, the environment factors with significant items are the technology providers support helped business in its ISSM implementation (SMR5), industry players support business SM initiatives (SMR4) and staff responsibility are significant in practising SM(SMR3).

As presented in Figure 5.2, Figure 5.3, Figure 5.4 items correspond to each items as discussed above, the researcher is able to conclude that the TOE factors influencing the ISSM maturity in the SMI/E. The results showed significant relationship of factors with the technology exercised and usage (Werlinger et al., 2009), and technology availability (Tsohou et al., 2010).

In the organization factors, the business size (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978), business type (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) and business length (Prananto et al., 2003a, 2003b) are independent factors which signify good influence level towards ISSM maturity. Besides, the above factors of the top management supports (Monfelt et al., 2011; Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010; Ozkan & Karabacak, 2010) is significantly related ISSM maturity based on the significant cross loading value of the PLS analysis. The results demonstrated that the importance of top management supports to achieve the ISSM maturity. Apart from the mentioned organization factors, the cross loading results agreed with the discussion from (Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010) which

dictated the importance of human resources. Yildirim et al. (2011); Albrechtsen (2007) also asserted the importance of systems users, internally and externally, which refers to the utilization of SM practices. Organization issues involved the business owner's responsibility and the human issues surrounding the business. These would include human resources management such as awareness level represented through exercised security by the staff of the business as part of their responsibility (Tsohou et al., 2010; Da Veiga & Eloff, 2010). Other than involving the human development, organization issue must also cover the policies and procedures governing a business (Hsu et al., 2012; Yildirim et al., 2011; Gillies, 2011). The policies and procedures formalize the business operation, hence is part of the formal linking structure of a business (Tornatzky et al., 1990). It is also represented as part of the business objective. This is important because it formalizes the business and the users to communicate, hence help to prepare the business for any security emergencies. Human related issues also surround the business owner's motivation and support (reflected in the top management support), which are essential in making the security management of a business successful (Gillies, 2011; Siponen & Willison, 2009). The encouragement and support between business owners and staff resulting to good SM practices habits is a good example of an informal linking structure.

Finally under environment factors, the variables signified the support from the business environment as important, where each variable respectively address the issues of support characteristics from suppliers and vendors (Kraemer et al., 2009) and the industry characteristics and market structure (Yildirim et al., 2011; Gillies, 2011).

RQ2) What are the underlying relationships of the factors in stimulating ISSM maturity in SMI/E, involved with e-commerce?

Through the PLS analyses, relationships of involved factors were predicted. This was shown from the result of the hypotheses decisions discussed in Table 5.8. Results showed eleven supported hypotheses which were:

H1b: Business length is related to organization factors in the SM practices;

H1c: Business length is related environment factors in the SM practices;

H2b: Business size is related to organization factors in the SM practices;

H2c: Business size is related to environment factors in the SM practices;

H3b: Business type is related to organization factors in the SM practices;

H4a: Top management support is related to technology factors in the SM practices;

H4b: Top management support is related to organization factors in the SM practices;

H4c: Top management support is related to environment factors in the SM practices;

H5b: Organization factors in the SM practices is related to ISSM Maturity;

H8: Business type is related to ISSM Maturity; and

H9: Top management support is related to ISSM Maturity.

These results showed significant relationship between independent factors with the TOE factors in order to achieve ISSM maturity in the SMI/E. Further analysis showed the inverse relationship in H1b, H1c and H8. The relationship of H1b and H1c showed that more recent business is the operation the higher organization and environment factors are involved and required. In order to practice ISSM at the initial stage of business set-up, high business resources and strong back-up from the environment are highly required in the organization, especially in SMI/E (Barlette & Fomin, 2008). As for H8, business type is referred to the e-commerce stage. The result showed that, the earlier level of business is in its e-commerce stage, the higher level of ISSM maturity a business could be achieved. This is true as in most novice e-commerce

stage, implementation of e-commerce technology or application is at minimal; hence SM implementation is straight forward and easily maintain especially by SMI/E with small resources (Kankanhalli et al., 2003). As for H2b, H2c, H3b, H4a, H4b, H4c and H9, scholars such as Hsu et al. (2012); Yildirim et al. (2011); Werlinger et al. (2009); Kraemer et al. (2009); Barlette and Fomin (2008); Fomin and Vries (2008); Zuccato (2007); Chang and Ho (2006); Zhuang and Lederer (2004) asserted in their research, the business size, business type and top management support are major influence in ISSM maturity, implementation and effectiveness.

Through the results presented, researcher was able to determine the significant of TOE factors involved in the SMI/E to achieve desired ISSM maturity. However, researcher felt that an in-depth investigation is essential to understand the ISSM maturity phenomena from the SMI/E CEOs and business owners. The qualitative investigation purpose seeks to elaborate, enhance, illustrate and clarify of results from quantitative results with the results from other method. Hsu et al. (2012), in their quantitative investigation discussed the extensive relationship of sociotechnical factors in an organization based on the result of the statistical analysis. In-depth discussions on how these relationships resulted are scarce. It is important to understand the in-depth relationship as Hsu et al. (2012) had defined the ISSM as an administrative innovation, where an innovation in nature, has to be dynamic and highly capable for adoption to ensure good implementation and exercises. Contrary to the quantitative method, a qualitative study, will be able to provide real life view of how these factors relate (Albrechtsen, 2007) and complements the findings in the quantitative research (Ivankova et al., 2006; Mingers, 2001). Hence, the qualitative research investigation was conducted, and analysis of this investigation is carried out in the next section. As ISSM maturity involved the state of full development or advanced stage of any process (Dictionaries, 2011) involved in a business, conclusively, the

researcher anticipate that the TOE factors have to highly inter-relate and have to be supported with business forces (where business has to be dynamic in nature) to ensure ISSM maturity of the business.

5.3 Qualitative Investigation Analysis

5.3.1 Overview

The research protocol used in this investigation were derived from the quantitative analysis. The findings below are what the researcher has gathered during the interview session with selected SMI/E CEO and business owners. The findings from the qualitative data investigation were compared and contrasted according to the research questions in the qualitative analysis. The relationship of each issue will be associated and referred to the conceptual framework developed in Chapter 3. The association, comparison and contrast will be discussed following the elements referred to the conceptual framework. In this second analysis phase, findings are to address issues of RQ2. The qualitative analysis is segmented into three important elements, which are technology, organization and environment. The subsections are constructed following an analysis made based on the transcription of data. The qualitative analysis continues the discussion of issues define in Table 2.10 which was derived based on the theoretical model as Figure 2.7 discussed in Chapter 2. The qualitative discussion carried out an in-depth discussion of the ISSM phenomena where the researcher discussed findings based on the interviews conducted with the selected business CEOs and business owners. Themes and sub-themes from the analysed transcriptions will help compare and contrast the findings appropriately. All excerpts are available in Appendix D. The discussion will highlight the appropriate excerpts from respondents based on rows of qualitative transcriptions from Appendix D.

5.3.2 Interview analysis: Section 1 - Technology-related elements

Technology, through the analysis of the interview, shows that it is divided into three main issues. It includes IT infrastructure, logical and physical tools and the process. From the three main issues, the most important features are discussed in the subsection below. This shows that to achieve ISSM maturity, each business depended on technology structures which were identified as technology availability and compatibility and technology characteristics.

5.3.2 (a) *Technology Availability, Compatibility and Complexity*

For the purpose of this discussion, the detailed qualitative analysis table can be referred to in Appendix D. In Appendix D, the “Row:” has become part of the coding scheme for participant reference. It defines the row number of where the CEO’s has mentioned the issues in his/her transcription. This “Row:” is used to help the researcher easily navigate and refer to the main transcriptions of all interviews. Hence, during each discussion onwards, there will be “Row:” mentioned for the purpose of referencing.

IT infrastructure, which addresses availability according to participant I5-NZA-GX and participant I7-AHS-PTS, affirmed that under technology infrastructure, connectivity and penetration is of utmost importance determination in deciding on the ISSM maturity. These reflect the state of availability of technology and services. Both CEOs, when questioned on technology influencing security management in order to determine ISSM Maturity, I7-AHS-PTS stated that

“...the broadband penetration, I really think that this will help” refer to I7-AHS-PTS, Row: 167

where I5-NZA-GX stressed

...connectivity is an issue. I believe the speed that we have here is just something that is really unacceptable...” refer to I5-NZA-GX, Row: 26-30

Technology availability in terms of ready to use technology is also crucial where

“(Translated version) I see there are many free open source tools. How good we are with these tools? This is a technical issue” by I7-AHS-PTS, Row: 465

I7-AHS-PTS asserted again

“(Translated version) If I consider tools, there are a lot of tools out there. Many tools which are free, cheap, inexpensive. There are many types of basic tools. Everything is there” I7-AHS-PTS, Row: 179

Technology compatibility is very closely related technology availability. The importance of having availability in terms of infrastructure which are usable and available tools define compatibility as an important feature. This is because available infrastructure is not enough to determine the ISSM maturity, as the technology tools must be able to be used to ensure effective SM practices in a business IS. Usually, the technology availability and compatibility are not major problems to the SMI/E’s e-commerce business as these businesses are new and many are at the entry stage of their businesses. They do not have old and outdated technology which they were inherited from their ancestors. Business with legacy system commonly have to go through the problem of incompatibility as the outdated technology and applications are not easily transferred to the latest technology due to complexity of the system upgrade. Often this kind of legacy system has become core business IS, which cannot be easily disused e.g. finance and payroll systems and the enterprise resources planning. One of the business cases (I7-AHS-PTS refer excerpt Row: 365) highlighted this issue during the interview.

“[translated version] I feel that SMI/Es do not need to worry too much on compatibility because we do not have so many issues on legacy. The good thing being SMI/E is that you can pretty much implement anything” Row: 365

He affirmed that for current business SMI/Es, issues of non-compatibility and non-availability are no longer excuses to not be involved in ISSM implementation, hence achieve ISSM maturity. He also asserted that the available technology, accessibility of the technology also influence the ISSM maturity. Another business CEO (I3-AR-HV) also highlighted the same issues.

“The important thing is that IS security has already matured in the IT world. You can use

whatever available. There is no need to buy" I3-AR-HV Row: 191

"[Translated version] Security implementation, if you look at it, I can not see too much budget in terms of software. Many of the tools are available" I7-AHS-PTS Row: 463

"[Translated version] I see there are many free tools. There are ample open source tools" I7-AHS-PTS Row: 465

5.3.2 (b) Technology Characteristics

(a) Proper and appropriate technology As for technology characteristics of IT infrastructure, the participants I2-HS-TB, I5-NZA-GX and I4-MD-SS addressed the importance of proper and appropriate technology, signifying the importance of technology characteristics. Proper and appropriate technology means technology which are in accordance to business requirement and needs. An example which reflect to this item is the usage of login and password is no longer proper and appropriate for transactional sites (e.g. shoppingcart site). Further SSL security certificates and security technology have to be implemented for this purpose. I4-MD-SS reflect to this matter as below:

"...not just rely on SSL, but we call it hash signature" refer to I4-MD-SS, Row: 8

I2-HS-TB asserted the importance of having proper tools,

"You have to really use proper tools, proper expertise" refer to I2-HS-TB, Row: 254

I4-MD-SS informed that in achieving ISSM maturity, appropriate tools for security management are required.

"...not just rely on SSL, but we call it hash signature" refer to I4-MD-SS, Row: 8

I5-NZA-GX stressed on the same characteristics, referring to the monitoring system required by a business to monitor server access. Appropriate monitoring systems will perform the security management tasks well and thus affect the ISSM Maturity.

"... and CCTV to monitor the server room, make sure who goes in and who goes out" refer to I5-NZA-GX, Row: 130

In logical security, the same attributes apply. Acceptable logical security technology is required, thus reflecting the importance of availability and technology characteristics. Workability, or we may also see it as proper and appropriate, is again very important in technology characteristics in terms of the logical security technology implemented.

“...what is recommended by a consultant is something that is workable, so we work within our means, building our own network, making sure we have our own internal system security, access control, software to manage the customer database” refer to I5-NZA-GX Row: 4

and again stressed by I5-NZA-GX of having acceptable and available tools,

“When I first heard about it, when a guy came to us and explained, I say this is complex. But I think let us take a simple step towards it. What is it we want to control and how do we control it? Then use available tools, which are available by Microsoft to manage security, access control and all the basic security management. Then we start to have log-in, passwords, and other simple security management procedures” I5-NZA-GX Row: 100

(b) Completeness Other technology characteristics considered to be important for the business to decide on its desired ISSM maturity is the completeness of the technology they need to depend on. Technology provided by a technology provider is viewed as complete by most of the participating CEOs. Most of them have at least mentioned their dependability on third party providers. This situation is clearly agreed by I4-MD-SS, I6-DL-US and I3-AR-HV. All three CEOs agreed that third party server vendors have the capability to provide completeness in the security management technology to assist them in their ISSM maturity effort. I4-MD-SS, I6-DL-US and I3-AR-HV asserted their high reliability towards this third party due to their completeness in security management tools.

“The reason why we rely on third party server is because they have complete set of security” I4-MD-SS Row: 124

“Usually the vendor will advise” I6-DL-US Row: 36

“We use third party hosting, we do not have our machine here, we do not have anything. We host it at the third party” I3-AR-HV Row: 67

. The I3-AR-HV Row: 67 above brings the meaning of businesses highly relying on the third party. The researcher interpreted that these mentioned statements refer to the high reliability of businesses to third party, but does not mean each business has a lack of resources and skill as the discussion made in the business premise does not show such. Also, the respective CEO has shown high SM understanding and knowledge on SM due to his 15 years' experience in the field of SM implementation and practice gained from the financial institution he has worked with before.

(c) Technology-specific processes As for processes involving technology, it is vital to have processes that support specific technology according to the business requirement. This is what specificity means in this research context. Thus, the business will be able to exercise appropriate SM practices according to the required process. This is heavily discussed by I2-HS-TB in his business case. The CEO has emphasised the importance of this issue during the interview especially when he needed to describe his business transaction activities, as he is very concerned about e-commerce which has high security risk.

"I structure a new verification flow. The flow looks at what happens when the order comes in and after the order got charge-back and the charge-back result. Once I did that, I pulled-up an automated system; system for the order to go through. It has to pass certain criteria such as IP does not match, phone number does not match, previous charge-back and credit scores" I2-HS-TB, Row: 17 and 19

This shows how technology-specific process is required to control risk. I2-HS-TB also mentioned

"For other businesses, they have to configure their own verification flow. It is not easy to do it. It took the company 1 year and a half to do the verification flow" I2-HS-TB Row: 45

(d) Technology usage: Ease of use and implementation During the interview, technology usage was also discussed by the business cases. The CEOs had frequently mentioned about ease of use and implementation as part of the requirements to achieve ISSM maturity. This is

because if technology is complicated and takes too long to be implemented, the SMI/Es usually have no resources to support complex technology, which will result in not using the technology at all. In this section, the issue of technology complexity is the main concern of the businesses. Technology compatibility was mentioned and discussed in earlier section, hence demonstrate that two technology related influences in the DOI theory were addressed in this analysis. As mentioned by I5-NZA-GX, I7-AHS-PTS and I4-MD-SS.

“Systems have to facilitate your business, but not to make your business more complicated” I5-NZA-GX, Row: 76

“...find the balance between security with user convenience.” I7-AHS-PTS, Row: 355-357

and

“It is not complex, unless you do not understand what security is all about. You need to know how SSL can do for you and how you need to protect your website from hackers.” I4-MD-SS, Row: 89-90

According to three CEOs above, findings demonstrate complexity is one vital issue that has to be addressed. It refers to system complexity and technology-specific complexity. Many SMI/Es business owners must understand this criteria in order to achieve ISSM maturity.

(e) Relative advantage The research analysis found that relative advantage has also influenced in determining ISSM Maturity. The ability to simplify job tasks, increase the Return of Investment (ROI) of the business and enhance user relationship will definitely play a role in ISSM maturity. In determining a technological innovation, businesses often assess the technology innovation and look at whether the technology can simplify the job task. The business will also look at the ROI increment if the technology is used, and lastly the ability of the technological innovation to enhance user relationship with the business. I4-MD-SS Row: 13-14, I2-HS-TB Row: 40-41, I5-NZA-GX Row: 13-14, and I3-AR-HV Row: 50-51, all of whom

had agreed that simplifying a job task by using a specific technological innovation (refer to the ISSM) could determine ISSM maturity of a business. I2-HS-TB Row: 248-249 and I5-NZA-GX Row: 106 and 108 have collectively reflected their increase of ROI in many forms. I2-HS-TB Row: 248-249 asserts that

“yes... (referring to ISSM) it has increased the sales...” I5-NZA-GX Row: 106 and 108

I5-NZA-GX also asserts that,

“I think before we implement security management we are unable to detect customers segments, but when we implemented our portal using our website we started to build a database (referring to secure implementation of website and database). After a while we are able to analyse and I get competitive advantages by implementing them”.

Analysis of the interview also found appropriate technology has increased user relationship, which is a very important relative advantage towards business. This could help the business to achieve its ISSM maturity. Collectively, all the CEOs who were interviewed have shown their agreement in the user relationship importance towards ISSM maturity. Better user relationships are seen in many ways including (i) increase of customer trust (I2-HS-TB Row: 242-243), (ii) satisfaction to customer (I5-NZA-GX Row: 139-142), (iii) positive customer perception with the increase of users confidence (I4-MD-SS Row: 54) and most importantly, (iv) customer feels safe (I3-AR-HV Row: 107) in the e-commerce site. These are some of the indicators that expressed the importance of having relative advantage from the specific technology usage.

The analysis of technology-related factors for ISSM maturity, represents a vital conclusion.

The findings of technology related issues are represented in Table 5.9.

Table 5.9: Technology related elements of qualitative analysis

No	Themes of analysis	Base theory	Relationship to theories	Technology-related elements issues reflected from analysis
1	Resources	TOE	TOE-Technology: Availability	a) services supported by the infrastructure are always present b) technology or tools is ready to use
2	Resources	TOE	TOE-Techno: Characteristics	a) proper and appropriate technology b) complete c) acceptable d) specific process
3	SM Diffusion	DOI-Relative advantage	Relative advantage	a) simplify job task b) ROI increase c) enhance user relationship
4	SM Diffusion	DOI-Complexity	TOE-Techno: Characteristics	a) ease of use b) ease of implementation
5	SM Diffusion	DOI-Compatibility	TOE-Techno: Availability	a) no legacy issues b) existing tools

Technology availability influenced the decision making in two ways. First, availability signifies the state where services supported by the infrastructure are always present and, secondly, the technology or tools are available and ready for use. As for technology characteristics, proper and appropriate technology, completeness, having appropriate technology-specific process, ease of use and implementation and finally, technology relative advantage are the main forms of characteristic for ISSM maturity. Proper and appropriate tools address the technology suitability towards the business. As for completeness, it refers to the complete set of technology usage to support the business specific IS. It was discussed by the CEOs that it is important to have complete technology to support business IS which only though this, their businesses could achieve the ISSM maturity. Having technology-specific process is vital to support business process. The ease of use is part of technology characteristics as it determines the user-friendliness

of a specific ISSM tools to achieve maturity. Technology must also be easy to implement to ensure better usage in the businesses.

5.3.3 Interview analysis: Section 2 - Organization-related elements

Under organization-related elements, there are six ISSM maturity factors identified, where four were tested in the quantitative analysis. Through the qualitative analysis, the researcher found that the discussion continues with issues on formal and informal linking structures, human resources, utilization of SM which mainly focuses on the business communication process and slack. These issues were found to be critical in SMI/E as they influenced the business SM practices. Many CEOs highlighted that these issues are important to address the business requirements which many SMI/Es are currently facing in their organizations.

5.3.3 (a) Formal and informal linking structures

(a) Formal linking: Formalization The analysis shows formalization through SM policies and business procedures which influence ISSM maturity. This is an example of a formal linking structure, whereby through formalization, business processes are controlled formally. In the case of ISSM maturity, formalization determines the seriousness of an organization to achieve its ISSM maturity. Business ISSM policies and procedures are the basic forms of formalizing business and its processes to achieve secured business processes. Formalization is important as it creates assurance to all business processes. In the formalization process, the CEO usually gives directives to staff to regulate appropriate SM practices in the business. This is when business processes are controlled and exercised. As a business is control according to SM standards and procedures, the business will be able to achieve system assurances, hence increase the IS

quality of the business. All staff are required to follow the defined regulation to increase business performance and achieve the business objectives. Formalization is found to be an influence to the business to achieve ISSM maturity as agreed by I2-HS-TB Row and I7-AHS-PTS below.

“AZ: Do you think it is important for you to base on the security standards?, HS: Yes, you have guidance and assistance. You should really appreciate it and use it because it will help you a lot” I2-HS-TB, Row: 200-201

“AZ: Do you think when you have business policies and procedures, it will actually help you do your work, in a way it means simplify your task?, AHS: [Translated version] That is true...” I7-AHS-PTS, Row: 232-233

Through formalization the business will have proper work organization, ability to predict risks and secure data backups. All properties above were discussed during the interviews and were mentioned by I4-MD-SS Row: 32, I2-HS-TB Row: 309 and I3-AR-HV Row: 51.

“We have to use the detection system to manage and minimise the risks” I4-MD-SS, Row: 32

“One thing you have to think about is you can not remove it, but you can reduce it. That is the fact” I2-HS-TB, Row: 309

“Security means a good definition of “who-do-what and who-received-what”; This is because when you want to be secure, you must know these two things” (I3-AR-HV Row: 51)

In conclusion, formalization is an important business aspect in SMI/Es. This is achieved by implementing appropriate SM policies and procedures according to the current ISSM standards. Formalization also encourages staff to practice and exercise SM good-practice or ethical business conduct as business has defined its requirements to all staff formally. With good business conduct, the business will be able to achieve its ISSM maturity.

(b) Informal linking: Top management support (top-down directive and motivation) Formalization in a business is influenced highly by top management support. The top management support is a form of informal linking structure. The support expressed by the top management motivates the business to practise and exercise SM. Top management support leads to many

good influences to the business for example motivation. With high top management support involved in security related practices, staff will be highly motivated to practise the SM in their everyday tasks. Motivation pushes the internal linking agents to support the business ISSM to achieve maturity. From the quantitative analysis, top management support is tested as the independent factor. However, in the discussion conducted with the CEOs of the SMI/Es, the researcher found that the informal linking structure in a business is crucial. This informal structure is highly related to the top management which usually defines the well-being of the business. Personal motivation and the CEOs' education background strengthen the support given by the top management as they understand the advantage of having ISSM, hence accelerate the ISSM maturity of the business. I7-AHS-PTS in Row: 345 asserted that:

“[Translated version] I am personally very interested (referring to security management and its technology). So I make sure we keep up with the current technology. I do a lot of self-reading, as I am keen about it. Only when it comes to the technical implementation, I will pass it to my IT staffs. Big ideas come from me, because I personally have strong interests in it”
I7-AHS-PTS, Row: 345

and I5-NZA-GX is motivated on ISSM implementation to achieve ISSM maturity as I5-NZA-GX optimistically mentioned in Row: 54 and Row 88 that ISSM has promised good investment and is therefore crucial for the business.

“I consider the security management as capital investment. We believe that some point or rather it is a long-term investment that would bring in money, but we struggled with the fact that it is not bringing in money fast enough.”

“...from the first day I started the business, secured website is already a critical element we knew we needed to have; we revamped, and we restructured and we changed accordingly”

The top management will direct the business to participate in SM following top-down directives. When top-down directive is implemented, the top management usually will ensure all factors to achieve ISSM maturity will be met, including education and training. High top management support is usually based on the level of knowledge a top management has and his or her motivation in the success of the business. Directives of IS security management implemen-

tation are commonly addressed by the top management. A clear ISSM directive received from the CEO will expedite the implementation of technological innovation (ISSM) to ensure business security. I3-AR-HV Row: 114-115, I7-AHS-PTS Row: 311, I5-NZA-GX Row: 109-110, I1-KY-SW Row: 111-112, I2-HS-TB Row: 168-169 and I6-DL-US Row: 87-88 collectively agreed that CEOs and business owners of the businesses determined the ISSM in the business.

“AZ: When you implement security management, who determine the implementation of it?, HV: It is from the top; the CEO of course” I3-AR-HV, Row: 114-115

“[Translated version] Actually in our company, there is the IT personnel, but they will wait for my directive. They will usually wait for my directives as I will allocate budget. Only then they will work on it” I7-AHS-PTS, Row: 311

“AZ: Who determines security management in your company?, GX: Yes, I do” I5-NZA-GX, Row: 109-110

“AZ: Who determines whether to implement or not the security management?, KY: I am” I1-KY-SW, Row: 111-112

“AZ: When you want to implement your security flow or the verification flow, who actually determines whether to implement or not?, HS: The managers and the CEO.” I2-HS-TB Row: 168-169

“AZ: Who determines it (refer to ISSM implementation) in your business?, US: Most of the time, I decide on the implementation. In this business I have three partners; myself, Mrs. Hanny and my husband. My husband is more of a technical person. Usually, when we want to discuss about technical issues (refereeing to technical issues of SM), I will pass the matter to him” I6-DL-US, Row: 87-88

5.3.3 (b) Human resources

Human resources quality is also a major influence in the determination of ISSM maturity. The top management defines the type and resources needful for quality human resources. To achieve this, there are important findings showing that ISSM maturity is achievable through quality human resources via good security management formal education, informal exposure, experience and defined security management expertise. With good staff exposure and clear management support and directive, a fluent communication will be achieved as represented by I7-AHS-PTS

Row: 311, clearly stating that staff are clearly communicated with when they need to exercise and practice ISSM, which are free and beneficial for the company. This means that a business that has clear directives from the CEO and staffs that are exposed to ISSM will result to good ISSM practices to the business.

"[Translated version] What they do (refer to the IT staff) on their own is security management practices which are without cost, for example hardening the server. This activity they will do it themselves. I do not need to inform them, they know this task" I7-AHS-PTS, Row: 311

Hence, to achieve ISSM maturity, good quality human resource is highly necessitated. Good quality human resources as discussed by the CEOs are the suitable people who will be able to handle and implement SM practices. They are usually with good experience in ISSM in businesses.

" You really have to find suitable person to handle this (refer to security management). It is really not easy to find someone..." I2-HS-TB, Row: 252-254

Good quality human resource with vast ISSM experience is not easy to find, as mentioned by I2-HS-TB Row: 252-254. This condition is agreed by I4-MD-SS Row: 124 where in I4-MD-SS business, this has influenced their decision to rely on third parties as they possessed SM experts or good quality staff who can handle ISSM for a business.

"... that is the reason why we rely on third party server, because they have a complete set of security. We definitely do not have the expertise to manage it" I4-MD-SS, Row: 124

5.3.3 (c) Utilization: Communication process

Utilization is also part of the organization factors which influence ISSM maturity. Utilization refers to the processes involved in the organization in communicating and carrying out SM practices. Proper work assignment reflects good communication process in a business. Each staff member is usually allocated with a clear job scope and responsibilities to perform the everyday work. A clear job scope and responsibilities are important and is highly influential as discussed

by I3-AR-HV Row: 51

“As we define security is a crucial issue in the business, we know who is responsible for what, and who is supposed to do specific task. We have to assign task properly. . .” I3-AR-HV, Row: 51

By having a good communication process during utilization of SM practices, the business has reflected the exercise of control in a business. In the security management scenario, proper work assignment is highly required where it will reflect responsibility of a staff member. By practising roles and responsibilities, it will be easier to detect misconduct according to the threats encountered in a business. Besides, the communication structure also shows how security management is communicated in the business. The majority of security management is formally conducted under the directive of the CEO. There may be some occurrences whereby simple security management is conducted by the staff as a security routine, which is well understood by the staff example simple SM practices like virus updates, patching and server hardening. Usually these tasks do not involve any amount of money.

“[Translated version] What they do (refer to the IT staff) on their own is security management practices which are without cost, for example hardening the server. This activity they will do it themselves. I do not need to inform them, they know this task” I7-AHS-PTS, Row: 311

5.3.3 (d) Slack

Slack is an influence towards achieving ISSM maturity in a business. CEOs involved in the interviews had mentioned this issue and the researcher found that this attribute is important due to the frequency of discussion on this matter. There is no standard definition of slack resources. However the most quoted definition of slack resources comes from Bourgeois (1981). Slack resources is the cushion of actual or potential resources, which allows an organization to adapt successfully to internal pressures for adjustment or to external pressures for change in policies, as well as to initiate changes in practice with respect to the external environment. The cushion of actual or potential resources in SMI/Es may not be common and may be scarce due to

their small business structure and limited resources. The qualitative analysis showed that slack does influence a business in ISSM implementation thus achieving ISSM maturity. Business resources and business requirements are low as mentioned by I4-MD-SS Row: 124, I7-AHS-PTS Row: 227, I2-HS-TB Row: 252-254 and I6-DL-US Row: 161.

“... that is the reason why we rely on third party server, because they have a complete set of security. We definitely do not have the expertise to manage it” I4-MD-SS, Row: 124

“As a business owner, I know it is important (referring to ISSM). But as an owner you know how much you want to put into it. Because I think our needs and requirements right now are consider quite small.” I7-AHS-PTS, Row: 227

“You really have to find a suitable person to handle this (ISSM). It is really not easy to find someone. Its about strength; you have to really use proper tools and proper expertise” I2-HS-TB Row: 252-254

“I see a need for that. Like what I have mentioned, it is based on the maturity of the company. As security is important, I realized that it all depended on the level of the company resources and focus” I6-DL-US, Row: 161

Findings show that slack resources determine ISSM maturity. Table 5.10 represent the analysis for organization related issues.

Table 5.10: Organization related elements of qualitative analysis

No	Themes from data analysis	Base theory	Relationship to theories	Organization-related elements issues reflected from analysis
1	Resources	TOE	TOE-Organization: Formal linking structure	a) formalization
2	Organizational structure	Organization Factors	TOE-Organization: Informal linking structure	a) Top management support
3	Organizational structure	TOE	TOE-Organization: Informal linking structure	a) Slack-Low business resources b) Slack-Low business requirement

5.3.4 Interview analysis: Section 3 - Environment-related elements

Findings from the interviews showed environment related issues are crucial in a business as they influence the business to achieve ISSM maturity. Under environment related elements there are (i) government regulations, (ii) technology support infrastructure, (iii) industry characteristics and market structure and (iv) user influence/satisfaction. All four elements were mentioned and discussed by the CEOs, hence found to be important in the ISSM maturity decision-making.

5.3.4 (a) Government regulations

Government regulations are mandatory for ISSM maturity. Under the government entity, three attributes which were found to be commonly discussed were the (i) government support systems, (ii) government readiness and (iii) legislation and guidelines. These three indicators address the issue surrounding the government regulations efforts. In the ISSM initiatives, the government must provide the support systems, for example special task force to assist SMI/E to implement its ISSM. One of the main functions of the task force could be to provide training to enhance skills of the business staff, awareness programs and funding/grants. For example a specific government initiated body mentioned by I1-KY-SW which oversee and advise security implementation in a business IS

“Cybersecurity has a grant that allows you to implement security. That is why we went to them. They are paying for consultants to look through our security management of the IS. They are experts and they kind of look at where we are weak on. We have applied for that, and we will be call for interview. I do not know whether I will get it, but they will advise us on what has to be done” I1-KY-SW, Row: 128

“If they can only allocate or put one of their campaigns or talks as security for e-commerce, I am sure everyone will turn up” I2-HS-TB, Row: 97

As for funding and grants, the government should provide this as part of the government regulation initiatives where it has to be developed to support a business in the context accordingly.

This means, government has to provide a support system based on the business type and business phases of the SMI/Es. This is important because each business is unique and requirements for each business differ in the SMI/Es. The government must also be ready to support the SMI/Es and implement ways to control and justify the grants given to prevent from misused.

As asserted by I5-NZA-GX in Row: 62, 80 and 52

“The government has many grants, but every time we apply we do not qualify for any grants. We are not start-up, however all available grants are for the start-up. My company have already been in the business for 8 years. What are we? We are at growth stage. The government have to prepare to deal with the growth of SMI/Es.” I5-NZA-GX, Row 62

“The government grants that are being given out to companies are not tailored to the service industries” I5-NZA-GX, Row 80

“If the government think there are abuse in the grants given, they just need to appoint trusted agencies or university that will come and help us implement the security management required. The priority has to be given to the company that the government believe they could benefit from it” I5-NZA-GX, Row 52

The government regulations also must provide the rules and procedures as a common standard for the usage of all SMI/Es. Besides, having smart partnership, soft loans and context-focus campaigns, one other important issue seen to be important in the government regulation is the legislation and enforcement. In terms of legislation, I4-MD-SS Row: 146 affirmed this;

“When the government mentioned on security implementation, this does not means to protect your business only but to protect the users. Most of the regulations are to protect the general public. It is good to have that. It will become standard implementation” I4-MD-SS, Row: 146

The same concern was demonstrated by I6-DL-US Row: 203, asserting the importance of guidelines, where specific authority must be given to control technology vendors and suppliers.

“The government has to make sure that the security systems such as in the hosting are based on guidelines, which needs to be imposed on the vendors.”

I6-DL-US in Row: 269 also affirmed that without the guidelines and enforcement, it will be dangerous for the SMI/E businesses because the vendors and suppliers could be an imposter who fakes all information provided, hence put the business at a risk.

“If there were no guidelines, or there were no one to monitor people doing the right way of e-commerce business, it can be very dangerous” I6-DL-US, in Row: 269

5.3.4 (b) *Technology support infrastructure*

Having the government regulations as affirmed by the CEOs are not the only external factors to determine ISSM maturity. Other frequently discussed issues for business to achieve ISSM maturity is the level of exposure that suppliers and vendors who are providing the technology support infrastructure. A majority of the CEOs agreed that the technology vendor highly influences the ISSM maturity. As asserted by I5-NZA-GX,

“I think it is about exposure, because readiness is not there, the environment here is not at the level yet. So I think it is more on the environment that we have that has not encouraged us to achieve the readiness level” I5-NZA-GX, Row: 22

Due to the technology of the vendors’ and technology manufacturers’ capacity, they are the most appropriate parties to disseminate information and provide ways to increase understanding towards types of ISSM features for the benefit of the business. I7-AHS-PTS Row: 29 and 39 and I4-MD-SS Row: 84 commented that vendors, resellers, software providers and manufacturers are the focal point to provide exposure appropriate with the capacity they own on the technology they are providing in ISSM.

“[Translated version] Unless vendors start to open their eyes, and start to focus to the SMI/Es market” I7-AHS-PTS Row:29

and

“[translated version] I think it has to start from the manufacturers, when manufacturers appoint focus resellers, then only it will work” I7-AHS-PTS, Row:39

“I think the software providers could be of help. This is because they provide most of the solution and experience” I4-MD-SS Row:84

5.3.4 (c) *Industry characteristics and market structure*

(a) Outsourcing: Another issue identified in the analysis is the outsourcing. Outsourcing has, in a way, shaped the SMI/Es implemented technology. Outsourcing has become an industry characteristic and market structure. The SMI/Es conduct outsourcing activities due to many reasons, including the outsource servicing company has the required capacity and expertise to implement the effective IS for SMI/E business usage. An excerpt from the transcription shows that I4-MD-SS employs an outsource service to support his business IS. This outsource service company usually provide technical expertises to the business, hence the SMI/Es are not required to employ technical expertise which will burden the business. Expertise is important because only competent staff can support ISSM implementation in any business to ensure ISSM maturity. It is affirmed by I4-MD-SS and I7-AHS-PTS from the interviews conducted.

“... that is the reason why we rely on third party server, because they have a complete set of security. We definitely do not have the expertise to manage it” I4-MD-SS, Row: 124

“[translated version] The third party who will provide us the services. They will have to provide us the security as much as possible. I do not want to do it in-house because I do not have experts. we do not have in-house experts” I7-AHS-PTS, Row: 227

“[translated version] It is better for the business to outsource. They have staff (experts) to look for it compared to the incompetent in-house staff” I7-AHS-PTS, Row: 485

Besides the outsource business technology capacity and expertise in the technology recommended, outsourcing helps the business to lessen overhead costs due to the high salary demanded by technology experts recruited to help define ISSM. This is affirmed by I7-AHS-PTS Row: 423.

“ This is common in SMI/E. I think the approach that we have take is outsource security. This is because you know you are not competent to do it in the company. Can you afford to hire? How much is their (experts) salary?”

5.3.4 (d) User influence/satisfaction

On many occasions, all businesses consider users as not having an influence over the SM practices, over the business IS in the SMI/E. However, in the current business environment, one of the most important business criteria is user requirement and satisfaction considerations. Users may want an easy system to use, however, with every improvement to provide better business IS example providing secure business environment for users, these users will appreciate the systems more, hence users will become accustomed to the SM practice and finally this will become the user requirement. A CEO who has implemented SM practices finds out that,

“AZ: When you implemented the particular security flow, does it bring any changes to the business?, HS: Yes of course. We make more profit. There is a small spike in refund rate, however our customers believe us more. We gain customers’ trust and our customers were validated” I2-HS-TB, Row: 242-243

It is also important to have user satisfaction for the business as part of the attributes to achieve ISSM maturity because from I5-NZA-GX Row: 139-142, she mentioned that,

“AZ: Basically, from your point of view, it is important to have security implementation and IT management. This is to make sure your business and processes are in control, GX: I find that this can satisfy our customer, AZ: Do you think it should satisfy the business, not just the customer?, GX: From my opinion, if it satisfies the business and my customer is not happy, I have done it wrongly”

Through the findings from the qualitative analysis, a conclusion could be made. The relationship of TOE is complex. SM practices showed influence in ISSM maturity were the findings were discussed in the interviews, e.g. in I3-AR-HV Row: 191, I3-AR-HV Row: 185, I6-DL-US Row: 203, I4-MD-SS Row: 124. The qualitative discussions concluded that SM practices are important to achieve ISSM maturity. It is also demonstrated in the discussion that the relationships between TOE attributes contributed towards SMI/E ISSM maturity. Table 5.11 represents the environment related issue findings of the qualitative analysis conducted.

Table 5.11: Environment related elements of qualitative analysis

No	Themes of analysis	Base theory	Relationship to theories	Environment-related elements issues reflected from analysis
1	Government	TOE	TOE-Environment: Government regulations	a) government support systems b) legislation and guidelines c) readiness
2	Technology Vendor	TOE	TOE- Environment: Technology support infrastructure	a) exposure
3	Outsourcing	TOE	TOE- Environment: industry characteristic/ market structure	a) business/technology capacity b) expertise
4	User influence	TOE	TOE- Environment: User influence and satisfaction	a) user requirement (secure IS applications) b) technology preferences

The qualitative findings shows that technology, organization and environment are dynamically related. It is shown in discussion of the qualitative analysis that technology, organization and environment attributes have to inter-relate to achieve the most conducive business condition in order to achieve ISSM maturity. Findings from the technology related issues discussed with the CEOs showed (i) technology availability and compatibility highly rely on the support of the technology vendors and suppliers, (ii) technology availability is dependent on the business age (legacy issues) (iii) technology availability and compatibility are highly influence by industry characteristics and market structure (open source initiatives and mature practices involved in the ISSM). Besides these it is also demonstrated by the CEOs that technology related issues are closely related to the organization issues, as technology has to be managed and controlled by human power to achieve the system's effectiveness.

As for the organization related issues, human resources and linking structures play important

role in ISSM maturity. A business can only achieve the intended ISSM maturity when organization attributes are inter-related. This means that the organization has to consider technological factors in deploying a specific process to support the business IS. If the business has failed to consider attributes own by a technological factors such as complexity of the technology or the relative advantage a technology owned, there will no dynamics in the business. It is shown in the discussion that communication process involved in the business is vital. However, the communication process in a business depends highly on the type of technology employed by a business to support specific process, where in this research context, process involved refers to the SM practices. Apart from that, formal linking structure in a business is highly related to the government regulations. A business can only formalize its business SM practices according to the government regulations and standards. The SMI/Es businesses must have a set of guidelines to exercise SM practices, which in this context, the government has to play an important role for this task.

Finally, the environment related issues, it is clear from the technology and organization above, the environment has shown an important influence in the ISSM maturity of a business. The (i) government regulations influences the business formalization activities, (ii) technology support infrastructure defines the task of a vendor or technology supplier to accommodate business requirement hence address slack issues in a business, (iii) industry characteristics and market structure discussed on the technology status available such as open source and the outsourcing trend of current market structure and the (iv) user influence or satisfaction. Both characteristics basically provide help to assist SMI/Es to achieve the ISSM maturity. Lastly are the inter-related issues between (iv) user influence/satisfaction with the organization and technology related issues. Here users influenced business to provide a secured IS by practising secured

business processes, which the business has to formalize. Secondly, users highly influenced the type of technology infrastructure or characteristics that the business must support. This is because users are the ones who own the devices and are the ones who will be using the system provided by the SMI/Es. For instance, a business has to make available secured mobile IS application as users in Malaysia consist of 42.6 million mobile subscribers with 143% of penetration rate (TheStar, 2013). This qualitative discussion complements the earlier quantitative findings, thus integration of the results are discussed in the mixed-method analysis, which is represented in the analysis integration and interpretation subsequent to this discussion. In conclusion, the researcher interpreted relationships with the factors identified, where association between these identified factors are presented in Table 5.12.

Table 5.12: Factor Inter-relationship from Qualitative Findings

No	Factors involved	TOE inter-relationship
Ir1	TECHNOLOGY and ENVIRONMENT	Technology complexity, capability and relative advantage are connected to how technology support structure by the vendors
Ir2	TECHNOLOGY and BUSINESS CHARACTERISTICS (INDEPENDENT FACTORS) and ORGANIZATION	Technology availability is connected to top management support, business size and business type. (This relationship is based on the researcher observation on the discussion. One SMI/E proved this relationship is important)
Ir3	TECHNOLOGY and ORGANIZATION	Technology characteristics are connected to the formalization conducted by the business
Ir4	TECHNOLOGY and BUSINESS CHARACTERISTICS (INDEPENDENT FACTORS)	Technology usage is related to business length (This relationship is based on the researcher observation on the discussion. There at least two SMI/E proved this relationship is important)
Ir5	TECHNOLOGY and ORGANIZATION	Technology availability is connected to the communication manner that happens in the business
Ir6	TECHNOLOGY and ORGANIZATION	Organization redundant resources can increase technology availability in the business
Ir7	ENVIRONMENT and ORGANIZATION	Government regulation is connected to type of formalization happens in the business
Ir8	ENVIRONMENT and ORGANIZATION	Industry characteristics affect the way of business formalization adopted by business
Ir9	ENVIRONMENT and TECHNOLOGY	Outsourcing has increased the technology availability and usage in the business
Ir10	ENVIRONMENT and TECHNOLOGY	User satisfaction is connected to how business leverages technology for its information systems

From the qualitative discussion and business observations, the researcher was able to conclude that the relationships of these identified TOE factors are very much influenced by the SMI/Es' forces which stimulate business to change and progress in the business ISSM implementation. Hsu et al. (2012) indicated in their research that in ISSM implementation of a business, institutional forces are important in a business and is not limited to technology alone. These forces drive changes and stimulate progress in a business which is highly required for the business to achieve ISSM maturity. This forces come from top management support and cultural acceptability (security culture e.g. security budget allocation, awareness, attitude, behaviour and competency in security-related necessities (informal security communication and security procedures) and maintenance (policies flexibility) in a business. These forces have encouraged

change or progress in the SM practices in the business. In order to understand the extent of each factor inter-relationship and the forces, the researcher conducted a quantitative and qualitative findings integration and interpretation discussed in the subsequent section. The identified forces associated to the inter-related TOE factors are presented in Table 5.13.

Table 5.13: Forces associated to TOE factors observed from the Qualitative Findings

No	Factors involved	Forces involved in the identified relationship
Id1	TECHNOLOGY and ORGANIZATION	Top management involves in all security effort conducted by the business
Id2	ENVIRONMENT and TECHNOLOGY	Business positively exercises security practices in the business using technology and environment support received
Id3	TECHNOLOGY and ORGANIZATION	Top management decides fully on security management practices in the business
Id4	TECHNOLOGY and BUSINESS CHARACTERISTICS (INDEPENDENT FACTORS) and ORGANIZATION	Business conduct compulsory security management education as part of business process
Id5	ENVIRONMENT and ORGANIZATION	Government regulates security management practices in business especially e-commerce business
Id6	TECHNOLOGY and ENVIRONMENT	Business is flexible to technology changes and positively adapt to changes
Id7	ENVIRONMENT and ORGANIZATION	Technology vendors highly force business security management users to implement state-of-the art security technology and applications
Id8	ENVIRONMENT and ORGANIZATION	Business conducts security management to secure applications to support their e-commerce

5.4 Quantitative and Qualitative Analysis Integration and Interpretation

The final stage of analysis is where the integration of both quantitative and qualitative results presentation happens. The integration and interpretation section, the quantitative and qualitative results are discussed and interpreted whereby the researcher will be able to deduce the TOE elements for the model building purposes. Figure 5.2, Figure 5.3 and Figure 5.4 shows all related TOE factors which were derived from the quantitative analysis. Discussion on all variables in these figures were discussed in the quantitative result analysis in Section 5.5.2. These factors are supported by significant relationship derived through the hypotheses assessment and

results were presented in Table 5.8. These findings, plus conclusions from the discussion in qualitative interviews concluded the elements which become the ISSM maturity factors. ISSM maturity factors consisted of three main ISSM elements, which are technology, organization and environment. ISSM maturity factors introduced the importance of coexistence of TOE in a business. The ISSM maturity factors are represented in Figure 5.8.

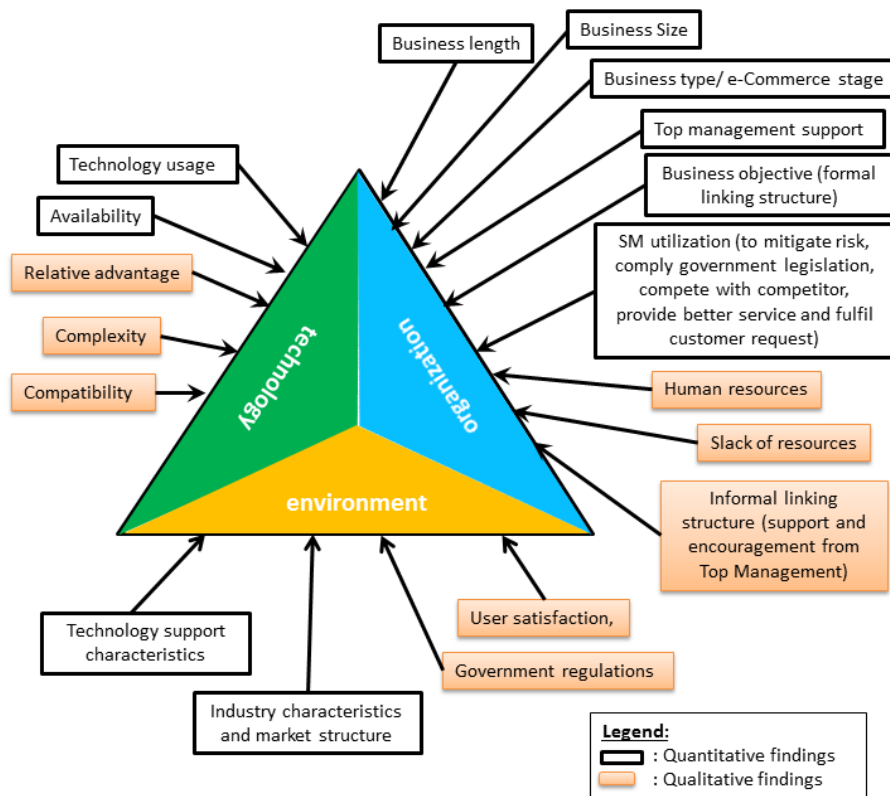


Figure 5.8: ISSM maturity factors derived from mix-method analysis

Through the integration of the quantitative and qualitative analysis, the research has identified factors influencing ISSM maturity as presented in Figure 5.8. The important factors representing the technology influence which define the state of technology on the SMI/Es. These include the (i) technology availability, (ii) technology compatibility, (iii) technology characteristics, (iv) technology complexity, (v) technology usage and finally the (vi) relative advantage provided by the technology. All these findings are presented and emphasized by the ISSM lit-

erature discussed in Chapter 2 including Hsu et al. (2012); Tsohou et al. (2010); Al-Awadi and Saidani (2010); Werlinger et al. (2009); Fomin and Vries (2008); Hu et al. (2007); Chang and Ho (2006); Prananto et al. (2003a, 2003b); Kankanhalli et al. (2003). As for the organization influence, factors representing the organization include (i) business length, (ii) business size, (iii) business type, (iv) top management support, (v) formal and informal linking structures, (vi) human resources, (vii) communication process and (viii) slack of resources. The same findings were represented in studies from Hsu et al. (2012); Monfelt et al. (2011); Yildirim et al. (2011); Tsohou et al. (2010); Da Veiga and Eloff (2010); Ozkan and Karabacak (2010); Chang and Ho (2006); Kankanhalli et al. (2003). Lastly under the environment influence, the researcher has successfully determined 4 important factors which are the (i) government regulations, (ii) technology support infrastructure, (iii) industry characteristics and market structure and (iv) user influence or satisfaction. Again scholars such as Hsu et al. (2012); Gillies (2011); Kraemer et al. (2009); Chang and Ho (2006); Farn et al. (2004); Kankanhalli et al. (2003) have highlighted these factors in their previous studies.

The qualitative analysis subsequently derived the factor relationship, through which the researcher has presented the factor inter-relationship based from the discussions of the interviews analysis (refer to Table 5.12). The researcher also identified forces that relate to the factor inter-relation which was presented in Table 5.13. The TOE factors are always inter-related and seldom being discussed separately. This is asserted by many studies in the ISSM, for example Hsu et al. (2012); Yildirim et al. (2011); Monfelt et al. (2011); Gillies (2011). As mentioned earlier in the qualitative forces determination, institutional forces are important elements for ISSM implementation (Hsu et al., 2012). According to Table 5.12 and 5.13, the researcher concluded that relationship between these two elements (which are factor inter-relation and

forces stimulating changes or also known as dynamic) into one table of relationship. The main reason of concluding these two findings together in this section of the analysis is to understand how both elements are related, hence promote business to achieve the ISSM maturity the business requires.

The integrative table of forces and TOE inter-relation present the importance of factors relationship towards ISSM maturity. As these two elements were observed in the SMI/Es conducted interviews, the researcher has evaluated the observed findings with seven randomly chosen SMI/Es interviews results to understand the extend of importance on both TOE inter-relation associated to the forces. The chosen SMI/Es were based on their business types or e-commerce stage. The SMI/Es must have achieved more than stage 2 for its e-commerce stage (business type). This is because; SMI/Es businesses which are in higher e-commerce stage must have practise strong security culture in order to mitigate their business risks especially when being online. The randomly selected SMI/Es must also display top management ISSM knowledge level of more than average. This is because with a higher level of ISSM knowledge possessed by the CEO, the better understanding the SMI/E has on the importance of ISSM implementation towards a business. Hence, top management support is predicted to be high. The demography of the seven cases are listed in Table 5.15. The demography of the business shows businesses are in stage 3 and above on its e-Commerce. The top management level also showed all top management have more than average knowledge in the ISSM implementation. Thus, issues of top management being oblivious with regards to ISSM implementations are not applicable here. There are high possibilities that the business forces/dynamics being high because all top management involved in this case are knowledgeable in ISSM. The conclusion of both TOE inter-relation and forces are represented in Table 5.14.

Table 5.14: Business forces associated to TOE inter-relation observed from the Qualitative

Findings

No	Factors involved	TOE inter-relationship	Business forces involved in the identified relationship (Dynamics)
1	TECHNOLOGY and ENVIRONMENT	Technology complexity, capability and relative advantage are connected to how technology support structure by the vendors	Business is flexible to technology changes and positively adapt to changes
2	TECHNOLOGY and BUSINESS CHARACTERISTICS (INDEPENDENT FACTORS) and ORGANIZATION	Technology availability is connected to top management support, business size and business type. (This relationship is based on the researcher observation on the discussion. One SMI/E proved this relationship is important)	Business conducts compulsory security management education as part of business process
3	TECHNOLOGY and ORGANIZATION	Technology characteristics are connected to the formalization conducted by the business	Top management involves in all security effort conducted by the business
4	TECHNOLOGY and BUSINESS CHARACTERISTICS (INDEPENDENT FACTORS)	Technology usage is related to business length (This relationship is based on the researcher observation on the discussion. There are at least two SMI/Es proved this relationship is important)	
5	TECHNOLOGY and ORGANIZATION	Technology availability is connected to the communication manner happens in the business	Top management decides fully on security management practices in the business
6	TECHNOLOGY and ORGANIZATION	Organization redundant resources can increase technology availability in the business	
7	ENVIRONMENT and ORGANIZATION	Government regulation is connected to type of formalization happens in the business	(i) Government regulates security management practices in business especially e-commerce business AND (ii) Business conduct security management to secure applications to support their e-commerce
8	ENVIRONMENT and ORGANIZATION	Industry characteristics affect the way of business formalization adopted by business	Technology vendors highly force business security management users to implement state-of-the art security technology and applications
9	ENVIRONMENT and TECHNOLOGY	Outsourcing has increased the technology availability and usage in the business	Business positively exercises security practices in the business using technology and environment support received
10	ENVIRONMENT and TECHNOLOGY	User satisfaction is connected to how business leverage technology for its information systems	

Using the seven business cases below, the factor inter-relation and business forces/dynamics are analysed. Each issue identified in each case is rated as “1” and for no issue identified is

rated “0” as depicted in Table 5.16 and Table 5.17.

Table 5.15: Seven cases business demography

Case No (C)	Business Size	Business Length	Business Type	eCommerce Stage	Top management ISSM Knowledge level
1	<10 staff 50K <= RM <= 99K	<= 3 years	product	stage 3	above average
2	<10 staff 50K <= RM <= 99K	<= 3 years	product	stage 3	above average
3	<10 staff 50K <= RM <= 99K	3 <= age < 5	services	stage 3	above average
4	<10 staff RM <= 15K	<= 3 years	product	stage 3	above average
5	10 < staff <= 30 15K <= RM <= 49K	6 <= age <= 9	product	stage 4	above average
6	<10 staff RM <= 15K	3 <= age < 5	product	stage 3	above average
7	10 < staff <= 30 RM > 100K	6 <= age <= 9	product	stage 4	above average

Table 5.16: Business forces and dynamics identified issues

No	Business forces and dynamics issues identified	C1	C2	C3	C4	C5	C6	C7
Id1	Top management involves in all security effort conducted by the business	1	1	1	1	1	1	1
Id2	Business positively exercise security practices in the business using technology and environment support received	0	1	1	1	1	0	1
Id3	Top management decide fully on security management practices in the business	1	1	1	1	1	1	1
Id4	Business conduct compulsory security management education as part of business process	0	0	0	0	1	0	1
Id5	Government regulate security management practices in business especially e-commerce business	0	0	0	0	0	0	0
Id6	Business is flexible to technology changes and positively adapt to changes	1	0	1	1	1	0	1
Id7	Technology vendor highly force business security management users to implement state-of-the art security technology and application	0	0	0	0	0	0	0
Id8	Business conduct security management to secure applications to support their e-commerce	1	1	1	1	1	1	1

Table 5.17: Factor inter-relation identified issues

No	Factor inter-relation issues constructed	C1	C2	C3	C4	C5	C6	C7
Ir1	Technology complexity, capability and relative advantage is connected to how technology support structure by the vendors	0	1	1	1	0	1	1
Ir2	Technology availability is connected to top management support, business size and business type	0	1	1	0	1	1	1
Ir3	Technology characteristics is connected to the formalization conducted by the business	1	1	1	0	1	0	1
Ir4	Technology usage is related to business length	0	0	0	0	0	0	1
Ir5	Technology availability is connected to the communication manner happens in the business	1	1	1	1	1	0	1
Ir6	Organization redundant resources can increase technology availability in the business	1	1	0	1	1	1	0
Ir7	Government regulation is connected to type of formalization happens in the business	0	0	0	0	0	0	0
Ir8	Industry characteristics affect the way of business formalization adopted by business	1	1	1	1	1	1	1
Ir9	Outsourcing has increase the technology availability and usage in the business	1	1	1	1	1	1	1
Ir10	User satisfaction is connected to how business leverages technology for its information systems	1	0	1	1	1	0	1

From Table 5.16 and Table 5.17, the findings are then calculated into average percentage of the SMI/E to determine the level of TOE factors inter-relation and forces/dynamics of the business. These percentages are presented in Table 5.18. The result shows level of TOE factors inter-relation, forces/dynamics of the business and the maturity level of the business. From the average percentage calculated, the researcher could conclude that for the business to be mature, the % of maturity must exceed 75%. For the business to achieved advanced level, reading of maturity is between 50% to 75%. All readings between 25% to 50% are considered as intermediate and any reading below 25% represents the novice stage.

Table 5.18: Percentage of Maturity in seven selected SMI/E

Case No (C)	Factor interrelation	Factor dynamics	Maturity percentage	Maturity level
1	60%	50%	55.56%	advance
2	70%	50.00%	61.11%	advance
3	70%	62.50%	66.67%	advance
4	70%	62.50%	66.67%	advance
5	70%	75%	72.22%	advance
6	50%	37.50%	44.44%	intermediate
7	80%	75%	77.78%	mature

In order to confirm the level determination, remaining cases involved in the qualitative investigations were compared and findings are presented in Table 5.19. From the percentage calculated as presented in Table 5.19, the % level or reading showed a similarity in terms of defining the maturity level of the SMI/Es. This demonstrates the TOE inter-relation and forces/dynamics are consistent within the multi-background of SMI/Es businesses.

Table 5.19: Percentage of Maturity in fourteen selected SMI/E

Case No (C)	Factor interrelation	Factor dynamics	Maturity percentage	Maturity level
1	20%	37.50%	27.78%	intermediate
2	20%	50.00%	33.33%	intermediate
3	20%	37.50%	38.89%	intermediate
4	20%	50.00%	44.44%	intermediate
5	60%	87.50%	72.22%	advance
6	20%	50.00%	33.33%	intermediate
7	60%	87.50%	72.22%	advance
8	20%	37.50%	27.78%	intermediate
9	20%	50.00%	33.33%	intermediate
10	20%	50.00%	33.33%	intermediate
11	20%	37.50%	27.78%	intermediate
12	30%	75.00%	50%	advance
13	20%	37.50%	27.78%	intermediate
14	20%	50.00%	33.33%	intermediate

The demography of the fourteen cases are represented in Table 5.20. Compared to the 7 cases

discussed above, the 14 cases are mostly in the stage 1 of e-commerce implementation level, where the CEO of the businesses possessed novice to average knowledge in ISSM implementation. This showed that between the 7 cases and 14 cases assessed, these 14 business cases should represent novice to advance ISSM maturity level.

Table 5.20: Fourteen cases business demography

Case No (C)	Business Size	Business Length	Business Type	eCommerce Stage	Top management ISSM Knowledge level
1	<10 staff 50K <= RM <= 99K	<= 3 years	services	stage 1	novice
2	<10 staff 15K <= RM <= 49K	<= 3 years	product	stage 1	average
3	<10 staff RM<= 15K	<= 3 years	services	stage 1	average
4	31 < staff <= 50 50K <= RM <= 99K	3 <= age < 5	services	stage 2	average
5	<10 staff RM <= 15K	<= 3 years	services	stage 2	average
6	<10 staff RM<=15K	<= 3 years	product	stage 1	novice
7	<10 staff 50K <= RM <= 99K	<= 3 years	services	stage 2	average
8	<10 staff 50K <= RM <= 99K	3 <= age < 5	product	stage 1	average
9	<10 staff RM< 15K	<= 3 years	product	stage 1	average
10	10 < staff <= 30 RM <= 15K	<= 3 years	services	stage 1	average
11	<10 staff RM<= 15K	<= 3 years	services	stage 1	average
12	<10 staff RM<= 15K	<= 3 years	product	stage 3	average
13	<10 staff RM <= 100K	<= 3 years	service	stage 1	average
14	<10 staff 15K <= RM <= 49K	<= 3 years	service	stage 1	average

The important conclusion here is that, all acSMI/E are influenced by the TOE factors interrelation and the business forces, identified in the qualitative stage of the analysis. The integra-

tion of quantitative and qualitative proved TOE factors inter-relation and forces consistency for all participating SMI/Es in this research. Hence, the research interpreted the ISSM maturity model must consider this condition besides the identified factors TOE from first research investigations.

5.5 Validity and Reliability of Data

5.5.1 Quantitative: Data Validity

Validity and reliability of scale were tested in consistency with the traditional research process (Neuman, 2009). In the quantitative research investigation carried out, there were two important validity concerns involving the instrument used during the research. These two concerns represent the validity of the instrument, which refers to the logical and empirical based. In logical based validity, the researcher focused on the content validity. The empirical based validity is conducted in the construct validity process. These two validity processes are conducted separately.

5.5.1 (a) Quantitative: Content Validity

Content validity is the degree to which items in an instrument reflect the content universe where the instrument will be generalized (Boudreau, Gefen, & Straub, 2001). Often this validity is achieved through literature review and an expert panel selected in this procedure. Content validity was carried out with five experts who have tested the questions' scoring or levels of scores (Lickert scales used) and the suitability of the content. Another content validity test was conducted through content validity score by Lawshe (1975). Although content validation procedures are highly subjective (Straub, Boudreau, & Gefen, 2004) where it usually depends

on the context of the research, these content validation procedures conducted are the common evaluation procedures in achieving content validity. Once all of the validation steps are successfully conducted, we can assume that the measurement model analysed has demonstrated its content validity (Urbach & Ahlemann, 2010). The researcher could then proceed with the data collection process once all of these steps have been conducted and assessed.

A content validity ratio (Content validity ratio (CVR)) was also conducted to identify that the responses received from the experts were essential. The CVR (Lawshe, 1975) was calculated based on the responses received using the CVR formula:

$$CVR = [(n_e - (N/2))/(N/2)] \quad (5.1)$$

where

n_e -number of the Subject Matter Expert or the panellists indicating "essential"

N -total number of the Subject Matter Expert panellists

Thus for this research the value of the CVR is:

$$CVR = [3 - (5/2)/(5/2)] = 0.2 \quad (5.2)$$

As asserted in (Lawshe, 1975), if the CVR equation takes on a value of between -1.0 and +1.00 this means that 50% of the number of N believed that the measurement item is essential. The value of CVR based on equation 5.2 is 0.20. This shows that the CVR result is more than 0.00. The result shows that the measurement items were essential.

As for the qualitative research investigation instrument, a content validation was carried out by four selected e-commerce business owners' higher management personnel. They are the CEOs and business owners. The objective of the content validation is to assess the content of the interview script and suitability of the interview to the remaining of the participants. The outcome from the validation process was mainly on the length of questions and technical terminologies mentioned in the semi-structured interview protocol. The researcher has conducted revisions based on the suggestions and the revisions were reviewed by the e-commerce business owner via email.

5.5.1 (b) Quantitative: Construct validity

The construct validity generally means the level to which an operationalization measures the concept it is supposed to measure (Boudreau et al., 2001; Bagozzi & Yi, 1988). Construct validity has become the fundamental issue in many organizational researches, as it is a measurement procedure. Measurement errors (commonly divided into random error and systematic error) influence the validity of the research findings. Hence, it is important that the researcher has to carry out validity of measure before testing or predicting any theory related to the research (Bagozzi & Yi, 1988). As asserted by Boudreau et al. (2001) the construct validity is important, firstly because it assessed the items in the construct are able to move together to become an intellectual whole, and secondly it rules out possibility of the construct being artificial, not directly observable in nature but is captured in the measurement model. Using PLS as a quantitative tool for analysis, all of these measurements were conducted during the assessment of the reflective measurement model. Results from quantitative assessment show significant coefficient value; hence demonstrate the high validity of the constructs. All results were discussed in the quantitative analysis discussion in Section 5.2.

5.5.2 Qualitative: Data Validity

As for the qualitative research investigation, validity is a concept which has been discussed in a wide range of terms. Qualitative research scholars accentuate validity issue as key issue because it determines legitimacy of qualitative research. This is because if qualitative research fails to consistently produce a valid result, prediction from this research cannot be relied on (Maxwell, 2004, 1998). Validity is a concept which has become an issue discussed in a wide variety of terms (Golafshani, 2003; Maxwell, 1998). Validity is very relative to and dependent on the community it accounts to (Maxwell, 2004, 1998) where it is tied to the processes and intentions of particular research methodologies and projects (Golafshani, 2003). Thus, on a whole, validity defines the degree of measures taken to investigate what the research intended to investigate, whether the researcher's observations reflect the phenomenon intended of the research (Kvale & Brinkmann, 2008).

5.5.2 (a) Credibility

Guba and Lincoln (1985) proposed two types of validity criteria, which are credibility and transferability in qualitative research. Following these two recommended criteria, the researcher is able to assess transferability. Credibility is conducted through member checks (Shenton, 2004) where it looks at how legitimate the results are to the participants. In this research, the results were reported back to the participants where comments were mostly received during the personal meet-ups and phone calls with the participants after the interviews. The researcher also welcomed comments from participants through emails, unfortunately no comments were written as a majority of these CEOs are more comfortable with face-to-face communications.

5.5.2 (b) *Transferability*

Transferability defines the extent to which the findings of one research can be applied to other situations (Merriam, 1998). In the context of this research, the qualitative data involved a small number of business individuals with limited amount time to conduct on-site data collection and observation (Shenton, 2004). Generalization of the qualitative analysis is no longer applicable based on the limited research context. However, with the concern on transferability issues of the qualitative investigations, this research is able to derive with specific conclusions based on the specific business context defined in this research. Findings are very much based on specific business context in the SMI/Es in Malaysia, which reflected the micro-SMI/Es that conducted the e-commerce business. Hence, the conclusion of the ISSM maturity model design highly supports this business context.

5.5.3 **Reliability in Quantitative and Qualitative Data Analysis**

5.5.3 (a) *Reliability in Quantitative Data Analysis*

Reliability determines measurement accuracy. It determines that the instrument produces consistent and error-free results (Maxwell, 2004; Boudreau et al., 2001; Maxwell, 1998). Hence reliability is very important in any research. In a quantitative analysis, reliability is conducted during the assessment of the reflective measurement model. The reliability of the instrument is assessed using the composite reliability, Cronbach's Alpha and R^2 reading analysed using the SmartPLS software. In conclusion, the quantitative data analysis of this research achieved high reliability score as the coefficient value of all assessment mentioned are reported to be at a significant level. The results showed all composite reliability and Cronbach's Alpha values are

above 0.8 which proved to be reliable. As for the R^2 values involved in this research, showed average to substantial explanatory power, whereby this research is able to address average to substantial issues involved in the ISSM maturity. Further discussions on all this results can be found in Section 5.2.

5.5.3 (b) Reliability in Qualitative Data Analysis

The reliability issues in qualitative research have received mixed opinions as discussed in (Golafshani, 2003). Reliability in qualitative research requires researchers to be consistent in the research process for further replication by other researchers (Alfawaz, 2011). Having a research protocol for the qualitative investigation and applying more than one data collection source (Yin, 2008; Miles & Huberman, 1994) may help increase reliability in qualitative research. The concept of reliability emphasized on the quality of data involved in the qualitative investigations. Here, the researcher employs the interview protocol and two types of qualitative data collection to ensure reliability of data.

5.6 Conclusion

Quantitative analysis determines the factors which influence the ISSM maturity. These factors were presented in Section 5.5 which was earlier agreed by many ISSM scholars discussed in Chapter 2. The qualitative analysis demonstrated the factor relationship, whereby the TOE factors inter-relation and forces were found to be associated in defining the relationship. However, security management practices do not seem to be mediating the ISSM maturity as presented in the hypothesis results of Table 5.7. The mediation relationship may not be reflected well based on the hypotheses result due to the reason that the respondents for this research were not

too many. Therefore, the researcher has conducted a qualitative research investigation to complement results derived from the quantitative analysis. Through the qualitative investigations, many inputs were received from the SMI/E CEOs and business owners. Many agreed on the importance of security management practices which has influence towards business ISSM maturity. It is important for SMI/E e-commerce businesses to define their technology, organization and environment factors, before aiming for ISSM maturity. By identifying these factors, the businesses will be able to define the relationships between the factors and fixed any in appropriate connection to work on business ISSM maturity. Through the quantitative and qualitative analysis integration and interpretation, the researcher is able to demonstrate the level of maturity score for the purpose of model building in Chapter 6. This maturity scores were derived based on the analysis of factor inter-relation and business forces/dynamics which were identified from the discussion of the qualitative analysis.

CHAPTER 6

MODEL BUILDING

6.1 Introduction

The model building chapter describes how the ISSM Maturity framework is built. In this chapter, discussion on ISSM maturity model is conducted. This chapter involves the model building process and ISSM prototype discussion. The model building process involved three basic steps which include model selection, model fitting and model validation (Sematech, 2012). In the model building chapter, the researcher has focused on the proposed ISSM maturity model based on the findings discussed in Chapter 5. The designed ISSM maturity model reflects the current ISSM maturity standards issues. However, issues of consideration differ as this research concentrates on the socio-technical factors identified in the data analysis as compared to ISSM maturity standards, which emphasized on purely security management matters.

It is important for the researcher to differentiate model building and theory building. Model building is not similar to theory building as theory building requires on going comparison between data collected and theory (Glaser & Strauss, 1967). Theory building refers to the process or recurring cycle by which coherent descriptions, explanations, and representations of observed or experienced phenomena are generated, verified, and refined (Lynham, 2000). Model building involves a simpler approach in formulating ideas representation in order to achieve specific goals, such as achieving ISSM maturity in a business.

6.2 Model Building Process

The model for ISSM maturity is designed based on the findings of the mixed-method research investigation conducted earlier. The model construction begins by defining the model selection, followed by model fitting and finally with model validation (Sematech, 2012). Using these three simple steps, research described the model building process in developing ISSM maturity model as Figure 6.1 below.

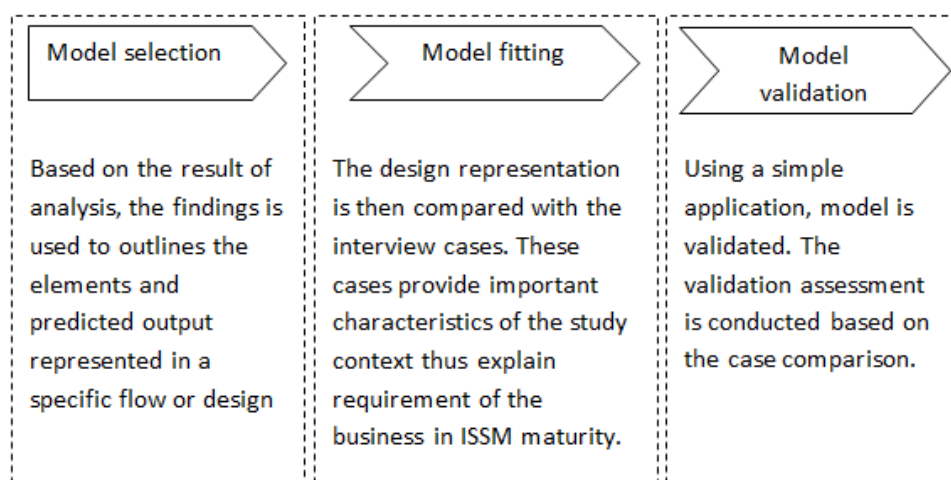


Figure 6.1: Model Building Process

The model building process stages are discussed in the next section according to the work conducted in this research.

6.2.1 The Model Selection

Through the analysis of the results, a few important characteristics were identified. The independent elements in the conceptual relationship presented in Chapter 3 demonstrated varied results after the quantitative and qualitative analysis. The top management support is the dominant variable from the organization factor that influenced the SMI/E ISSM Maturity. The

mixed-method analyses also inferred that different sizes of business projected different levels of ISSM maturity. The demographic information reflected that businesses with a bigger number of staff (bigger in size) have different perspectives and implementation of ISSM in their businesses. These businesses are deduced to have higher ISSM maturity level than the smaller business. These businesses show a range from intermediate to advanced ISSM maturity levels in their e-commerce from the mixed-method analysis integration and interpretation. To directly assess the SMI/E ISSM maturity using current ISSM maturity framework may be difficult, as they have not implemented detailed security management solutions recommended by the ISSM maturity standards. It is even more difficult to recommend to these businesses the appropriate ISSM practices, if the SMI/Es are not able to gauge their business capability. In this research context, the SMI/Es business capability is based on the TOE factors identified as the main influence of ISSM maturity. These TOE factors are similar factors deduced from the SM practices which assist a business to achieve its ISSM maturity. As such, the ISSM maturity model were designed and developed based on the TOE factors identified and interpretation from the mixed-method research conducted in Chapter 5. The ISSM maturity model for SMI/E with e-commerce will provide the basic identification of the business position based on TOE elements involved in their businesses. It is through this identification that business will then be able to determine what type of ISSM maturity level in accordance to standards so they could achieved the ISSM maturity based on their current business TOE capabilities.

Before the four quadrants were deduced, few models of maturity were compared and contrasted for the purpose of model building. Based on the literature analysis in Chapter 2, there are three maturity models being compared which were the maturity levels SSE-CMM (Carnegie-Mellon, 1999) or currently known as the ISO/IEC21827:2008 (as presented in Figure 2.6), the Information Security Program Maturity Grid (Stacey, 1996) defined in Table 2.5 and the information

security management maturity model (ISM3) (Aceituno, 2006a) discussed in Table 2.7. From the literature review, all maturity levels were determined according to grid from level 1-5. The maturity levels were determine according to the process that the business has taken rather looking at the level of TOE factors and business forces/dynamics. In this research context, it focuses on the maturity level development on the four quadrant because this research wants to assist the SMI/Es determine their business capabilities through the TOE factor identifications and the forces each business have to drive ISSM. These socio-technical factors are the basic rules towards achieving ISSM maturity as discussed by many scholars in Chapter 2. Following these discussions, the findings determine four main sections of ISSM maturity level which are the novice, intermediate, advanced and matured. The sections were divided in four quadrant as in Figure 6.2. The discussion of each quadrant is dissected and discussed in the model deduction.

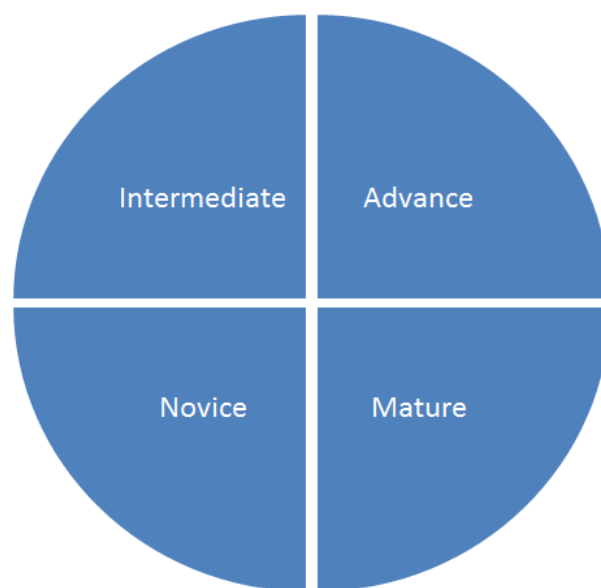


Figure 6.2: Four quadrant of ISSM model

6.2.1 (a) *Model deduction*

(i) Novice stage deduction The novice stage is the stage where businesses are able to define organization, technology and environment elements associated to ISSM maturity. Unfortunately, the SMI/Es are still ineffective in inter-relating the TOE factors available in the business. At the novice level, inter-relation of the TOE factors are very minimal. The forces/dynamics are also very low, as the business focus is on the other matters besides ISSM implementation. There is also a high probability that the top management support was minimal in the ISSM, hence this is reflected in the low inter-relation of TOE factors and forces/dynamics in the business. This level shows zero (0) level of ISSM maturity. Based on the analysis, there are no surveyed respondents that reflect this stage. Although this stage shows failure of the business in exploiting the identified items of TOE in the business, however the business managed to classify and identify the TOE elements involved in the business. This situation occurs because of many situations, some them have been mentioned in the analysis where these include the failure to identify business related TOE factors. As for the business forces/dynamics, the forces identified were minimal where many of the discussions highlighted the low exposure was one of the vital reasons. Knowledgeable staff, top management support and vendor support are the most common issues associated to business exposure.

Due to the minimal association between the TOE factors taking place in the business, it is impossible for the business to determine steps on exercising ISSM maturity standards to further reach their ISSM maturity goal. At this point, the business is either less aware of the implication of the ISSM or its usage, and support are very minimal for the security management practices. As such the three rings of TOE factors are arranged close to each other without overlapping as depicted in Figure 6.3. As many SMI/E business involved in e-commerce are usually at the

early stage of understanding ISSM and its importance towards business, the interrelation among the TOE factors may still not be achieved. Through this representation we could deduce that early and less-knowledgeable businesses are among the businesses in this novice level. There may be other types of businesses in this level, for example SMI/Es with e-commerce that do not involve transactions, but in this research context, businesses in the novice level are mostly involved in the category of early e-commerce entry. Most commonly, the top management also possessed little knowledge in the ISSM implementation. The Venn diagram of Figure 6.3 depicts the situation of TOE inter-relation and forces in the novice category.

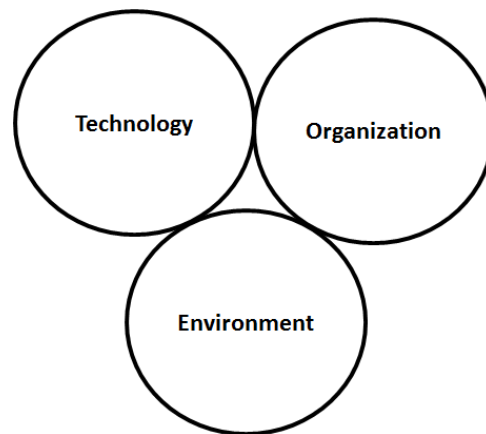


Figure 6.3: Independent circles of TOE in the Novice level

(ii)Intermediate stage deduction Similar to the novice stage deduction, the intermediate stage deduction for the ISSM maturity framework is also based on the analysis of the data collected from the earlier research investigations. The intermediate stage defines that the connection of the TOE factors are at an intermediate or moderate point of interaction. This shows small factor inter-relation and business forces/dynamics. This means, for example, management of the organization has shown support towards security management by leveraging the related technology factors. It is also braced by the environment factors, for example the ven-

dors and suppliers who have given the right amount of support to the business. The technology used also moderately supports the ISSM implementation of this business. The usage of technology in the organization and the support from the environment are in moderate manner to support the ISSM of the business. There is also a number of strong factor inter-relation and dynamics involved in this stage, however it is very minimal. The strong factor inter-relation and forces/dynamics are situated in the middle of the Venn diagram depicted in Figure 6.4. From this diagram, the researcher concluded that there are interrelationships between the organization and technology and environment, and vice versa, but not many identified TOE factors were exercised in the SMI/Es to reach a matured ISSM level. There are also still many other TOE factors in the business which are not linked. For example, technology and environment factors such as the government regulation and formalization of SM practices in the business (which are commonly found in SMI/E currently). As such, only an intermediate level of TOE inter-relation and dynamics have been achieved in this quadrant. The intermediate stage could be deducted as Figure 6.4

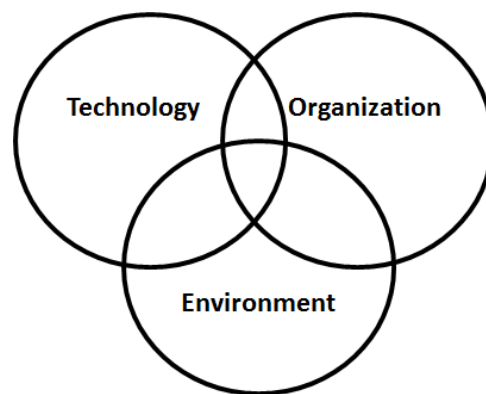


Figure 6.4: TOE factors interrelation and forces in the Intermediate Level

(iii) Advanced stage deduction The advanced stage represents a higher factor inter-relation and dynamics compared to the intermediate stage. Figure 6.5 shows that the TOE factors are

associated at an improved level, progressing from the intermediate level previously. This involved high association of TOE factors to achieve an advanced stage of ISSM maturity. It infers that the business has fully utilized the technology usage, characteristics, availability and other related factors at its full capacity. This is achieved through leveraging the organization factors and complemented by the environment factors mentioned in Chapter 5. Through having these dynamics, businesses could accomplish an advanced ISSM stage of maturity. The relationships of factors showed that with the maximum association of TOE factors, and business forces/dynamics, the SMI/Es are able to utilize full business capacity associated to the TOE factors owned by the businesses. According to the analysis, the advanced stage is deduced as Figure 6.5. This level shows bigger overlapping between the TOE factors. As such a bigger inner circle is achieved. This represents a higher TOE factor inter-relation and business forces/dynamics available and exercised effectively in the SMI/Es. Hence, through this understanding, the SMI/E is able to leverage business advantage to exercise ISSM towards maturity.



Figure 6.5: Overlapping circles of ISSM dynamics of Advance level of ISSM

(iv) Matured stage deduction As for the matured stage deduction, it is predicted that the business is able to leverage the relationship between all TOE factors to the level where these relationships have become business routine. The matured stage of ISSM requires all three fac-

tors to inter-relate and blend to become the business's core activity. It is in this level, that all three factors are able to bond, where through this connection; businesses will be able to enjoy the benefits at the maximum level. However, according to the literature review, this stage seems unrealistically achievable due to the technology-related reasons which are impossible for SMI/Es to address total technology attributes as they have limited technology resources. This also due to the slack issues commonly found in the SMI/Es because SMI/Es seldom have the cushion of resources since they are newly start-up businesses, with limited organizational resources (especially human resources), and not much experience in the business. Finally, the environment neglect is also another problem SMI/Es face as these businesses are struggling with government regulations and enforcement. The government enforcement can be very expensive, for example implementation of specific security standards in the business. As such, in the matured stage, the researcher deduced a ISSM maturity model that incorporates all TOE factors and forces in one single ring as it defines total factors interrelationship and high business forces/dynamics.

As technology keeps changing and e-commerce is a volatile business, ISSM implementation has to follow the movement of these influencing factors. Although this situation is seldom achieved by the SMI/Es, analysis of the research showed that there is possibility for a business to achieve ISSM matured stage. From Chapter 5, there is a single SMI/E who has achieved the matured stage of TOE factors inter relation and forces/dynamic in the business. Observations from the interviews conducted by the researcher deduced that the 7 SMI/E cases from the case comparison showed high knowledge of the CEO on the current TOE factors involved and required in the business. The CEO is highly motivated and knowledgeable in the ISSM and SM technology alternatives, which makes the business flexible towards changes in the complex

world of e-commerce business. Due to the CEO's high motivation, it has created a positive business culture in SM practices, hence promote the business revenue which currently make this business a leading book publisher in Malaysia. Figure 6.6 shows the matured stage of ISSM in the SMI/Es studied context. The ability to leverage on TOE factors to its fullest is crucial, which has to be championed by knowledgeable and highly motivated top management.

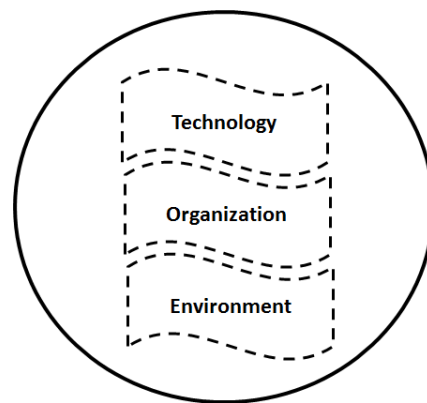


Figure 6.6: Matured ISSM quadrant

Using these four stage deductions, each deduction is then arranged in the four quadrants determined earlier. The identification of a quadrant is made due to the fact that all businesses had to go through a cycle of business improvement process. The arrow represents the business conditions which developed from the novice stage to the intermediate, and then advances through to the matured stage. The ISSM maturity quadrant as Figure 6.7 below is designed to represent each of the stages discussed in the model deduction.

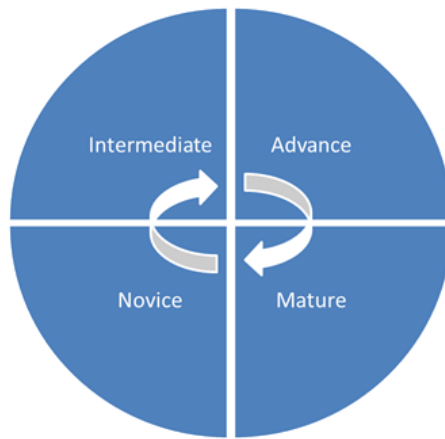


Figure 6.7: Four-quadrant model of ISSM maturity

Each stage is then represented in the ISSM maturity model as in Figure 6.8 below. All models deduced are derived from the understanding made from analysis integration done in Chapter 5. Each quadrant is represented by its appropriate TOE representations. The “novice ring” in the novice stage, the “intermediate relation diagram” in the intermediate stage, the “flower blooms” in the advanced stage and finally the “TOE globe” in the matured stage.

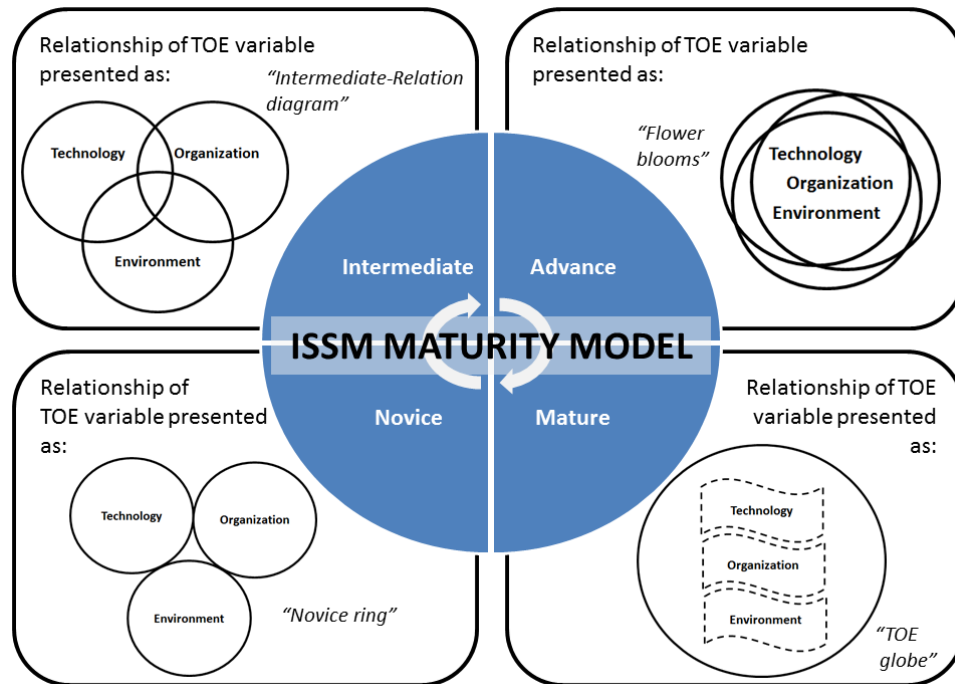


Figure 6.8: ISSM maturity model

The next step in model building is the model fitting process. The discussion on model fitting process refers to the seven cases as findings presented in Table 5.18 to find the suitability of the depicted ISSM maturity model.

6.2.2 The Model Fitting

The model fitting process involved tasks to identify whether selected designed model is applicable in the context of the research. Straightforwardly, it means to assess the designed model based on using samples or cases. In this research, the cases were built based on the analysis of the one-to-one interviews, which were carried out earlier in this research. Seven cases were compared and contrasted following the ISSM maturity dynamics-related issues. The TOE factors inter relations and the forces/dynamics were deduced during qualitative analysis in Chapter 5 and were assessed in the mixed-method analysis integration and interpretation. All assess-

ment were discussed in Chapter 5.

These seven cases were compared based on the issues identified and have been analysed in Section 5.3. The result from the seven cases proved that the maturity levels are according to the four quadrants of maturity levels, starting with novice, intermediate, advanced and finally the matured level. The level for each quadrant comes from the summation of TOE factors inter-relation with the business forces/dynamic and is deduced in a percentage. The maturity quadrant is deduced according to a quarter from novice, intermediate, advanced and matured. Readings below 25% is the novice stage and percentage score of more than 25% and less than 50% is referred to the intermediate stage. Readings above 50% but less than 75% represented the advanced stage, and finally all readings of more than 75% indicate a business in the maturity stage. This reading is used as the average of total TOE factors inter relation with the forces/dynamic defined in the qualitative analysis. The reason of using this reading scale is that assessment conducted in Table 5.18 showed four different ranges of maturity levels from the total of 100%. However, to determine the business is in the appropriate quadrants, the business must be able to address the TOE factors interrelation and forces in the appropriate maturity levels. If one of the issues is addressed in a lower maturity level than other one, the business is deduced to be in the lower rank of maturity levels. This is because from the qualitative discussion, all CEOs have addressed the importance of issues consistency between factor inter-relation and business forces/dynamic. Both issues have to be at the same level of maturity to achieve the specific maturity level in the ISSM maturity. This means SMI/Es need to reach both readings in the factor inter-relation and forces/dynamics of more than 75% to reach the matured stage. Without 75% factor inter-relation and forces/dynamics, businesses are still considered as being in the advanced stage, because a matured ISSM requires high factor inter-relationship

and high forces/dynamics in their businesses. These applies to all levels of maturity.

Table 5.18 shows the maturity reading for the seven cases selected. The detailed analysis of factor inter-relations and forces/dynamics identified were carried out in Chapter 5. Comparison of the cases showed five cases in the advanced stage, one case in the intermediate stage and one case in the matured stage. There is no case that falls under the novice stage. This finding reflects that SMI/Es with e-commerce are ready and equipped to exercise ISSM maturity standards available in the market.

In Table 5.15 in Chapter 5 page 179, SMI/Es demography of these seven cases were presented. From the business demography, the researcher deduced that businesses which are bigger in size and have been in the business scenario for a longer time usually have a higher reading of maturity as compared to the remaining cases. These findings agreed with the literature review discussed in Chapter 2, that business size and business length influenced the ISSM maturity of the SMI/Es. Business length provides an experience advantage compared to the new SMI/Es, as such the business force and dynamics is higher. All top management equipped with above average ISSM knowledge, and have highly reflected this on the maturity score of each business in the seven cases compared.

6.2.3 The model validation

In the model validation, assessment is carried out to measure the selection of the model using the model fitting exercise. The model validation is conducted based on the respondents gathered during focus group sessions. There were fourteen SMI/Es involved in this validation purpose. The results were presented in Table 5.19. These SMI/Es are involved in e-commerce

from a small to large scale, where the majority are still at the early stage. The objectives of the model validation exercise are to compare and contrast the ISSM maturity model designed earlier in model selection, validate the model fitting exercised and thus conclude the findings. The findings represent the applicability of the ISSM maturity model developed.

In this validation process, most of the CEOs have novice to average knowledge of ISSM implementation compared to the earlier group in the model fitting. The earlier cases were set to be compared with the validation process cases for the purpose of validating the model built. The business types varied from product offerings to services. These businesses were small in size with the majority of the business income annually from e-commerce activities still being small. Table 5.19 represents the assessment conducted for model the validation purposes.

It is expected that there will be contrasts between the cases comparisons as there were differences in business size among these cases. Through the assessed issues, the findings show that the majority of the businesses are in the intermediate stage of ISSM maturity. Three SMI/Es have reached the advanced stage, with readings of more than 50% of factor inter relations and business forces/dynamics. No SMI/Es achieved the matured stage as there was no SMI/E that achieved a reading of more than 75% in each of the factors analysed.

There is no major comparisons shown between these businesses in terms of business size with the maturity level of a business. Comparison between top management ISSM knowledge possessed by all SMI/Es did not show any major comparison either. Most of the CEOs agreed they have the novice to average level of knowledge of ISSM implementation. However, at the observation during the focus group conducted, two CEOs were categorized as having more ex-

perience than the rest in terms of ISSM implementation based on their previous professional exposures. These two CEOs were previously involved in the corporate business focusing on ISSM related implementation, before they ventured into their own businesses. These two businesses show advanced ISSM maturity level. The two SMI/Es are in advanced level, where the factor inter relation and business forces/dynamics are highly inter related compared to the rest of the SMI/Es. The rest of the CEOs not have achieved the average ISSM knowledge.

A validation process was also conducted with the five experts previous who were involved in the initial validation process at the beginning of this research. The researcher discussed about the designed ISSM model together with the findings on the factor inter-relations and business forces/dynamics, which were derived from the analysis of the findings. Separate meetings were conducted with five different experts. The meetings were conducted in the experts' office. In the validation process, the researcher had highlighted on the research findings which were the factor inter-relation issues and the business forces/dynamics, plus the 4 defined quadrants of four types of maturity stages. Mixed inputs were received in the factor inter-relation issues and the forces/dynamics as presented in Table 6.1. However, all five experts agreed to the four quadrants presented in this research. A simple evaluation form was used to in this validation process. The evaluation form consisted of the objectives and scope of the evaluation, the factor inter-relation issues and the forces/dynamics. These issues were assessed based on Likert scale of 1-5, where 1 is slightly agree, 3 is moderately agree and 5 is highly agree. The results were presented in percentage (%) to show the importance of these factors towards the research.

Table 6.1: Expert Validation Result on Factor Inter-relation and forces/dynamics

NO	Factor inter-relation (Ir) and Forces/Dynamics (Id)	Ir1	Ir2	Ir3	Ir4	Ir5	Ir6	Ir7	Ir8	Ir9	Ir10	Id1	Id2	Id3	Id4	Id5	Id6	Id7	Id8
1	Expert 1	5	5	1	1	3	3	5	5	3	1	5	5	5	5	3	3	1	5
2	Expert 2	5	5	5	1	5	3	5	5	5	5	5	5	5	5	5	5	1	5
3	Expert 3	3	5	3	3	5	3	5	3	3	5	5	5	3	5	5	3	5	5
4	Expert 4	3	5	3	5	5	3	5	3	1	5	5	3	5	1	5	5	3	5
5	Expert 5	3	5	5	3	5	3	5	5	3	3	5	5	5	5	5	5	5	5
Total sum (Σ)		19	25	17	13	23	15	25	21	15	19	25	23	23	21	23	21	15	25
Percentage (%)		76	100	68	52	92	60	100	84	60	76	100	92	92	84	92	84	60	100

Note: Ir represents item discussed in factor inter-relation

Based on the Table 6.1 above, the researcher deduced that all factors were average to high in percentage referred to the research context. All factors are between 52% to 100% related. There were two factors inter-relation and two business forces/dynamics considered to be highly important to ensure the ISSM maturity in a business. These two factors inter-relations were Ir2: Technology availability are connected to top management support, business size and business type and Ir7: Government regulation is connected to type of formalization happened in the business. As for the business forces/dynamics, the Id1: Top management involves in all security efforts conducted by the business and Id8: Business conducted security management to secure applications to support their e-commerce.

6.3 Case conclusion and findings

The seven of businesses cases from the one-to-one interviews were used in the model fitting process to determine the quadrants and level of maturity. The remaining business cases consisted of fourteen SMI/Es, were then used to confirmed the designed quadrants and lastly, the five experts were called to conduct the validation on the designed model. Three different sets of group were involved in this model building purpose is to ensure that each step of the development was assessed accordingly. All businesses involved in the research are unique in nature,

however selection of respondents for the research had been conducted earlier. Hence, there are no issues on comparison should occur as selection had already being conducted in the earlier stage of the research. From the assessment conducted, the researcher deduced below conclusions:

- (i) Business size influences the ISSM maturity level.
- (ii) The longer a business has been involved in e-commerce, the higher the business forces or dynamics thus increasing the tendency to implement ISSM effectively.
- (iii) The ISSM knowledge levels (deduced from the Table 5.15 and Table 5.20) amongst the CEOs do not directly affect the ISSM maturity. However, observation during the interviews showed that the CEOs' ISSM experience were connected to the ISSM maturity of a business. The SMI/Es CEOs who had previous professional experience in SM were highly passionate in ISSM maturity as they understood the importance and benefit ISSM brings to the business, hence these CEO are very attentive to all technology development, its risks and benefits towards the business.
- (iv) Both cases (in model fitting and in model validation) agreed that TOE factors inter relation and business forces/dynamics have higher influence towards ISSM maturity as compared to business characteristics alone, which are business size, type, length in business and knowledge.

The factor inter-relation and forces/dynamics occurred in each stage were reflected by the results from the validation conducted with the experts. In the novice stage, there were no factor inter-relation and forces/dynamics identified. In the intermediate maturity stage, there were four proposed issues from factor inter-relation and forces/dynamics within the most inner portion of the Venn diagram. These issues were 100% agreed by experts through the validation process. The issues consisted of: Ir2: Technology availability is connected to top management

support, business size and business type and Ir7: Government regulation is connected to type of formalization happened in the business, Id1: Top management involved in all security efforts conducted by the business and Id8: Business conducted security management to secure applications to support their e-commerce as depicted in Figure 6.9.

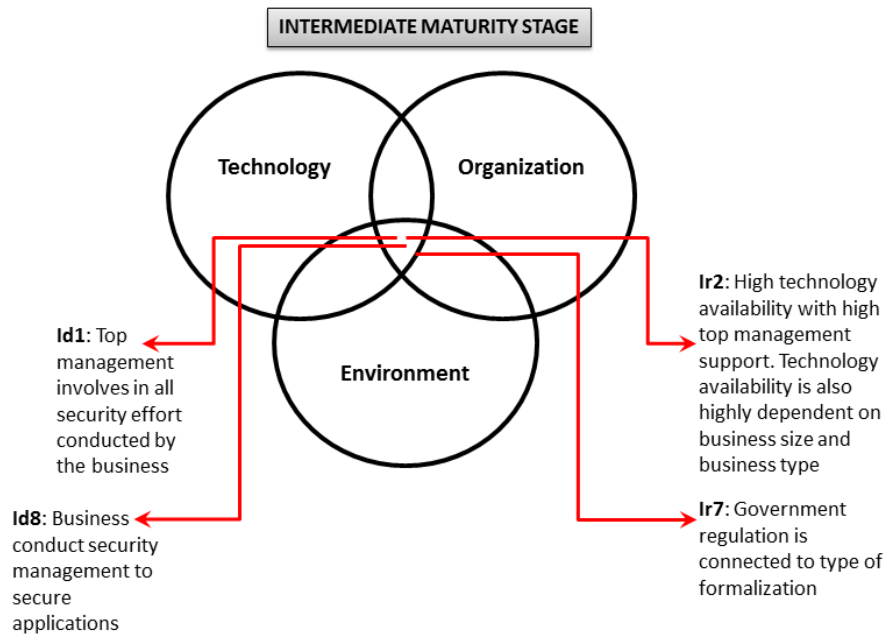


Figure 6.9: ISSM maturity in intermediate maturity stage

As for the advanced maturity stage the factor inter-relation and forces/dynamics were depicted in Figure 6.10. In advanced stage, it involved six factors inter-relation and seven forces/dynamics in a business as discussed earlier in Chapter 5. As for the matured stage, all factors were expected to inter-relate and supported by business forces. Hence, all factors were inter-related and forces/dynamics were well positioned in the business. The Figure 6.11 represent the matured stage involving all factors involved in the ISSM matured business.

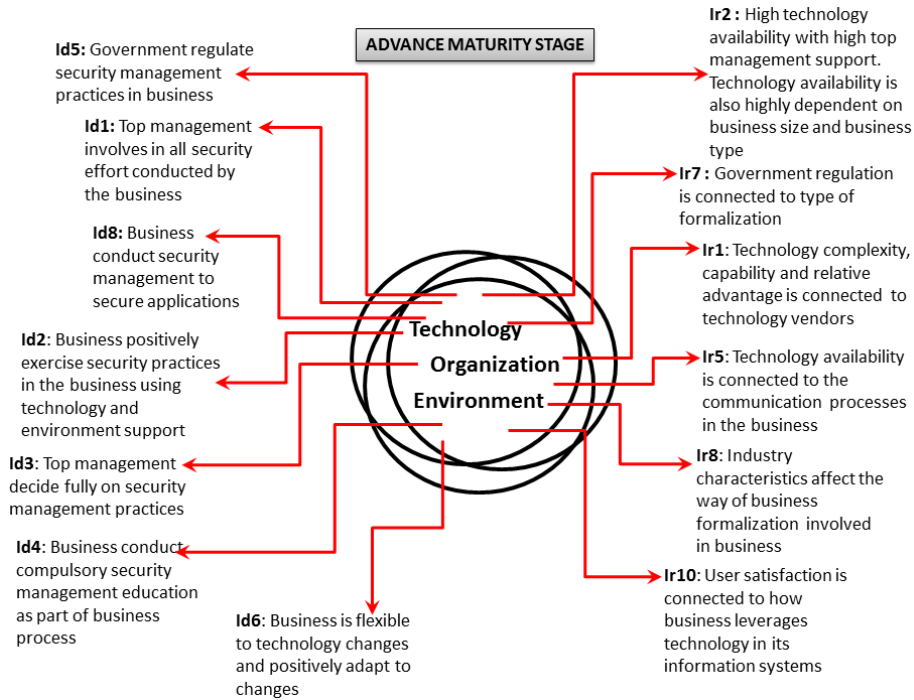


Figure 6.10: ISSM maturity in advanced maturity stage

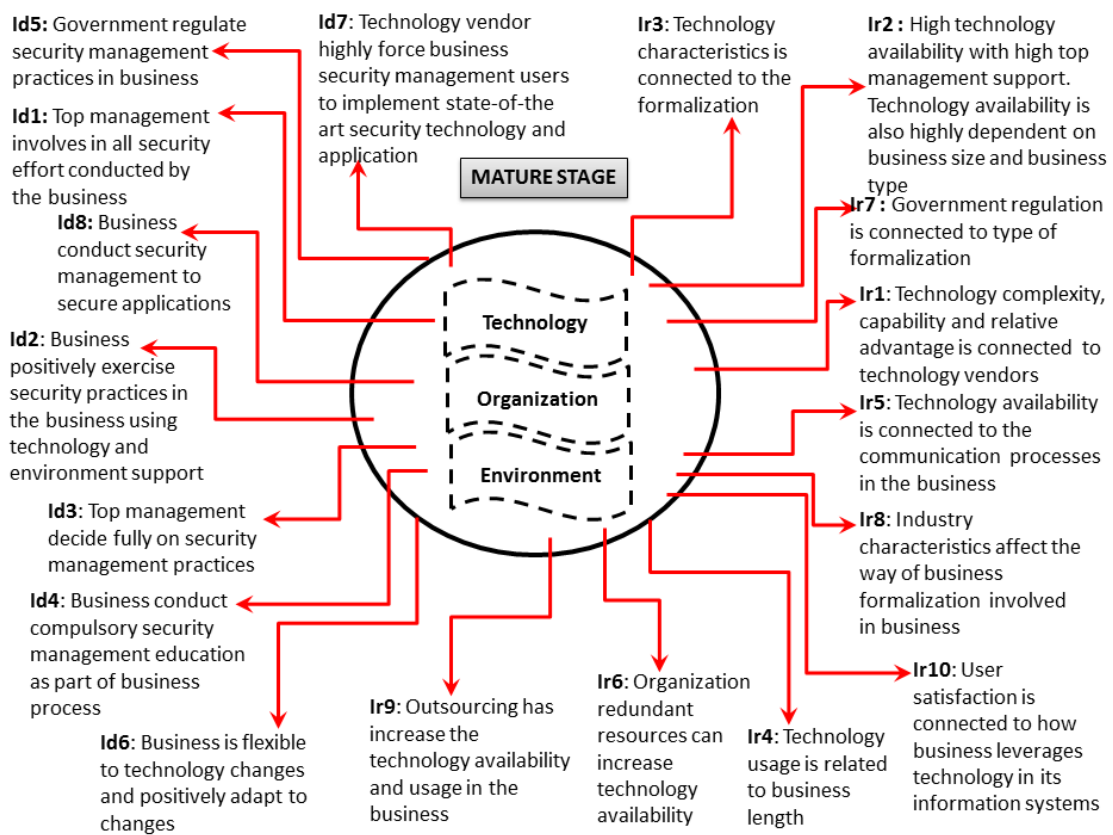


Figure 6.11: ISSM maturity in matured stage

The designed and validated ISSM maturity model demonstrated all required factor inter-relation and business forces required for each level or quadrant. Business assessed their current ISSM maturity through the related relationship discussed in each quadrant. The relationship also reflected the required TOE factors by the business. As this model provide overall business characteristics, business will require a tool to assess their business characteristics in simpler and practical format. Hence, based on the ISSM maturity model, the researcher has developed a ISSM maturity validation tool prototype to help business to assess their ISSM maturity. This validation tool is one of the contribution of the research. The validation tool was developed based on the ISSM maturity model using the computer system/application environment which can be accessed by the SMI/E via the Internet. This tool provide easy validation scheme, where businesses are required to answer questions in segments available in the prototype. Each segments will be discussed in the prototype development later in this chapter. Besides providing business with their current ISSM maturity level, the tool is also capable to recommend other types of SM practices, which will help improve their ISSM maturity to become better.

In conclusion, the designed ISSM validation tool was developed based on ISSM maturity model, which presented the required factors inter-relation and business forces. The ISSM model was designed base on the mix-method results integration discussed in Chapter 5. As such, the validation tool created had considered all related factors, relationships and issues pertaining to achieving the ISSM maturity for a business. In this research context, the ISSM maturity model addressed issues related to the SMI/Es e-commerce. With the ISSM maturity validation tool, the SMI/E in this research context will be able to have an accessible tools to validate their current status of ISSM maturity in a fast and practical manner.

6.4 Development of ISSM maturity prototype

Through the ISSM maturity model, the researcher has developed a prototype of the ISSM validation tool for the SMI/Es usage. The development of the prototype uses the same issues constructed in the model fitting to assess businesses. The prototype involved 5 different segments. The segments consisted of (i) business demography, (ii) factor inter-relationship issues, (iii) business forces/dynamics issues, (iv) ISSM current implementation in business and finally, (v) the ISSM maturity level results and recommendations. Segment (ii) and (iii) will provide the value of ISSM maturity level of the business. Segment (iv) will evaluate the current ISSM practice of the business. Segment (v) presented the results of the whole assessment whereby in this segment, business will be able to know their current TOE factors, relationship and business issues. The result segment also provides business with recommendation on the SM practices businesses may need to consider to improve their ISSM maturity level to become better. The prototype developed should be able to define and inform the businesses on their ISSM maturity and provides information on further SM practices thus increase the business performance in terms of the ISSM maturity level.

6.4.1 Business demography

Segment (i) consisted of the business demography questions and answers. Business demography consists of important information about the business. The information required are the business size, which were measured the number of staff in the business and annual income of the business. Other than that, information about the business included in business demography are the business type (product or services), the e-commerce stage and top management ISSM knowledge level. These information are important as it will provide the actual business's current demography. The demographic information are required for the purpose of assessment in

the prototype. The demographic questions are as depicted in Figure 6.12. The business demography indirectly will provide a better picture of the business, in terms of predicting the ISSM maturity of the business.

The screenshot shows a web browser window with the following content:

- Browser:** Firefox, localhost:8084/issm_azah/jsp/form/biz_create.jsp
- Page Title:** Information System Security Management
- Subtitle:** This is a validation tool on Information System SM Maturity in e-commerce
- Form Fields:**
 - Biz Length:** Less than 3 years
 - Biz Size:** Less than 10 staff
 - Level Of E-Commerce:**
 - Level 1- Display basic information on company, products (goods and services) and contact (such as postal address, telephone/fax number and email address)
 - Level 2- Besides above, additional function include shopping cart, use cookies to track users, feedback form and product/services rating/review system to be used by customers
 - Level 3- Besides above, additional function include receive payment online (credit and/or debit card), facility/system for company to buy from suppliers online, electronic auctions and facilities to other companies (third party) to place their catalogues of suppliers online
 - Level 4- Besides above, additional function include payment facility (payment gateway) in secure environment to purchasers, linking to customer relationships management (CRM) system, link to supply chain management (SCM) system and link to production and planning control (MRP) system
 - Biz Type:** Services Product
 - Annual Income:** Less than RM15,000
 - Security Management:** In House Outsource
- Tab:** Biz Demographic

Figure 6.12: ISSM Prototype: Business Demography

6.4.2 Factor interrelation

Factor interrelation assesses how the business operation has inter-related the identified factors which will influenced the business ISSM maturity. This is reflected in the segment (ii) of the validation tool which involve 10 factor inter-relation questions. All the factors influencing ISSM maturity are gathered from the revised ISSM maturity factors as presented in Figure 5.8 in Chapter 5. The ISSM maturity factors inter-relation and forces/dynamics are presented in Table 5.12 in Chapter 5. Issues addressed are the TOE factors. The interrelationship between TOE is observed in this matter. For example; organization's redundant resources (e.g. money and human resources) can increase technology availability in the business (O-T). In this example, we deduce that slack resources could influence technology availability in the business. Through technology availability, businesses will be able to achieve the desired ISSM maturity.

The factor inter-relation questions are as depicted in Figure 6.13

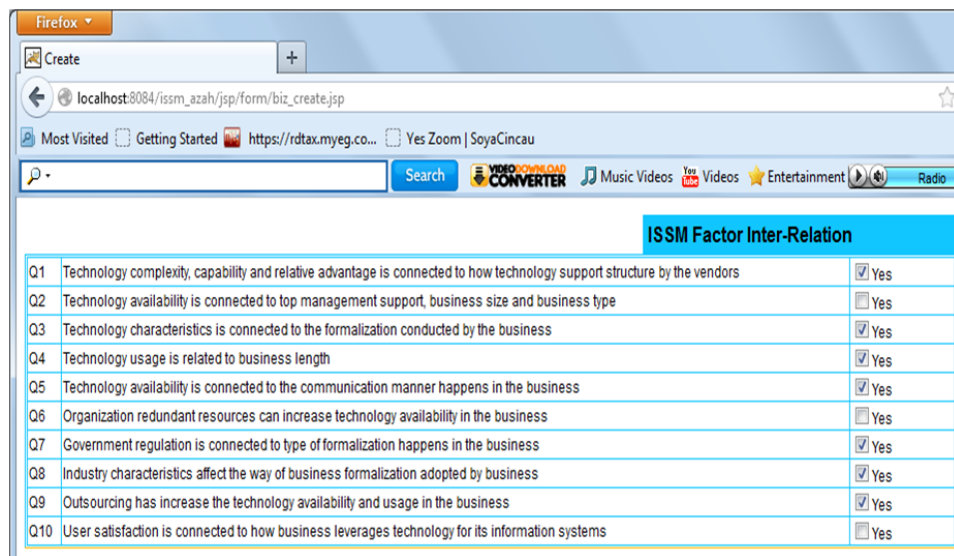


Figure 6.13: ISSM Prototype: Factor inter-relation

6.4.3 Business Forces or Dynamics

Segment (iii) consisted of the business forces/dynamics issues. Business forces/dynamics are presented in Table 5.13, Chapter 5. The business forces/dynamics reflect the business position towards changes especially related to the ISSM changes. The forces/dynamics are important to assess business readiness especially towards ISSM maturity. The factor forces/dynamics questions are depicted in Figure 6.14.

ISSM Factor Dynamics		
Q1	Top management involves in all security effort conducted by the business	<input checked="" type="checkbox"/> Yes
Q2	Business positively exercise security practices in the business using technology and environment support received	<input type="checkbox"/> Yes
Q3	Business positively exercise security practices in the business using technology and environment support received	<input checked="" type="checkbox"/> Yes
Q4	Business conduct compulsory security management education as part of business process	<input checked="" type="checkbox"/> Yes
Q5	Government regulate security management practices in business especially e-commerce business	<input checked="" type="checkbox"/> Yes
Q6	Business is flexible to technology changes and positively adapt to changes	<input type="checkbox"/> Yes
Q7	Technology vendor highly force business security management users to implement state-of-the art security technology and application	<input checked="" type="checkbox"/> Yes
Q8	Business conduct security management to secure applications to support their e-commerce	<input type="checkbox"/> Yes

Figure 6.14: ISSM Prototype: Forces/dynamics

6.4.4 ISSM level of practice

In the ISSM prototype, an assessment of the ISSM maturity includes the ISSM level of practice. Here there are 37 items of SM practices, adopted from Aceituno (2006b) related to ISSM practices which are discussed by many security standards. Many of them classified a business using the ISSM level of practice, which in this research, the ISSM maturity is very much influenced by the TOE of a business. However, the level of ISSM practice is used as part segment of the prototype to clearly indicate the business ISSM situation. The list of ISSM practices recommended by Aceituno (2006b) is required as the prototype need to know the level of the SM management practices of a business. Through this list, the validation tool will be able to collect observable and unobservable SM practices as part of the input to assess and provide the businesses with the level of their ISSM maturity. SM involved all types of security related practices currently employed by the business. As ISSM may include many possible SM practices, the prototype created will be based on the current ISSM practices suggested by the security management standards (Aceituno, 2006b) to assess adequacy of related practices. Security practices depend highly on what is available in the business and security management procedures exercised daily. Non-exercised security management implemented will not be considered as part of the currently employed security management by the business. The ISSM level of practice is

different to the ISSM maturity issues (factor inter-relation and business forces) as it provides information on types of SM practices to have secured business process. However, the ISSM maturity, looks at the TOE factors and how these factors inter-relate and how business forces stimulate this relationship (such as defined in the business forces) to achieve business ISSM maturity. The 37 important and related security practices as reflected in Figure 6.15.

The screenshot shows a Firefox browser window displaying a web form titled "ISSM Level Of Practice". The form contains a list of 37 security practices, each with a corresponding checkbox and the word "Yes". The practices are numbered 1 through 37. The browser's address bar shows the URL "localhost:8084/issm_azah/jsp/form/biz_create.jsp". The browser's search bar is empty, and the search button is labeled "Search". The browser's toolbar includes icons for "VIDEO CONVERTER", "Music Videos", "Videos", "Entertainment", and "Radio".

ISSM Level Of Practice	
1	Document management
2	ISSM audit
3	ISSM design
4	Report to management/stakeholders
5	Coordination
6	Resource allocation for ISSM
7	Manage resources for ISSM
8	Security target management
9	Service level management
10	Insurance management
11	Define environment and life-cycle
12	Background check
13	Security Personnel selection
14	Security Personnel training
15	Disciplinary process/ exercise process
16	Security awareness program
17	Select tool for SM
18	Inventory of SM
19	ISSM change control
20	Patching
21	Cleaning
22	Hardening
23	Application development life-cycle control
24	Segmentation and filtering
25	Malware protection
26	Access control
27	User registration
28	Physical protection
29	Backup
30	Reliability and availability management
31	Operation continuity management (redundancy)
32	Information quality and compliance
33	Archiving management
34	Alerts monitoring
35	Events detection and analysis
36	Handling incidents
37	Forensics

Figure 6.15: ISSM Prototype: ISSM Security Practices

6.4.5 Prototype technological considerations

The prototype building was developed using Java programming language with Tomcat-Apache. The prototype was developed using available tools on the net to prevent complications and time consumption due to unavailability and non-interoperability of programming language with the basic supporting hardware owned by the researcher. Besides, by using these simple tools, the ISSM validation tool can be evaluated online or remotely. As the prototype is used to validate the model fit, a simple user layout was created. The main objective of the prototype was to test on appropriateness and the validity of deduction from the model selection and model fitting as in the discussion above. There is no complex application and technological hardware used in designing this prototype.

6.4.6 Prototype design and layout

The design of the prototype was categorized into four segments; (i) business demography, (ii) factor inter-relationship issues, (iii) business forces/dynamics issues and (iv) ISSM current implementation in the business. It is followed by the result of the maturity level and recommendations to ISSM improvement. The first phase refers to business demography, which requires business fundamental information. The second phase looks at the factor inter-relationship issues discussed in sub-section factor inter-relation. The third phase of the design focuses on the business forces/dynamics issues. The final phase design reflects on the ISSM level of usage or practice. Businesses are required to select only security management practice which are used and practised by their individual business. All security management practices are referred to the description given by the chosen ISSM maturity standard. Each business must answer only applied and exercised security management in the business, leaving out planned or future security management implementation to ensure reliable assessment. The results from the prototype

showed that the percentage (%) of maturity and list of improvement required by the business. This is depicted in Figure 6.16. The full prototype design is attached in the Appendix E.

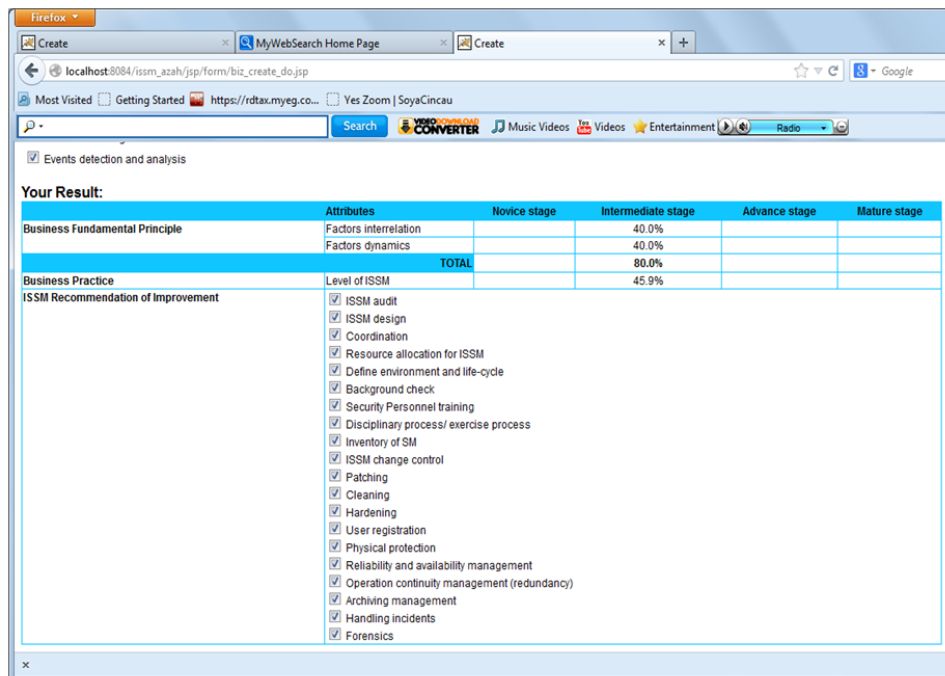


Figure 6.16: ISSM Prototype: Result page

6.4.7 Prototype evaluation

The prototype was evaluated by five experts who were involved in the instrument construction at the earlier phase of the research. All five experts were visited in five different meetings in their offices. The evaluations were conducted from between 45 minutes to 1 hour and 15 minutes. A validation form (as referred in Appendix F) was constructed for this purpose which consisted of 5 sections from section A- Expert personal details, Section B- Validation objectives and activities check list, Section C and D- Model testing purpose and finally the Section E- Prototype evaluation. The system evaluation section was based on the section E questions. Three main parts were questioned which were the system usability, output and purpose. Simple deterministic questions were designed for each parts, as the researcher are very concern on

the time given by the experts during the prototype evaluation. The prototype evaluation was conducted with two purpose which were, firstly, to validate the model designed derived from the model selection and model fitting process. Secondly, is to evaluate the prototype designed based on the designed ISSM maturity model. The prototype was presented to the experts. The experts accessed the online prototype during the evaluation sessions. The prototype was tested and questions on the system applicability and appropriateness was put forwards for the purpose of system evaluations as Appendix F. Result of the testing are as Table 6.2.

Table 6.2: Prototype evaluation results

No	System Evaluation	EX1	EX2	EX3	EX4	EX5
	System Usability					
1	System provides clear input for SMI/E to agree upon.	Y	Y	Y	Y	Y
2	The technical jargon displayed in the system is fairly easy to understand	N	Y	N	Y	N
3	Business will not need to have high-level of security management understanding to use this system, hence provide business clear position of the business	Y	Y	Y	Y	Y
	System output					
1	The system calculated the business security management position clearly	Y	Y	Y	Y	N
2	Through the result output business will be able to understand their security management maturity position	Y	Y	Y	Y	Y
3	Recommendation towards improvement is mentioned for business attention	Y	Y	Y	Y	Y
4	It is appropriate for the four segmentation of ISSM maturity for this business context based on the representation of the results	Y	Y	Y	Y	Y
	System purpose					
1	The purpose of the system is to provide level of maturity in terms of percentage is achieved	Y	Y	Y	Y	Y
2	Through the result business has an idea of the business security management status.	Y	Y	Y	Y	Y
3	The simple recommendation for improvement provides a guide to business on the security management area need to be improved.	Y	Y	Y	Y	Y

6.4.8 Problems and issues

The major problem in the prototype development is the inability to capture enough information from the business to deduce their ISSM maturity level. The researcher is concerned on lengthy issues addressed, which will derail the focus of these CEOs in the upcoming assessment. As such, issues constructed to address factor interrelation and forces/dynamics are based closely on the revised ISSM maturity factors deduced in the analysis as presented in Figure 5.8 in Chapter 5. Besides, issues on observable ISSM practices were quite hard to capture as some businesses considered them to be confidential such as the SM practices conducted in the business to reflect ISSM maturity. As such the mechanism in gathering the ISSM practices of a business is required. The simplest option is to capture level of ISSM practices in the business by asking the CEOs to determine them in the ISSM maturity validation tool prototype (as reflected in the ISSM level of practice module as Figure 6.15 in the ISSM maturity validation tool). The researcher concluded from the model validation and prototype evaluation conducted, that the ISSM maturity model has appropriately addressed findings from the research. Whereas the prototype were shown to be appropriate for the purpose of assessing the level of maturity of SMI/E similar to the research context. The conclusion is presented in Table 6.3 based on the discussion carried out during the evaluation.

Table 6.3: Prototype evaluation conclusion

N ^o	Item evaluated	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
1	Factor inter-relation correctness and appropriateness	Highly related	Highly related	Highly related	Highly related	Averagely related
2	Business forces/dynamic association	Highly related	Averagely related	Highly related	Highly related	Highly related
3	ISSM practices according to the ISSM standard is correct	Yes	Yes	Yes	Yes	Yes
4	Maturity quadrant appropriateness towards research context	Yes	Yes	Yes	Yes	Yes
5	System proposed ISSM improvement is highly needed	Yes	Yes	Yes	Yes	Yes

6.5 Conclusion

The ISSM maturity model is designed and developed based on the analysis of the data from Chapter 5. Through the analysis of Chapter 5, three important elements were identified which are the TOE factors. Based on the items listed under the respective TOE, the factor inter-relations were assessed to determine the model. Issues were constructed, and cases were built to facilitate the case comparison for the validation purposes. Constructed issues also addressed the business forces/dynamics as important and leading to the ISSM maturity discussed in the qualitative interviews. The ISSM maturity model involves four stages, or quadrants, which are novice, intermediate, advanced and matured. In each of these quadrants, different TOE circles of connection were identified.

To assess the applicability of these quadrants, the model fitting and model validation were conducted. As such two important issues were constructed to conduct the assessments which were the TOE factors inter-relation and the forces/dynamics. The constructed issues were then used to conduct the model fitting to test the model selected. Once assessments were completed and the model fit the selected design was done, model validation was conducted. The validation

was carried out using the same format as model fitting, where fourteen cases were compared. The validation process has provided the same results as the model fitting assessment. From the results of this process, the ISSM maturity model was deduced. It involved three non-connected TOE rings in the novice stage, an intermediate relation diagram for the intermediate stage, a flower bloom like connection in the advanced stage and a TOE globe where interconnection of TOE is at its maximum. Based on this designed model, the prototype was built. The same issues were involved in the prototype, except in the prototype, the ISSM level of practices is assessed to determine the level of practice by the business. This level of practice will provide the business a tool to gauge whether they have fully utilized and leverage the advantages the business currently has, based on the TOE possessed by the business. The prototype evaluation was carried out by five experts, where findings showed that the prototype of the ISSM validation tool is applicable for the SMI/E context.

CHAPTER 7

DISCUSSION AND CONCLUSION

7.1 Overview

ISSM maturity defines the level of maturity of a business for its security management exercise. Presumably, many ISSM maturity standards determine the ISSM maturity levels using the security management implementation in the business. The present security management recognizes the importance of people, processes and technology in order to build quality security management for a specific business context. However, in reality, the implementation of security management in a business still concentrates on technological issues rather than connecting the importance of people and processes. Thus, this research was carried out to assess the socio-technical factors in defining ISSM maturity of a business.

In the quest to identify the true influences of ISSM maturity, the IS theories, model and framework were chosen to understand the situation influencing a business to achieve ISSM maturity in the business. These include (i) the DOI by Rogers (1995), (ii) IS Success Model by DeLone and McLean (2003, 1992), (iii) TOE by Tornatzky et al. (1990) and the (iv) MIS organization factors by Ein-Dor and Segev (1978). The assessment of IS theories, model and framework define the importance of technology, organization and environment (TOE). As such, the research embarks to understand the influence of TOE in a business. This study is important and significant; both in terms of being the first, as far as the researcher is aware, to investigate what are the true ISSM maturity influences in the business and, in terms of how this has influenced and affected the business, or how can the business leverage this influence to implement effective

ISSM in the business, hence achieve ISSM maturity. The distinct benefits of this study include the definition of ISSM maturity factors in the business and description of the relationship of these factors with each other, which will contribute to the ISSM maturity. The factors relationship include:

- (i) Technology complexity, capability and relative advantage are connected to how technology support structure by provided by the vendors;
- (ii) Technology availability is connected to top management support, business size and business type;
- (iii) Technology characteristics are connected to the formalization conducted by the business;
- (iv) Technology usage is related to business length;
- (v) Technology availability is connected to the communication manner that happens in the business;
- (vi) Organization redundant resources can increase technology availability in the business;
- (vii) Government regulation is connected to type of formalization that happens in the business;
- (viii) Industry characteristics affect the way a business formalization is adopted by business;
- (ix) Outsourcing has increased the technology availability and usage in the business; and
- (x) User satisfaction is connected to how business leverages technology for its information systems.

This research carried out a mixed-method sequential research where it involved the quantitative investigation and followed by the qualitative investigations. The data collected during the quantitative investigations were analysed using the SEM PLS technique, where the TOE factors were identified. The sequence qualitative analysis was conducted using thematic coding where data were reduced through the data reduction technique to conclude the discussion in

socio-technical discussion themes.

This study clearly shows that, in order to be an ISSM-matured business, appropriate inter-relationship of TOE in a business must be considered. It also shows that technological implementation is not the only indicator to assess the business ISSM maturity. Organization and environment, which involve the people and processes, must be included in the assessment, to provide the holistic capability of the business. Associating the TOE influence with each other, where throughout this association business could exploit new benefit, can also increase the ability of the business to be in higher position in the ISSM maturity assessment. This assessment is especially true in the context of Malaysian SMI/Es who are involved in the e-commerce business, as these businesses require clear information and guides, leveraging on their inner resources and outer resources in the most maximum ways possible.

From the result of the data analysis, the researcher concluded a ISSM maturity model. This model provide the factors inter-relation and business forces/dynamics crucial in achieving the ISSM maturity. A simple ISSM validation tool prototype was also designed to determine the level of ISSM of a business. All businesses can accessed the tool online and test their current business ISSM maturity level based on the socio-technical considerations issues provided in the tool. The ISSM validation tool then concludes the results by presenting the maturity level of the business and provides recommendation on other ISSM practices a business could consider to achieve higher ISSM maturity level in the future.

The remainder of this thesis summarizes the study outcome in light of its contribution, research significance and limitations. The discussion will address how the research questions are answered and conclude the findings. The conclusion will also draw some of the implications of

the research in terms of ISSM maturity towards a business. The research concludes with the discussion of the research limitations and suggestions for future research.

7.2 Question addressed in this research

The research set out to answer this question: What are the core elements needed to be addressed, managed and structured in order to achieve information systems security management (ISSM) maturity for effective IS security practices in SMI/E in Malaysia involved with e-commerce?

The motivation of the whole research was to resolve the above issue and therefore provide a body of practical and beneficial recommendations for the SMI/E owners to exercise security management towards becoming an 'ISSM-matured' business in e-commerce. The recommendations were part of the contribution of the prototype ISSM validation tool, which recommends the ISSM improvement for the SMI/Es. In order to understand and provide light onto this issues, three research questions were constructed, and they were as follows:

RQ1) What are the factors that influence an organization to practice effective ISSM in order to reach ISSM maturity?

Through the quantitative investigation and analysis, ISSM maturity factors were derived to address RQ1. Figure 5.2, Figure 5.3 and Figure 5.4 shows all related TOE factors which were derived from the quantitative analysis. Discussion on all variables in these figures were discussed in the quantitative result analysis in Section 5.5.2. Whereby, in the top management support, there were two significant variables which are the top management support is significant in implementing new security tools and techniques (TM2), and secondly is the encouragement in

practising security implementation (TM8) by the top management. These factors influenced the business to achieve ISSM maturity.

As for the technology variables, the analysis had shown high significant on the variables of the technology and communication structure involved in the business. The significant technology variables are:

- 1) Usage of email is required to exchange information on new security tools and infrastructure (SMUS2);
- 2) Security information has to be communicated formally in the business (SMUS3); and
- 3) Security tools have to be practised by all staff (SMUS7) and is part of staff responsibility towards the business (SMUS9).

In the organization factors, items identified significantly influence ISSM maturity are:

- 1) Data integrity and system availability are business objective (SMPur6 and SMPur8);
- 2) Security tools and techniques are used to safeguard business assets (SMUU6), website (SMUU1), mitigate risk and threats (SMUU12), and prevent from system misused (SMUU3);
- 3) Security tools and techniques are adopted to follow business trend (SMUU13);
- 4) Security tools and techniques are used to provide new and better services (SMUU2), and promote business (SMUU4);
- 5) Security tools and techniques are used to compete with competitors (SMUU5) and fulfil user requests (SMUU7);
- 6) Security tools and techniques are used to comply with government legislation (SMUU8) and security standards (SMUU9).

Finally, the environment factors with significant items are the technology providers support helped business in its ISSM implementation (SMR5), industry players support business SM initiatives (SMR4) and staff responsibility are significant in practising SM(SMR3). These fac-

tors are also supported by significant relationship derived through the hypotheses assessment and results which were presented in Table 5.8. The technology factor reflecting the technology usage in security and communication, highlight the necessity of information security dissemination. It also means the technology availability (Hsu et al., 2012; Tsohou et al., 2010; Da Veiga & Eloff, 2010; Al-Awadi & Saidani, 2010) and technology usage (Tsohou et al., 2010; Gillies, 2011; Werlinger et al., 2009; Hu et al., 2007) as important in ISSM maturity. As for the organization influence, factors representing organization include (i) business length, (ii) business size, (iii) business type, (iv) top management support, and (v) formal linking structures. These findings agreed with the findings from previous research by scholars such as from Hsu et al. (2012); Monfelt et al. (2011); Yildirim et al. (2011); Tsohou et al. (2010); Ozkan and Karabacak (2010); Chang and Ho (2006); Kankanhalli et al. (2003). Finally, under the environment influence, the researcher has successfully determined environment related factors which are the technology support infrastructure and the industry characteristics and market structure. These findings showed that variables highly influenced ISSM maturity of a business. Again, scholars such as Hsu et al. (2012); Gillies (2011); Kraemer et al. (2009); Chang and Ho (2006); Farn et al. (2004); Kankanhalli et al. (2003) have highlighted these factors in their studies. The factors identified agreed with the earlier discussions by many scholars of the importance of TOE in any ISSM effort (Yildirim et al., 2011; Monfelt et al., 2011; Mansor & Amri, 2010; Ozkan & Karabacak, 2010; Werlinger et al., 2009; Kraemer et al., 2009; Zuccato, 2007; Chang & Ho, 2006; Caralli et al., 2004; Kankanhalli et al., 2003; Baskerville & Myers, 2002; Dhillon & Backhouse, 2000). As such, for all businesses to achieve ISSM maturity in the business, the same factors should be of influence.

In investigating the ISSM maturity factors, the researcher has defined ISSM as an innovation,

thus closely designed the research based on the TOE framework by Tornatzky et al. (1990), with the addition of a few other IS theories to address research findings from the literature review earlier. The other IS theories, IS models and IS organization factors included DOI (Agarwal & Prasad, 1998; Rogers, 1995), organization factors (Yildirim et al., 2011; Werlinger et al., 2009; Kraemer et al., 2009; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978) and IS success model (DeLone & McLean, 2003, 1992) which provide a research lens for this study. Remarkably, the idea of ISSM as an innovation is strengthened by the findings of a recent study from Hsu et al. (2012) asserting ISSM as an administrative innovation in a business. As such, the approach of determining ISSM maturity factors according to TOE framework is appropriate. This research has contributed to the body of knowledge by successfully representing innovation decision making in the organization context facing the challenges from TOE elements. There are small differences which are in terms of technology factors, the technology usage, complexity, compatibility and relative advantage is also important. These items are not directly presented in the TOE framework by Tornatzky et al. (1990), which can be seen in the items related to each TOE. In conclusion, the research is able to conclude that for a business to achieve ISSM maturity, TOE elements are the main elements which need attention by the business, whereby technology represents the usage of tools and techniques, organization includes the staff, top management support, business size, business type and communication structure and finally the environment consisting of users, government, industry players; and standards and legislation.

As for the second research questions, the research has determined the importance of the relationship of these factors. The importance of understanding the relationship of these factors was indicated during the analysis of the importance of ISSM standards. Many issues mentioned in

the standards refer to the TOE aspect of a business. However, many have failed to relate the TOE elements in business and hence effective ISSM is not achievable. This is because, there is small inter-relation between resources and the businesses failed to determine the degree to which TOE dynamics consisted in the business. The research Question 2 below sets forth the focus of sequence analysis from quantitative investigation and complemented by qualitative investigation.

RQ2) What are the underlying relationships of determined factors in stimulating ISSM maturity in the SMI/Es involved with e-commerce?

Part of the quantitative analysis had statistically determined the relationship of the TOE items to understand whether it has supported the entire hypotheses developed in this research. Through the PLS analyses, relationships of involved factors were predicted. This was shown from the result of the hypotheses decisions discussed in Table 5.8, where all hypotheses below were supported in this research. They were:

H1b: Business length is related to organization factors in the SM practices;

H1c: Business length is related environment factors in the SM practices;

H2b: Business size is related to organization factors in the SM practices;

H2c: Business size is related to environment factors in the SM practices;

H3b: Business type is related to organization factors in the SM practices;

H4a: Top management support is related to technology factors in the SM practices;

H4b: Top management support is related to organization factors in the SM practices;

H4c: Top management support is related to environment factors in the SM practices;

H5b: Organization factors in the SM practices is related to ISSM Maturity;

H8: Business type is related to ISSM Maturity; and

H9: Top management support is related to ISSM Maturity.

These results showed significant relationship between independent factors with the TOE factors in order to achieve ISSM maturity in the SMI/E. Further analysis showed the inverse relationship in H1b, H1c and H8. The relationship of H1b and H1c showed that more recent business is the operation the higher organization and environment factors are involved and required. In order to practice ISSM at the initial stage of business set-up, high business resources and strong back-up from the environment are highly required in the organization, especially in SMI/E (Barlette & Fomin, 2008). As for H8, business type is referred to the e-commerce stage. The result showed that, the earlier level of business is in its e-commerce stage, the higher level of ISSM maturity a business could be achieved. This is true as in most novice e-commerce stage, implementation of e-commerce technology or application is at minimal; hence SM implementation is straight forward and easily maintain especially by SMI/E with small resources (Kankanhalli et al., 2003). As for H2b, H2c, H3b, H4a, H4b, H4c and H9, scholars such as Hsu et al. (2012); Yildirim et al. (2011); Werlinger et al. (2009); Kraemer et al. (2009); Barlette and Fomin (2008); Fomin and Vries (2008); Zuccato (2007); Chang and Ho (2006); Zhuang and Lederer (2004) asserted in their research, the business size, business type and top management support are major influence in ISSM maturity, implementation and effectiveness.

However the relationship from the analysis is unable to explain in further depth on how and why this factors were related, hence the qualitative investigations were carried out. The qualitative research investigation was sequentially deployed to complement the earlier findings. The majority of the responses collected through the interviews had shown dissimilar results as to the earlier analysis. The security management practices are deemed to influence ISSM maturity through discussion on findings from the qualitative analysis (refer to discussion in subsection

5.3.2). However, the qualitative findings remarkably present the utmost important issues, which are the TOE inter-relation and business forces/dynamics. These issues contributed to the ISSM implementation and maturity in the SMI/E as found in some discussion from scholar such as Hsu et al. (2012); Albrechtsen (2007). Many studies also highlight the important of factor inter-relation with business forces to ensure that the ISSM maturity could be achieved (Hsu et al., 2012; Monfelt et al., 2011; Yildirim et al., 2011; Tsohou et al., 2010; Da Veiga & Eloff, 2010; Ozkan & Karabacak, 2010; Chang & Ho, 2006; Kankanhalli et al., 2003). Through qualitative analysis, findings complement the factors influencing ISSM which finally are depicted in the ISSM maturity factors inter relationship as in Table 5.12 and business forces/dynamics in Table 5.13.

RQ3) How has the identified relationship encouraged ISSM and promoted the ISSM maturity model?

By combining quantitative and qualitative analysis, the researcher presented the TOE factors and relationships influenced the ISSM maturity in the SMI/E e-commerce. Through the integration of the quantitative and qualitative analysis, the research has identified factors influencing ISSM maturity as presented in Figure 5.8. The mixed-method findings intergration also defines the factors inter relation through hypotheses results and interview discussion, where in-depth details were given to support the relationship define in Table 5.14. The researcher predicts an ISSM maturity model, based on the finding in Chapter 5 and validation conducted during the model validation proces. The designed model was assessed in the model-building process as discussed in Chapter 6. The mixed-method analysis integration and interpretation suggested that, any business that wants to achieve ISSM maturity needs to assess the TOE inter-relation and forces/dynamics of their business. This step provides the insight of a business capacity. The

TOE inter-relation defines the interrelationship of TOE items in the business, which have been leveraged or silently kept in the business. It defines the performance of a business of being able to identify resources internally and externally to ensure full utilization to reach higher ISSM maturity. The relationships between the ISSM inter-related factors and business forces/dynamic encourages business to move from novice stage to matured stage of ISSM maturity. Hence, promote the design of four-quadrant model of ISSM maturity for the SMI/Es. This model provides the important socio-technical relationships required in achieving the ISSM maturity.

As mentioned by Van Niekerk and Von Solms (2010); Da Veiga and Eloff (2010); Ruighaver et al. (2007), organization (specifically its business culture) represents the density of ISSM implementation and effectiveness in the business. As such, through the result integration and interpretation, the research determines the variety of factor inter-relation and forces/dynamics to represent the business conditions to reach ISSM maturity. The comprehensive view of the ISSM maturity provided by the mixed-method analysis allowed the researcher to depict the ISSM maturity model. The development of the ISSM maturity model based firstly on the factor inter-relation between technology, organization and environment. Secondly, is the business forces/dynamic, which is connected to the stimulus of changes applicable in the business towards implementing ISSM. The researcher concluded the existence of influences which determine the ISSM maturity of a business. Thus, the proposed ISSM maturity model is depicted in Figure 6.8 showing the importance of TOE factors in a business.

The quantitative analysis successfully address all related TOE factors influenced the ISSM maturity and the qualitative analysis defined all relationship and the influence of factor inter-relation and forces/dynamics discussed continuously from Chapter 5 to Chapter 6. Hence, from

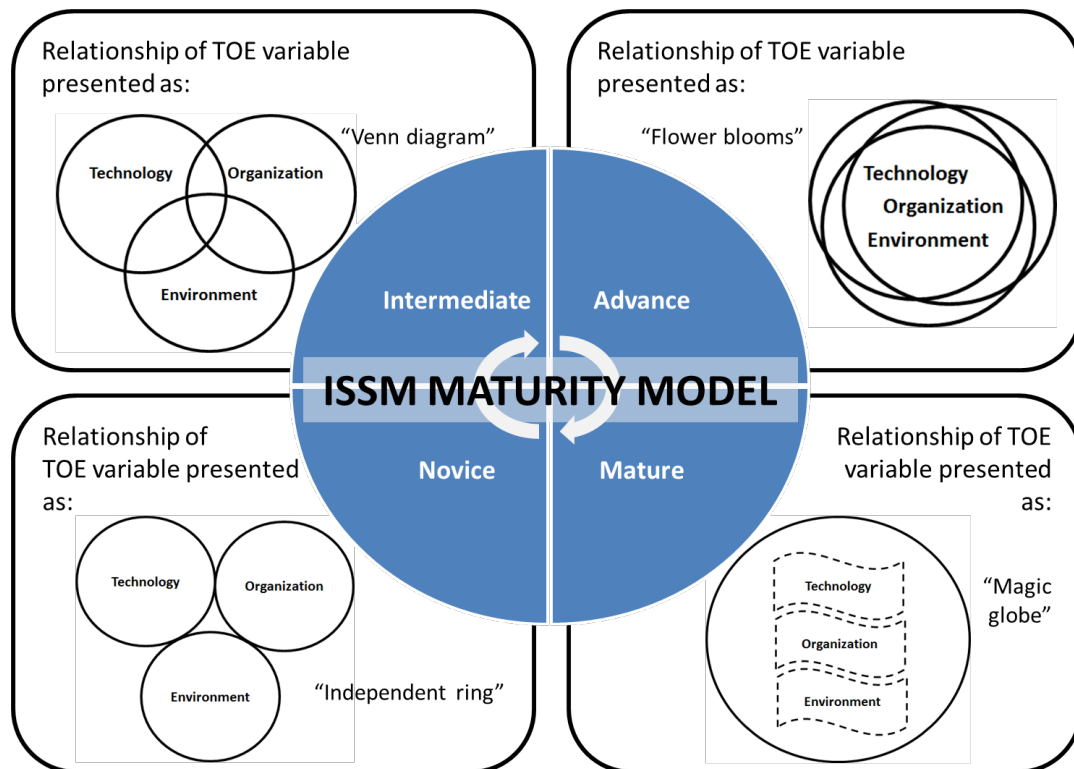


Figure 7.1: ISSM maturity model based on TOE

these two method of research, researcher gathered findings to build the ISSM maturity model and the ISSM maturity validation tool as the main contribution of this research.

7.3 Contribution

This study presented a comprehensive logical model through a combination of selected information systems theoretical perspectives drawn in one model of ISSM maturity as follows:

Firstly, this study presented a holistic conceptual ISSM maturity model for the SMI/E with e-commerce business as a basic to guide the businesses in their ISSM implementation. Using the same model, businesses could assess their current ISSM maturity in terms of TOE elements involved in the business. This proposed model could also provide ground level understanding of how current business resources must be leveraged on and hence used to the fullest.

Secondly, this study effectively determines the ISSM maturity influence in the SMI/E EC business context, which is often taken lightly in terms of ISSM maturity assessment. By establishing the ISSM maturity influence, businesses, especially the SMI/Es with e-commerce, now understand that ISSM maturity is achievable by a business even though it is small. The most important attributes of achieving ISSM maturity are not technological implementation, neither the size of business. But of the utmost importance is the TOE inter-relation and dynamics involved in the business.

Technology, organization and environment items defined under these elements have to inter-connect. For example, technology availability in the business alone cannot push the business towards achieving ISSM maturity; rather technology availability with support and push from technology vendors and management support will surely determine the path of business ISSM and its maturity. These findings show that the current assessment of ISSM maturity in the business may not be totally appropriate if these TOE elements are lacking in the business, although all technological requirements have been satisfied.

7.4 Implications

The conclusion of the current study has its implications in two perspectives; the academic and the organizational practitioners. The implications are listed below:

7.4.1 Theoretical implications

In terms of predicting the ISSM maturity model for businesses today, this research integrates selected IS theories, IS model and IS factors to be the platform on this research, where theoret-

ical ISSM maturity models were depicted to test the appropriateness of current ISSM maturity assessment. The result shows that in terms of ISSM practices which leads to ISSM maturity, technological and process issues are the only indicators. The dynamics of three elements, consisting of technology, organization and environment are important to determine the ISSM maturity of a business. There is no theory extension created in this study. However, this study proves ISSM implementations conducted based on practical experiences may not be enough for various types of businesses in the market, as important business characteristics are not addressed appropriately.

This study attempts to break boundaries by analysing the ISSM maturity in the SMI/E with e-commerce business based on TOE framework, defining ISSM as an innovation. This research has contributed to the body of knowledge by successfully representing innovation decision-making by an organization facing the TOE challenges where the TOE framework is not only limited to the technological innovation decision making; however, is applicable for administrative innovation decision making. Nevertheless, there are small differences between the items involved under TOE from the TOE framework with this study, appropriate with the issue it is addressing. ISSM maturity is built by the core elements of technology, organization and environment. The findings contribute to the body of knowledge in terms of the identification of the socio-technical factors derived based on the theoretical views of influential IS theory, framework and model.

It also contributes to the whole SMI/Es with e-commerce community by shedding light through creating ISSM management literature for the usage of the business context. This study has discussed the main influences of ISSM maturity of a business, which will facilitate the business to

implement, deploy and overcome issues pertaining to ISSM of the business, thus achieving the required ISSM maturity.

From the methodological perspective, the appropriateness of the mixed-method in the ISSM maturity study is highly reflected, where in this business context current literature is still minimal. Assessments on current e-commerce business, especially in the SMI/Es, are appropriate as these reduce ISSM naivety among business owners by portraying the importance of ISSM and its maturity to the selected business population, hence giving shape to the business security management practices. The sequential qualitative method complements the ideas generated in the research design, thus harvesting an in-depth understanding of ISSM maturity issues in the business, and therefore a realistic requirement is provided to help the business in its ISSM implementation and maturity achievement.

This research also developed a ISSM Maturity validation Tool for the usage of all SMI/E fit to this research context. The discussion on the prototype usage and evaluation were conducted in Chapter 6. The purpose of this tool is to assist SMI/E to gauge their business status on the ISSM status of the business. The developed tool is also able to recommend improvement for the business to increase its ISSM maturity for the business.

7.4.2 Practical implications

The present study elaborates on some of the important tasks a business may need to take to implement effective ISSM and, thus achieve ISSM maturity. However, ensuring success in achieving ISSM maturity in a business depends highly on the path charted by the owner and business CEO. The effectiveness of the task will highly depend on the aptness of the top management to

manoeuvre and leverage on current business resources. In terms of practical implications, the study presents them as follows:

- a) Using the contribution from this research, the business could now predict internal and external resources of the business before engaging in other expensive resources to implement ISSM. This is done by identifying the business TOE factors available in the business which have been identified in this research. This also applies to the businesses which have conducted ISSM, whereby to achieve specific ISSM maturity, these businesses could now categorize internal and external resources owned by each business and critically plan all owned resources before engaging in new complicated resources to achieve ISSM maturity. Therefore, the business could save maximum resources in terms of money and time;
- b) The ISSM maturity model is designed to help businesses position themselves at the required ISSM level depending on the e-commerce they are conducting. Businesses could now determine the remaining tasks they are required to undertake, rather than starting the task from ground level.

This study also proposed on leveraging on external resources available rather than engaging with an expensive off-the-shelf technology to implement the right ISSM. ISSM maturity is about success in inter-relating TOE factors, plus the presence of business forces/dynamics, which can be nurtured internally.

Slack resources are extremely low in SMI/Es with e-commerce. However, slack resources could come in many shapes. Experience and knowledge of the top management can be slack resources to a business. If this experience is fully utilized, with motivation and awareness by the staff, the business could achieve a higher level in the ISSM maturity stage. Cloud comput-

ing and open source are slack resources available to all businesses, be it hierarchical business or SMI/Es with e-commerce. Thus, the experience of the CEOs and business owners will set the course of the business on how to leverage on the applicable technology and help to achieve the targeted ISSM maturity.

Finally, the prototype development is a helping tool for the SMI/E to gauge the level of their current business ISSM maturity level. The prototype also includes recommendations towards business improvement, hence the SMI/E will have good understanding of the types of ISSM implementation required.

7.5 Limitation

This research limits its scope for the SMI/E with e-commerce business due to the gap available in the current ISSM maturity frameworks available. The context of the research also focuses on business in Malaysia, where government restrictions or culture implications may differ from other countries. This basically are some of the limitation which was not addressed in the model building which will become the research future work.

7.5.1 Theoretical limitation

The current research is solidly based on the selected IS theories, model and framework which highlight the TOE framework (Tornatzky et al., 1990), DOI (Agarwal & Prasad, 1998; Rogers, 1995), organization factors (Yildirim et al., 2011; Chang & Ho, 2006; Kankanhalli et al., 2003; Ein-Dor & Segev, 1978; Kraemer et al., 2009; Werlinger et al., 2009) and IS success model (DeLone & McLean, 2003, 1992), where these theories are deemed to be appropriate in the

ISSM context. This is based on the literature review conducted in the earlier stage. However, this research has not reviewed any behavioural or cultural frameworks. As the focus of this study is to understand current ISSM practices, the socio-technical factors influencing the ISSM maturity and its relationship with ISSM maturity. Currently, in the IS perspective, there is no specific security management theory designed to gear this research. Hence, researcher adopted the IS theory, framework and model to embark on the research, where it may provide different perspective of research and its outcome may differ totally.

7.5.2 Methodological limitation

The limitation of this study may probably not be on the method adopted by the researcher, but the population and sample gained for this research. As ISSM related issues are highly sensitive (Kotulic & Clark, 2004), the number of respondents who agreed to participate, was small, thus generalization of the whole study may be difficult. Another constraint on the respondent is due to the research requirement which focuses only on the SMI/E with e-commerce which has implemented ISSM. The limitation increases as researcher only focuses on the CEO and business owner for feedback and response. As the SMI/E is small, the CEO and business owner is the right respondent of the research as they are responsible for the business ISSM. Due to the research requirements and the fact that ISSM research is a highly sensitive issues towards business, this research faced with small respondents replies. However, appropriate measures in conducting this research were emphasized to minimise the research bias. Generalization can be done in a careful manner, appropriate with the study sample used. The CEOs become the primary focus of this study as this entity understands the vision of the business, besides in SMI/Es with e-commerce, the business usually has a flat business structure whereby no security officer is in charge. Thus this discussion may be limited to the understanding, knowledge and

experience of the CEOs.

7.6 Future research and recommendations

We identified several directions for future research from the emergent findings. It would be useful to use the emergent findings and test them using only a qualitative study in the chosen business, where a case study method and observation could be conducted. An action research method is also seen to be another exciting future research, as the research could participate in the improvement and changes in the business, especially in this study context, thus understanding better the issues of this business.

Besides focusing on the methodological approach on the same issue, this research could be extended to study issues of appropriating specific ISSM maturity standards, for example ISM3 by Aceituno (2006), into the business according to the maturity stage the business belongs to based on the ISSM maturity model represented in this study. Although this study concentrates on the SMI/Es with e-commerce in Malaysia, a comparative study could also be conducted with different countries or different business characteristics to test the difference or extension towards the developed ISSM maturity model.

It is also recommended that issues of security awareness and education to be emphasized in all research of SM. The findings from the research showed, that the top management support on is important. Knowledge and education in the high level management is important to influence support towards ISSM maturity. Human resources in the business are also identified as an important influence towards ISSM. In order to have reliable human resources to support business with the ISSM implementation, awareness and trainings have to become part of the

business responsibility (Tsohou et al., 2010; Da Veiga & Eloff, 2010). Besides awareness and education issues, culture or the religious belief may need to be associated to the security discussion as different countries are influenced by the culture and religion differences (Alfawaz, 2011; Da Veiga & Eloff, 2010; Van Niekerk & Von Solms, 2010; Ruighaver et al., 2007) .

7.7 Summary

This chapter concludes the research with the discussion on the outcomes in terms of its contributions, significance and limitations. This chapter discusses and presents how research questions have been addressed. Solutions and issues pertaining to the research questions were presented and concluded. Subsequently, the conclusion is presented in light of the contribution, implications and limitations surrounding this research. The contributions and implications of this study present an alternative ISSM maturity model to the focused of the business context in terms of deployment and assessment of ISSM maturity of the selected business. Finally, this chapter has presented the research limitations and some suggestions for future research.

Appendices

APPENDIX A

SURVEY INSTRUMENT



with cooperation of
Faculty of Computer Science and Information Technology, University of Malaya

Survey Form

Title: Information Systems Security Management Implementation in e-Commerce

28 SEPTEMBER 2010

Study overview: This survey aims to identify information systems security management in e-commerce in Small and Medium Enterprises (SMEs) which have adopted e-commerce in their business. Through this research, problems and issues faced by SMEs on information systems security management in e-commerce can be identified. The study also will help to design training or follow-up support worthy to be channeled to the SMEs to improve productivity and competitiveness of the SMEs to the current e-commerce available on the Internet.

Questions 1 to 3 are meant to collect information on your company background.

(Please choose ONLY one answer by crossing [x] appropriate box)

Questions	The company background	Answer choice
1	What is the size of your e-commerce company up to July 2010?	<input type="checkbox"/> less than 10 staff <input type="checkbox"/> between 10 to 30 staffs <input type="checkbox"/> between 31 to 50 staffs <input type="checkbox"/> more than 50 staffs
2	How long have you been in the e-commerce business up to July 2010?	<input type="checkbox"/> less than 3 years <input type="checkbox"/> between 3 to less than 6 years <input type="checkbox"/> between 6 to less than 10 years <input type="checkbox"/> more than 10 years
3	What is the stage of e-commerce adoption in your company?	<input type="checkbox"/> Display basic information on company, products (goods and services) and contact (such as postal address, telephone/fax number and email address) <input type="checkbox"/> Besides above, additional function include shopping cart, use cookies to track users, feedback form and product/services rating/review system to be used by customers <input type="checkbox"/> Besides above, additional function include receive payment online (credit and/or debit card), facility/system for company to buy from suppliers online, electronic auctions and facilities to other companies (third party) to place their catalogues of suppliers online <input type="checkbox"/> Besides above, additional function include payment facility (payment gateway) in secure environment to purchasers, linking to customer relationships management (CRM) system, link to supply chain management (SCM) system and link to production and planning control (MRP) system

Questions 4 to 13 follows was intended to address perception, adoption and adaptation about the Information Systems Security Management in your e-commerce organization. Please state whether you agree or disagree with each of the following statement about the security management implementation in your company?

(Please circle ONE answer either 1, 2 or 3)

Question 4	The presence of security measurement in your e-Commerce	Answer choice		
		Yes ↓	No ↓	Not applicable ↓
a	The company uses user log -in and password for system applications	1	2	3
b	The company uses SSL (Secure Socket Layer) certificate to secure web transaction	1	2	3
c	The company design policy e.g. for change of password every six months	1	2	3
d	The company design a policy for validation purposes e.g. when customer register to our website	1	2	3
e	The company store all users data and the system applications in secure servers	1	2	3
f	The company store all back-up data in a physical location equip with physical security e.g. physical location are secure with CCTV (Closed-circuit Television)	1	2	3
g	The company post the business terms and condition practices in the website for everyone to read	1	2	3
h	The company design the e-commerce site considering applicable security measures required	1	2	3
i	The company highlight security events in the website as a reminder to all including to the staffs	1	2	3
j	The company will test the e-commerce website every day on specific time which is always mentioned in the website as a reminder	1	2	3
k	The company update the e-commerce website every day on specific time which is always mentioned in the website as a reminder	1	2	3
l	The company develop the e-commerce website following secure architecture proposed by experts	1	2	3
m	The company uses standards and best practices to develop the policy and procedure for the e-commerce business usage	1	2	3
n	The company also conduct test on the network security following specific time	1	2	3
o	The company install other security measure e.g. patches and antivirus, which are appropriate for our business usage	1	2	3
p	The company conduct internal audit on the e-commerce business processes and activities	1	2	3

Question 5	The awareness level on security risk and management in your company	Answer choice		
		Yes ↓	No ↓	Not applicable ↓
a	The company have scheduled security training every year	1	2	3

Question 5	The awareness level on security risk and management in your company	Answer choice		
		Yes ↓	No ↓	Not applicable ↓
b	The company conducted knowledge sharing on security issues periodically	1	2	3
c	The company follow security procedure when it is required in the everyday work	1	2	3
d	The company understand that by practicing good security procedure it will protect the company asset better	1	2	3
e	The staff are responsible to read and understand the security events, policies and procedure the company developed for the use of everyday work	1	2	3
f	The company believed that by keeping the staffs up to date with the company security policy it can automatically protect the customer	1	2	3
g	The company have recruited highly responsible and motivated staff	1	2	3
h	The company is fully aware on the risks and threats an unsecure website can cost towards the e-commerce business	1	2	3
i	The company have formed a dedicated team to handle information security matters	1	2	3
j	The company has coordinated with the technology supplier to inform the management and officers on any latest security issues.	1	2	3
k	The staffs has the responsibility to report to the management on any internal suspicious act which may cause security threats	1	2	3
l	The company have created a policy and procedure to handle security incidents	1	2	3
m	The company have employed or engaged at least one accredited security professional to champion our effort in providing secure services through our e-commerce site to the customer	1	2	3
n	The company conducted risk analysis and assessment whenever there are any change in the process or in the system environment	1	2	3

Question 6	The purpose of having security measure in your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	Having security tools (technologies) are important for the company	1	2	3	4	5	6
b	Having security techniques (procedures and policies) are important to the company	1	2	3	4	5	6
c	Security is one of the main concern when deploying the e-commerce business	1	2	3	4	5	6
d	Security is one of the main issue management seek and emphasis when deploying the e-commerce business	1	2	3	4	5	6

e	Data confidentiality is the company objective when the company wants to deploy the e-commerce business	1	2	3	4	5	6
f	The integrity of data is the company objective when the company wants to deploy the e-commerce business	1	2	3	4	5	6
g	User authentication is the company objective when the company wants to deploy the e-commerce business	1	2	3	4	5	6
h	System availability is the company objective when the company wants to deploy the e-commerce business	1	2	3	4	5	6

Question 7	The value of security towards your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	Security implementation can help the company to increase the business reputation e.g. implementing WebTrust Seal on the e-commerce website	1	2	3	4	5	6
b	Security control implemented in the company e-commerce has increase users trust in using the e-commerce site	1	2	3	4	5	6
c	Security control practices in the e-commerce business have increase the company efficiency e.g. staff are clear about business procedure and expectations	1	2	3	4	5	6
d	Security control practices has increase e-commerce site availability	1	2	3	4	5	6
e	Security control practices has educate staff and users on the importance of confidentiality and data integrity	1	2	3	4	5	6
f	Security control practices have made the business more proficient as compared to other business competitors because everyday task is conducted following the policies and procedure underline by the company	1	2	3	4	5	6
	Security control practices implemented in the e-commerce business have indirectly support the government initiatives in providing better e-commerce services to the e-commerce users in Malaysia	1	2	3	4	5	6

h	All security control implemented and practiced in the e-commerce business has increase the business value towards in terms of the business structure and communication	1	2	3	4	5	6
i	Security investment is aligned to business objectives of the company	1	2	3	4	5	6

Question 8	The security usage in your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	The security tools and techniques are used to secure our company's website	1	2	3	4	5	6
b	The security tools and techniques are used in the e-commerce solutions to help the company provide new and better services to the users	1	2	3	4	5	6
c	The security tools and techniques adopted by the company can help deter and prevent users from system misused	1	2	3	4	5	6
d	The usage of security tools and techniques is one of the way company used to promote the business	1	2	3	4	5	6
e	The security tools and techniques adopted by the company helps the company to compete with the business competitor	1	2	3	4	5	6
f	The security tools and techniques are used to safeguard company asset e.g. users data	1	2	3	4	5	6
g	The security tools and techniques are adopted by the company to fulfill users request	1	2	3	4	5	6
h	The security tools and techniques are implemented in the company to comply with the legislation enacted by the government	1	2	3	4	5	6
i	The security tools and techniques adopted by the company follows the standards developed by the expert	1	2	3	4	5	6
j	The company can receive certification by standardization body e.g. SIRIM, by implementing effective and appropriate security tools and techniques	1	2	3	4	5	6

k	The security tools and techniques are used to increase customers' trust towards the company e-commerce business	1	2	3	4	5	6
l	The security tools and techniques is implemented to safeguard the company from any form of threats and risks	1	2	3	4	5	6
m	The security tools and techniques is adopted to follow the current business trend	1	2	3	4	5	6

Questions 9	The security communication structure in your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	Information on security tools and techniques available in the company is shared using the Intranet	1	2	3	4	5	6
b	Information on new security tools and techniques are circulated in the company using internal e-mail	1	2	3	4	5	6
c	All issues on security tools and techniques adopted by the company can be discussed formally in the company meetings	1	2	3	4	5	6
d	All issues on security tools and techniques adopted by the company can be discussed informally over lunch or break in the company	1	2	3	4	5	6
e	All new implementation or adoption of security tools and techniques has to be approved by the highest management in the company	1	2	3	4	5	6
f	All new implementation and adoption of security tools and techniques usually received strong support from the management	1	2	3	4	5	6
g	All security tools and techniques adopted must be practiced by all staff in the company	1	2	3	4	5	6
h	Information on security tools and techniques used for a specific task or specific employee are usually circulated to all staff via the Intranet	1	2	3	4	5	6
i	All security tools and techniques practices are the responsibility of the staff in the company	1	2	3	4	5	6

j	All security tools and techniques updates are inform formally in meeting	1	2	3	4	5	6
k	All security tools and techniques updates are inform informally by word of mouth	1	2	3	4	5	6
l	All new security tools and techniques demonstration is formally done and tested before full deployment	1	2	3	4	5	6
m	All new security tools and techniques demonstration are conducted in a special meetings involving all staff in the company	1	2	3	4	5	6

Question 10	The support and enabler for security implementation for your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	Budget are usually allocated for security implementation in a year	1	2	3	4	5	6
b	Security training is part of the staff Key Performance Index (KPI) in the company	1	2	3	4	5	6
c	Security knowledge sharing session is encouraged by the management	1	2	3	4	5	6
d	Security knowledge sharing session is conducted every month	1	2	3	4	5	6
e	Specific or special training required by critical staff in the company is conducted at least once a year	1	2	3	4	5	6
f	Incentives are given to staff who show fluency in company policy through dedicated programs e.g. quizzes conducted around the year	1	2	3	4	5	6
g	The Malaysia government has play an effective role to encourage security implementation in e-commerce business by allocating special consultancy body to help us	1	2	3	4	5	6
h	The standards and best practices available in Malaysia are appropriate to assist our e-commerce business to implement security practices	1	2	3	4	5	6
i	The technology provided by local vendors is enough to assist the quest to implement security for the e-commerce business	1	2	3	4	5	6

j	Communication technology provided by local communication providers are compatible with the security tools and security system the company is using currently	1	2	3	4	5	6
k	The technology chosen by the company to develop secure e-commerce business are sufficient to accommodate the business objective	1	2	3	4	5	6
l	The technology chosen by the company to develop secure e-commerce business are compatible with new Internet technology available in the market	1	2	3	4	5	6
m	The legislations available in Malaysia strongly support security implementation for any e-commerce initiatives	1	2	3	4	5	6

Question 11	The barriers to effective security in your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	The company does not give us much time to implement new security tools and techniques because of the high workload given	1	2	3	4	5	6
b	Currently, the company cannot afford to pay the high price of security tools and security implementation for the e-commerce business	1	2	3	4	5	6
c	The company do not have any security measures in the e-commerce business because security implementation is very difficult	1	2	3	4	5	6
d	There are no security trainings provided because it is too expensive	1	2	3	4	5	6
e	The company does not have many staff to help implement security controls and practices	1	2	3	4	5	6
f	There are no requirement from the management to learn new security tools and techniques which are not appropriate to our job scope	1	2	3	4	5	6
g	There are no new knowledge or information gained from the knowledge sharing session conducted periodically in the company	1	2	3	4	5	6

h	The company does not provide any incentives or reward to the staff that are fluent with company's security policy or procedure	1	2	3	4	5	6
i	The security tools implementation are too complex and complicated for us	1	2	3	4	5	6
j	The security techniques or mechanisms are too complex and complicated for us	1	2	3	4	5	6
k	There are no encouragement provided by the management to implement security tools and techniques	1	2	3	4	5	6
l	There are no necessity to implement any security tools and techniques because the e-commerce business is still small and the company consist of a small number of staff	1	2	3	4	5	6

Question 12	The types of security implementation influences in your e-Commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	The technology we used has influence the security implementation in the company	1	2	3	4	5	6
b	The company technology suppliers has provide an excellent support in the quest to implement security	1	2	3	4	5	6
c	The company have received extra funding from the government body to implement security tools and techniques	1	2	3	4	5	6
d	The management encourage security implementation in the e-commerce business	1	2	3	4	5	6
e	Even though the company consist of small staff, security is perceived as an important element as other work task in the business	1	2	3	4	5	6
f	All of the business competitors has implemented security practices in their business, thus it is important for the company to do so	1	2	3	4	5	6

g	In order to compete in the e-commerce world, the company need to have strong value in the services the company is offering where security is considered as an important value of an e-commerce business	1	2	3	4	5	6
h	Confidentiality, data integrity, users authentication and availability are important factors in e-commerce business	1	2	3	4	5	6
i	It is the requirement of the e-commerce users of the company to have security implemented in the e-commerce site	1	2	3	4	5	6
j	The standards and best practices available has influenced how the company implement security practices in the company	1	2	3	4	5	6
k	The government legislation has influence the company to implement security for the e-commerce site	1	2	3	4	5	6

Question 13	The security responsibility and current structure in your e-commerce	Answer choice					
		Strongly Agree ↓	Some what agree ↓	Neither agree or disagree ↓	Some what disagree ↓	Strongly disagree ↓	Don't know ↓
a	The government is responsible in the security implementation for e-commerce business	1	2	3	4	5	6
b	The company management is responsible in the security implementation for e-commerce business	1	2	3	4	5	6
c	The staff in the company are responsible in the security implementation for e-commerce business	1	2	3	4	5	6
d	The technology used and provided by local providers has to support the business requirement to help implement security practices in e-commerce business	1	2	3	4	5	6
e	The industry players has to support the security implementation in the e-commerce sector	1	2	3	4	5	6

f	There are no clear point of contact of the company can liaise to in the effort to assist e-commerce business to implement security management in the business	1	2	3	4	5	6
g	There are many efforts done by the local authority on security management implementation but these attempts are not transparent to the e-commerce business.	1	2	3	4	5	6
h	The Malaysian government has develop a specific body is entrusted to educate and enhance the awareness of the general public on the technological and social issues facing internet users, particularly on the dangers of getting online for example CyberSecurity Malaysia	1	2	3	4	5	6

ATTENTION: We invite company participation into our e-Commerce company model program.

Are you interested to become one of the company models?

(Please cross [x] your answer)

<input type="checkbox"/>	YES , I am interested. Please contact me.
<input type="checkbox"/>	NO , I am not interested. Do not include me in the list
<input type="checkbox"/>	NOT SURE . You can contact me later.

For feedback on trainings and support purpose, we will be happy if you could fill in the information below.

1	Name:	
2	Web address (website):	http://
3	Email address:	
4	Telephone No. and Fax No.:	
5	What is the estimated company annual income from the e-commerce business? (Please cross [x] one box)	<input type="checkbox"/> less than RM15,000 <input type="checkbox"/> between RM15,000 to RM49,999 <input type="checkbox"/> between RM50,000 to RM99,999 <input type="checkbox"/> more than RM100,000
6	What is your current position in the company? (Please cross [x] one box)	<input type="checkbox"/> Owner/ CEO <input type="checkbox"/> Management <input type="checkbox"/> Executive <input type="checkbox"/> Expert/ Consultant

PLEASE MAIL COMPLETED SURVEY FORM TO:

Ketua Pengarah
Perbadanan Produktiviti Malaysia
Peti Surat 64, Jalan Sultan
46904 Petaling Jaya
(UP: Puan Melissa Ahmad Arshad)

USING THE STAMPED ENVELEOP INCLUDED



APPENDIX B

OPERATIONAL VARIABLES AND INDICATORS

Table B.1: Independent constructs and indicators

No	Construct	Indicator construct	Code
1	Organizational size (formative)	size of your e-commerce company	ORGs
2	Business length (formative)	length being in the e-commerce business	BIZI
3	e-Commerce stage (formative)	stage of e-commerce adoption	ecS
4	Top management Support (TopMS) (reflective)	1. New implementation of security tools and techniques has to be approved by the highest management 2. New implementation of security tools and techniques received strong support from the management 3. Budget are allocated for security implementation in a year 4. Security training is staff Key Performance Index (KPI) 5. Security knowledge sharing is encouraged by the management 6. Security knowledge sharing is conducted every month 7. Training required by critical staff is conducted once a year 8. The management encourage security implementation 9. The management is responsible on security implementation	TM1 TM2 TM3 TM4 TM5 TM6 TM7 TM8 TM9

Table B.2: Mediator constructs and indicators

No	Construct	Indicator construct	Code
4	Security Management Purpose (reflective)	1. Security tools (technologies) important for the company 2. Security techniques (procedures and policies) important to the company 3. Security is main concern in deploying the e-commerce business	SMPur1 SMPur2 SMPur3

Continued on the next page

Table B.2 – *Continued from previous page*

No	Construct	Indicator construct	Code
		4. Security is the main issue emphasized by management	SMPur4
		5. Data confidentiality is the company objective	SMPur5
		6. The integrity of data is the company objective	SMPur6
		7. User authentication is the company objective	SMPur7
		8. System availability is the company objective	SMPur8
5	Security Management Value (reflective)	1. Security implementation help increase business reputation	SMVal1
		2. Security control implemented has increase users trust	SMVal2
		3. Security control practices has increase the company efficiency	SMVal3
		4. Security control practices has increase e-commerce availability	SMVal4
		5. Security control practices has educate staff and users of the importance of security management	SMVal5
		6. Security control practices has made business more proficient compared to other business competitors	SMVal6
		7. Security control practices indirectly support government initiatives in providing better e-commerce services	SMVal7
		8. Security control practiced has increase business value	SMVal8
		9. Security investment is aligned to business objectives	SMVal9

Continued on the next page

Table B.2 – *Continued from previous page*

No	Construct	Indicator construct	Code
6	Security Management Utilization (reflective)	1. The security tools and techniques are used to secure website	SMUU1
		2. The security tools and techniques are used in the e-commerce solutions to provide new and better services	SMUU2
		3. The security tools and techniques adopted help deter and prevent users from system mis-used	SMUU3
		4. The usage of security tools and techniques is a way to promote business	SMUU4
		5. Security tools and techniques helps compete with competitor	SMUU5
		6. Security tools and techniques use to safeguard company asset	SMUU6
		7. Security tools and techniques are adopted to fulfill users request	SMUU7
		8. Security tools and techniques are implemented to comply with the government legislation	SMUU8
		9. Security tools and techniques follows security standards	SMUU9
		10. The company can receive certification by standardization body with effective security tools and techniques	SMUU10
		11. Security tools and techniques used to increase customers' trust	SMUU11
		12. Security tools and techniques is implemented to safeguard the company from threats and risks	SMUU12
		13. Security tools and techniques adopted to follow business trend	SMUU13

Continued on the next page

Table B.2 – *Continued from previous page*

No	Construct	Indicator construct	Code
		14. Information on security tools and techniques are shared using the Intranet	SMUS1
		15. Information on new security tools and techniques are circulated using internal e-mail	SMUS2
		16. Issues on security tools and techniques are discussed formally	SMUS3
		17. Issues on security tools and techniques are discussed informally	SMUS4
		20. Security tools and techniques are practiced by all staff	SMUS7
		21. Information on security tools and techniques used for a specific task are circulated to all via the Intranet	SMUS8
		22. Security tools and techniques practices are the responsibility of the staff	SMUS9
		23. Security tools and techniques updates inform formally in meeting	SMUS10
		24. Security tools and techniques updates inform informally by word of mouth	SMUS11
		25. New security tools and techniques demonstration is formally done and tested before full deployment	SMUS12
		26. New security tools and techniques demonstration are conducted in meetings	SMUS13
7	Security Management Support and Responsibility (reflective)	6. Incentives are given to staff fluent with company policy	SMS6
		7. Malaysia government plays an effective role in security management by allocating special consultancy body	SMS7

Continued on the next page

Table B.2 – *Continued from previous page*

No	Construct	Indicator construct	Code
		8. Standards and best practices available are appropriate to assist e-commerce to implement security practices	SMS8
		9. Technology provided by local vendors is enough to implement security management	SMS9
		10. Communication technology provided by local providers are compatible with security implementation	SMS10
		11. Technology chosen to develop secure e-commerce are sufficient following business objective	SMS11
		12. Technology chosen to develop secure e-commerce are compatible with current Internet technology	SMS12
		13. Legislations available strongly support security implementation	SMS13
		14. Government is responsible on security implementation	SMR1
		16. Staff are responsible in the security implementation	SMR3
		17. Technology used and provided by local providers support the business requirement to implement security practices	SMR4
		18. The industry players support the security implementation	SMR5
		19. There are no clear point of contact to assist e-commerce business to implement security management	SMR6
		20. Many security efforts by local authority but are not transparent	SMR7

Continued on the next page

Table B.2 – *Continued from previous page*

No	Construct	Indicator construct	Code
		21. Specific body is entrusted to educate and enhance the awareness of the general public on security management	SMR8
8	Security Management Influence (reflective)	1. Technology influence the security implementation in company	SMI1
		2. Technology suppliers provide excellent support to implement security	SMI2
		3. The company received funding from the government to implement security	SMI3
		5. Even though the company consist of small staff, security is perceived as important	SMI5
		6. Business competitors implemented security practices thus it is important for the company to do so	SMI6
		7. In order to compete in the e-commerce world, security gives important value towards e-commerce business	SMI7
		8. Confidentiality, data integrity, users authentication and availability are important factors in e-commerce business	SMI8
		9. Security is users requirement for e-commerce	SMI9
		10. Standards and best practices has influenced security practices	SMI10
		11. The government legislation has influenced security practices	SMI11
		12. Not much time to implement new security tools and techniques because of the high workload	SMB1
		13. Cannot afford to pay high price of security implementation	SMB2

Continued on the next page

Table B.2 – *Continued from previous page*

No	Construct	Indicator construct	Code
		14. Do not have security measures because security implementation is very difficult	SMB3
		15. Security trainings not provided because it is too expensive	SMB4
		16. Not many staff to implement security controls and practices	SMB5
		17. No requirement from management to learn new security tools and techniques	SMB6
		18. No new knowledge gained from the knowledge sharing session conducted periodically in the company	SMB7
		19. Company does not provide any incentives to staff who are fluent with company's security policy or procedure	SMB8
		20. Security tools implementation are too complex and complicated	SMB9
		21. Security techniques are too complex and complicated	SMB10
		22. No encouragement by management to implement security tools and techniques	SMB11
		23. No necessity to implement any security tools and techniques because e-commerce business is small	SMB12

Table B.3: Dependent constructs and indicators

No	Construct	Indicator construct	Code
No	Construct	Indicator construct	Code
9	ISSM Maturity Consideration (reflective)	1.The company uses user log -in and password for system applications 2. The company uses SSL (Secure Socket Layer) certificate to secure web transaction	SMPos1 SMPos2

Continued on the next page

Table B.3 – *Continued from previous page*

No	Construct	Indicator construct	Code
		3. The company design policy e.g. for change of password every six months	SMPos3
		4. The company design a policy for validation purposes e.g. when customer register to our website	SMPos4
		5. The company store all users data and the system applications in secure servers	SMPos5
		6. The company store all back-up data in a physical location equip with physical security	SMPos6
		7. The company post business terms and condition in the website for everyone to read	SMPos7
		8. The company design the e-commerce site considering applicable security measures	SMPos8
		9. The company highlight security events in the website as a reminder to all	SMPos9
		10. The company test the e-commerce website on specific time which is mentioned in the website	SMPos10
		11. The company update the e-commerce website on specific time which is always mentioned in the website	SMPos11
		12. The company develop the e-commerce website following secure architecture proposed by experts	SMPos12
		13. The company uses standards and best practices to develop the policy and procedure for the e-commerce	SMPos13
		14. The company also conduct test on the network security following specific time	SMPos14
		15. The company install other security measure e.g. patches and antivirus	SMPos15

Continued on the next page

Table B.3 – *Continued from previous page*

No	Construct	Indicator construct	Code
		16. The company conduct internal audit on e-commerce business processes and activities	SMPos16
		17. The company have scheduled security training every year	SMPos17
		18. The company conducted knowledge sharing on security issues periodically	SMPos18
		19. The company follow security procedure when it is required in the everyday work	SMPos19
		20. The company understand by practicing good security procedure it will protect company asset	SMPos20
		21. The staff are responsible to read and understand the security events, policies and procedure of the company	SMPos21
		22. The company believed by keeping the staffs up to date company security policy it can protect the customer	SMPos22
		23. The company have recruited highly responsible and motivated staff	SMPos23
		24. The company is aware on the risks and threats an unsecure website can cost towards the business	SMPos24
		25. The company have formed a dedicated team to handle information security matters	SMPos25
		26. The company coordinate with the technology supplier on latest security issues.	SMPos26
		27. The staffs has the responsibility to report to the management on suspicious act which may cause security threats	SMPos27
		28. The company have created a policy and procedure to handle security incidents	SMPos28

Continued on the next page

Table B.3 – *Continued from previous page*

No	Construct	Indicator construct	Code
		29. The company have employed one accredited security professional to champion effort to provide secure services	SMPos29
		30. The company conducted risk analysis and assessment	SMPos30

APPENDIX C

QUANTITATIVE DATA ANALYSIS RESULTS USING PARTIAL LEAST SQUARE (PLS)

Table C.1: Outer Loading Score for Variables involved in the ISSM Maturity

No	Items/ Variables	Code	Variable Loading)
1	Length being in the e-commerce business	Business Length	1
2	Size of your e-commerce company	Business Size	1
3	The stage of e-commerce of the business	Business Type	1
4	New implementation of security tools and techniques received strong support from the management	TM2	0.812724
5	The management encourage security implementation	TM8	0.77796
6	Information on new security tools and techniques are circulated using internal e-mail	SMUS2	0.726324
7	Issues on security tools and techniques are discussed formally	SMUS3	0.835152
8	Security tools and techniques are practiced by all staff	SMUS7	0.718939
9	Security tools and techniques practices are the responsibility of the staff	SMUS9	0.777887
10	The integrity of data is the company objective	SMPur6	0.785509
11	System availability is the company objective	SMPur8	0.774487
12	The security tools and techniques are used to secure website	SMUU1	0.750788
13	Security tools and techniques is implemented to safeguard the company from threats and risks	SMUU12	0.72568
14	Security tools and techniques adopted to follow business trend	SMUU13	0.779572
15	The security tools and techniques are used in the e-commerce solutions to provide new and better services	SMUU2	0.78571
16	The security tools and techniques adopted help deter and prevent users from system misused	SMUU3	0.758358

Continued on the next page

Table C.1 – *Continued from previous page*

No	Items/ Variables	Code	Variable Loading
17	The usage of security tools and techniques is a way to promote business	SMUU4	0.784823
18	Security tools and techniques helps compete with competitor	SMUU5	0.789099
19	Security tools and techniques use to safeguard company asset	SMUU6	0.740168
20	Security tools and techniques are adopted to fulfill users request	SMUU7	0.856802
21	Security tools and techniques are implemented to comply with the government legislation	SMUU8	0.774517
22	Security tools and techniques follows security standards	SMUU9	0.791906
23	Staff are responsible in the security implementation	SMR3	0.865903
24	Technology used and provided by local providers support the business requirement to implement security practices	SMR4	0.731652
25	The industry players support the security implementation	SMR5	0.809415
26	The company uses user log -in and password for system applications	SMt1	0.763449
27	The company uses standards and best practices to develop the policy and procedure for the e-commerce	SMt13	0.72841
28	The company also conduct test on the network security following specific time	SMt14	0.844292
29	The company install other security measure e.g. patches and antivirus	SMt15	0.71007
30	The company conduct internal audit on e-commerce business processes and activities	SMt16	0.717263
31	The company have scheduled security training every year	SMt17	0.791749
32	The company conducted knowledge sharing on security issues periodically	SMt18	0.778739
33	The company understand by practicing good security procedure it will protect company asset	SMt20	0.803647
34	The staff are responsible to read and understand the security events, policies and procedure of the company	SMt21	0.841053
35	The company believed by keeping the staffs up to date company security policy it can protect the customer	SMt22	0.757277
36	The company have recruited highly responsible and motivated staff	SMt23	0.731416

Continued on the next page

Table C.1 – Continued from previous page

No	Items/ Variables	Code	Variable Loading
37	The company is aware on the risks and threats an unsecure website can cost towards the business	SMt24	0.836189
38	The company have formed a dedicated team to handle information security matters	SMt25	0.742173
39	The staffs has the responsibility to report to the management on suspicious act which may cause security threats	SMt27	0.806721
40	The company have created a policy and procedure to handle security incidents	SMt28	0.765046
41	The company conducted risk analysis and assessment	SMt30	0.830591
42	The company design a policy for validation purposes e.g. when customer register to our website	SMt4	0.740014
43	The company store all users data and the system applications in secure servers	SMt5	0.822485
44	The company design the e-commerce site considering applicable security measures	SMt8	0.784296
45	The company highlight security events in the website as a reminder to all	SMt9	0.718963

Table C.2: Cross Loading Score for Variables involved in the ISSM Maturity

	Code	Biz Length	Biz Size	Biz Type	Top Mngt Support	Techno	Org	Environ	ISSM Maturity
Business Length		1.0000	0.5845	0.4550	-0.0115	-0.0032	-0.0014	-0.1972	-0.2684
Business Size		0.5845	1.0000	0.0913	-0.0291	0.0262	0.1293	-0.0512	-0.1014
Business Type		0.4550	0.0913	1.0000	-0.2468	-0.1731	-0.1408	-0.3141	-0.5161

Continued on the next page

Table C.2 – Continued from previous page

	Code	BizLength	Business Size	Business Type	Top Mngt Support	Tech	Org	Environ	ISSM Matu- rity
Top Man- age- ment Support	TM2	-0.0593	-0.1811	-0.1004	0.8480	0.6889	0.6212	0.6492	0.3475
	TM8	0.0450	0.0388	-0.2965	0.8575	0.6121	0.6567	0.6460	0.6075
Technology	SMUS2	-0.2472	-0.1204	-0.2775	0.4840	0.7454	0.4577	0.3644	0.3644
	SMUS3	-0.0250	0.0880	-0.1261	0.6271	0.7912	0.6562	0.6325	0.2185
	SMUS7	0.1939	0.0759	-0.0160	0.6420	0.8262	0.4751	0.5357	0.2589
	SMUS9	0.0268	0.0231	-0.1590	0.7287	0.8699	0.6715	0.6864	0.3783
Organizational	SMPur6	0.0656	0.1885	-0.0675	0.4982	0.5210	0.7553	0.5016	0.2723
	SMPur8	0.0322	0.3132	-0.1380	0.4839	0.5111	0.7573	0.5235	0.3633
	SMUU1	-0.0548	0.2457	-0.2483	0.6926	0.5952	0.7807	0.6950	0.4844
	SMUU12	0.0303	0.1273	-0.0369	0.6867	0.6228	0.7529	0.6281	0.4448
	SMUU13	-0.0185	0.1438	-0.0490	0.6835	0.6463	0.8058	0.7271	0.4726
	SMUU2	-0.1216	0.0150	-0.1531	0.6199	0.5091	0.8174	0.7220	0.4398
	SMUU3	-0.0154	0.1196	-0.0952	0.6391	0.4928	0.7870	0.6753	0.4551
	SMUU4	0.0301	0.0409	0.0328	0.5434	0.4814	0.7980	0.6420	0.2500
	SMUU5	-0.0255	-0.0220	-0.1430	0.5453	0.5490	0.7977	0.6643	0.4443
	SMUU6	-0.1391	-0.0721	-0.1908	0.6735	0.5655	0.7688	0.7222	0.4545
	SMUU7	0.0666	0.1163	0.0495	0.6624	0.6569	0.8733	0.6771	0.4153
	SMUU8	0.1544	0.1331	0.1812	0.5183	0.5473	0.7712	0.5941	0.2501
SMUU9	-0.0120	0.1776	-0.2365	0.6860	0.6841	0.8092	0.7101	0.4206	
Environment	SMR3	-0.1526	0.0260	-0.2385	0.7581	0.5865	0.6914	0.8414	0.5051
	SMR4	-0.1998	-0.0977	-0.3028	0.6482	0.5263	0.7252	0.8822	0.4845
	SMR5	-0.1726	-0.0702	-0.2938	0.7617	0.7262	0.7191	0.9258	0.4748
ISSM Matu- rity	SMt1	-0.1045	0.0086	-0.4935	0.3814	0.2541	0.2443	0.2985	0.7532
	SMt13	-0.0228	0.0508	-0.2130	0.5820	0.3916	0.4515	0.4864	0.7397
	SMt14	-0.2512	-0.0836	-0.4079	0.4833	0.3213	0.3895	0.3883	0.8716
	SMt15	-0.2678	-0.1797	-0.4253	0.4199	0.3264	0.4677	0.3758	0.7314
	SMt16	-0.2160	0.0000	-0.3264	0.4810	0.3500	0.4202	0.5605	0.7230

Continued on the next page

Table C.2 – Continued from previous page

	Code	BizLength	Business Size	Business Type	Top Mngt Support	Tech	Org	Environ	ISSM Matu- rity
	SMt17	-0.2991	-0.2294	-0.4230	0.3667	0.1987	0.2996	0.4183	0.7703
	SMt18	-0.1933	-0.0060	-0.3988	0.4167	0.2648	0.3868	0.3817	0.7949
	SMt20	-0.3390	-0.2380	-0.3480	0.4735	0.3031	0.4328	0.5027	0.8016
	SMt21	-0.2374	-0.1094	-0.3202	0.3985	0.2850	0.4167	0.5296	0.8504
	SMt22	-0.2147	-0.0893	-0.1748	0.3752	0.3065	0.4777	0.4051	0.7685
	SMt23	-0.2210	0.0355	-0.3005	0.4432	0.3423	0.4292	0.4770	0.7550
	SMt24	-0.1156	0.0031	-0.3192	0.4652	0.3299	0.5213	0.4722	0.8584
	SMt25	0.0652	0.0042	-0.3680	0.4441	0.2584	0.3556	0.2861	0.7205
	SMt27	-0.3160	-0.2230	-0.4614	0.4940	0.3662	0.4547	0.6380	0.8001
	SMt28	-0.3265	-0.1775	-0.5539	0.4389	0.3587	0.3537	0.5115	0.7656
	SMt30	-0.2512	-0.1101	-0.4623	0.3769	0.2189	0.3812	0.4122	0.8394
	SMt4	-0.2860	0.0542	-0.5603	0.3714	0.2752	0.3838	0.3841	0.7611
	SMt5	-0.3421	-0.1422	-0.5761	0.4257	0.2994	0.2854	0.4445	0.8349
	SMt8	-0.0176	0.0344	-0.4129	0.4678	0.2707	0.3609	0.3835	0.7612
	SMt9	-0.1327	-0.1143	-0.3875	0.4365	0.1632	0.2305	0.2440	0.7173

APPENDIX D

QUALITATIVE ANALYSIS TABLE

ISSM Maturity: Qualitative Analysis Table

No	Themes	Sub-themes	Issues	Quotes	Reference	Relationship to theories
1	Organization	Business type/ structure	Business need/ requirement/ business mission/ business objective	<i>AZ: ...other influence in you implementing security... GX: I think in mine, because most of my customer are multinationals and also principle are.. I deal with vendors supplier from overseas</i>	I5_NZA-GX Row: 65-66	organization -formal linking structure
				<i>HS: ...I used to do a lot of work with international authorities, so manage to make a lot of contact with European authorities, and they sometimes pass me some cases to investigate...</i>	I2_HS-TB Row: 63	
				<i>AHS: security tools apa yang ada yeh.. consideration dier lah...satu needs... AZ: so keperluan company nih important lah... AHS: mcm company nih needs two cost, we will not go with the most expensive ones or nor e will use the cheapest ones.</i>	I7_AHS-PTS Row: 281-283	
				<i>US: I see a need for that, like i said based on the maturity of the company. Because security is important. I realized that cuma depending on the level of the company punya resources dier focus dier.. tu semualah kan. So if you have the tool it should be based on certain number of website ker network ker, but if you have standards that people can use, to assess their security level, it would be good laa</i>	I6_DL-US Row: 161	
				<i>SS: ...no.. security must suit business objective... that is why they have many choices.. you have to understand exactly, what type of security that you need and what type of data you need to protect, so as I say just now.. it cannot rely on SSL.. but few other things we have to implement all together</i>	I4_MD-SS Row: 94 and 96	
				<i>GX: also the nature of my business.. i think we deal with intellectual property, consulting and training. SO that nature of business is something that we need to protect</i>	I5_NZA-GX Row: 70	
				<i>KY: well, Firstly as I think as an owner of a business, coming from that perspective, you have to understand the business very well, the industry that you are in and how security fits into that whole ecosystem, right.</i>	I1_KY-SW Row: 20	

ISSM Maturity: Qualitative Analysis Table

				<i>AHS: dier kan semua nak buat (referring to security management)... tapi resources tak de, and then saiz takde...</i>	I7_AHS-PTS Row: 89
				<i>AHS: As owner.. I know it is important. But as an owner you know how much you want to put into it. Because i think our need and requirement right now is consider quite small. Because our e-commerce site pun is considered small.</i>	I7_AHS-PTS Row: 227
				<i>AHS: something that is already hurting them or has hurt them.. haaaa... yang itu dier akan letak duit dulu</i>	I7_AHS-PTS Row: 271
				<i>AZ: for you that is number one that you have to take care if you want to do e-commerce... SS: yes, that is actually the priority.. when you think about e-commerce the transaction data.. there are the most you have to think about. You have to solve and find solution for that first before you start</i>	I4_MD-SS Row: 11-12
				<i>SS: ok.. e-commerce actually we can say it relate 100% to security. You cannot implement e-commerce without that, it is not just protecting your customer but it is protecting you, because of fraud .. what so ever, like my example just now.. gateway provider, payment gateway provider.. will not take any responsibility, everything is actually bounced back to us, so that is why we have to take care of our part.. whatever that happen later we have a proof from our side. So don't thing security for your website is just a simple-simple one.. because it is very important</i>	I4_MD-SS Row: 200
				<i>HV: ...Nothing to do with hard ware...nothing to do with all is about what you need to do in business je. What to ensure the business runs, nothing to do with technology.. all is influence by the need for the company to survived</i>	I3_AR-HV Row: 95
				<i>HV:tapi if u want to be competitive.. your market is not Malaysia, the you have to do it.. if you need to do global.. u need to do e-commerce....if you want to do e-commerce you need to have securitylaa.. that is important.</i>	I3_AR-HV Row: 219
				<i>AZ: so it is also important that when you are in the market you have to know what type of security management to implement... KY: correct, fits</i>	I1_KY-SW Row: 49-50

ISSM Maturity: Qualitative Analysis Table

		<p><i>your market. Yaah</i></p> <p><i>AZ: Basically it (refer to security management) depend on what you users want and do not want, according to the business requirement... KY: correct</i></p> <p><i>AZ: company objectivelah kirernya... HV: yeah.. i mean you want.. our business model is on the internet based so we can't afford to not protect our system, nothing to do with technology...</i></p> <p><i>AZ: how about the company type? Do you thing type of business you play in the e-commerce important for you to implement security or not, you know like finance... HS: they should, of course they should. For them they have to play another part of role la.. different part of roles,...</i></p> <p><i>AHS: ...sebenenarnya our security focus for this year is securing our internal network. Not so much of our e-commrce site... Because...our internal problem... bila kita dah ada 150 devices... PC Laptop, phones, fax semua. Masalah mcm staff running illegal program.. dah ada.. kemudian ialah virus, kemudian nak manage internet access kat dalam. So you start putting on firewall lah, nak kene manage itulah, securing our work now. Sekarang data lost is one big area we are worried now.</i></p> <p><i>AHS: I fikir buku nih orang tak berapa sgt apalah.. sebab choice banyak, tapi I rasa our e-commerce akan naik bila kita start offering e-book... I rasa masa tuh baru betul2, baru betul2 business.... AZ: problemnya bila expand tuh some of the problem mcm nih lah...the copyright issue come in... AHS: of course, mau tak mahu kita terpaksa laa...</i></p>	<p>I1_KY-SW Row: 121-122</p> <p>I3_AR-HV Row: 96-97</p> <p>I2_HS-TB Row: 132-133</p> <p>I7_AHS-PTS Row: 243 and 247</p> <p>I7_AHS-PTS Row: 99 and 101-103</p>	
Top management support	motivation and perception	<p><i>AHS: sbb kalau kita tengok issue dier.. i personal memang i minat, so we keep up.. i do a lot of self-reading. So i minat, Cuma bila sampai hal technical jer i pass it to the budak2 itlah, kalau tak i sendiri takdelah kan...tapi big ideas.. masih lagi kat kita lah. Tapi itu sebab personal.. itu issue dier, sebab i minat, not applicable to all cases tau. I personal memang i minat</i></p>	<p>I7_AHS-PTS Row: 345</p>	<p>organization informal linking stucture (human resources)</p>

ISSM Maturity: Qualitative Analysis Table

				<p>AHS: ...whatever you like cannot be in your business. Kadnag2 business tak selaju macam kita punya .. our own fascination tu kita layan sendiri jek. So business masih kene ikut business</p>	<p>I7_AHS-PTS Row: 351</p>
				<p>AZ: ... do you get enough support from your management to implement security... HS: my company.. of course...not in the beginning but once they see that this verification flow is actually helps them a lot then of course</p>	<p>I2_HS-TB Row: 111-112</p>
				<p>US: ...we do not want to be bothered by all this security issues</p>	<p>I6_DL-US Row: 225</p>
				<p>GX: ...or if you think your process is not good enough buy a system and adopt to that system adapt your process to that system, but willing to change... the ability to change is also another issues in SME, are we flexible enough to change...</p>	<p>I5_NZA-GX Row: 78</p>
				<p>GX: ...oohh do we have to weigh this between advertising, marketing.. which one comes first. Is it sale come in first or is it technology comes in first and most of the time sale will take priority. So that is why when you ask a lot of people.. do you invest on security or do you invest in advertising.. ohh every one will go.. advertising because at least I know my product is being sold. But investing for technology (security)...</p>	<p>I5_NZA-GX Row: 72</p>
				<p>AHS:Until today.. you cuba bayangkan. this is old industry (publishing)..setengah tak boleh buat apa.. mati camtuh jer takleh buat apa2. mcm tuh jer, so not easy</p>	<p>I7_AHS-PTS Row: 159</p>
				<p>AHS: kalau u cakap pasal average SMI haa.. the non-technology based company apa? Assumption kata security is in house.. is probably wrong</p>	<p>I7_AHS-PTS Row: 475</p>
				<p>US: so security management....[pause] I guess, i know it is important but implementation wise we don't really see that as a focus for our business.</p>	<p>I6_DL-US Row: 4</p>

ISSM Maturity: Qualitative Analysis Table

			<p>GX: ...A lot of SME think... ohh no we need firewall.. we need this we need that.. then we go like, you don't really need to do that.. you know what I mean. Look at it as a simple perspective. Security management means to ensure whatever information that you have internally is being controlled and managed.</p>	I5_NZA-GX Row: 100	
			<p>GX: like for us we do capital investment, consider that as capital investment.. we believe that some point or rather it is a long term investment that would bring in money but we struggle with the fact that it is not bringing in money fast enough.</p>	I5_NZA-GX Row: 54	
			<p>GX: ...so we try to look at cost effective ways of doing this and I find that for SMEs, there are cost effective ways to do this laa,</p>	I5_NZA-GX Row: 4	
			<p>GX: ...and i can access my system from overseas and I can monitor and I can view. And I know that.. it gives me that comfort... AZ: meaning there is availability.. with security there is availability... GX: yeah...</p>	I5_NZA-GX Row: 54-56	
			<p>AZ: You don't know whether government should create a body to foresee all this but whatever they want to do it has to start from the rootlaa kirernya... US: yes.</p>	I6_DL-US Row: 208-209	
	directive		<p>AZ:who determines security management in your company, you yourself? ...GX: Yes I do</p>	I5_NZA-GX Row: 109-110	Organization - formal linking structure
			<p>AZ: ...who determines implement or not to implement security? ...KY: me</p>	I1_KY-SW Row: 111-112	
			<p>AZ: when you want to implement your security flow or your verification flow, who actually determines to implement or not to implement... HS: managers, CEOs.</p>	I2_HS-TB Row: 168-169	
			<p>AZ: ...who determines it in your business?... US: most of the time myself, in this business i have three partners, myself, hanny and my husband. So my husband is more of the technical person laaa. Usually kalau kita nak discuss pasal technical issues, I will pass to him...</p>	I6_DL-US Row: 87-88	

ISSM Maturity: Qualitative Analysis Table

		<p>AZ: ...when you implement security management siapa determine implementation of security management?... HV: its from the top, the CEO of course</p>	I3_AR-HV Row: 114-115	
		<p>AHS: sebenarnya dalam small company mc PTS, IT ada tapi they will wait for the que from me lah, usually lah, they wait for the que from me baru allocate budget yang banyaklah.</p>	I7_AHS-PTS Row: 311	
		<p>GX: ...from the first day I started business, website (including security management) is already a critical element we knew we needed to have, and we revamped, and we restructured and we change</p>	I5_NZA-GX Row: 88	
	Business size	<p>AHS: dier kan semua nak buat... tapi resources tak de, and then saiz takde...</p>	I7_AHS-PTS Row: 227	organization-size
		<p>AZ: ... will that (security management) help you to simplify your business process in a way... US:: at this point, not really, at this point... tak because kita tak de banyak2 branch lagi kan. It is just here kan..</p>	I6_DL-US Row: 9-10	
		<p>AZ: I am sure CEO are aware of security implementation... US: big CEO yeaahh... but the little ones</p>	I6_DL-US Row: 216-217	
		<p>AHS: As owner.. I know it is important. But as an owner you know how much you want to put into it. Because i think our need and requirement right now is consider quite small. Because our e-commerce site pun is considered small. But probably next year when we strat e-book punya maybe we ave to increase our budget for securities issues...</p>	I7_AHS-PTS Row: 89	
		<p>HS: you see small company don't have so much loses. You know one time we have fraud company coming in buying everything with fake credit card fake credit card and then chow. This is the company we target... the big guys. These guys don't go to the small2 e-commerce they go to the big e-commerce. The small company do not have so much loses... maybe they have but maybe 20%? There wasn't much for them; they know this is the risk they have to take.</p>	I2_HS-TB Row: 29	

ISSM Maturity: Qualitative Analysis Table

				<i>SS: so far no.. as long as it is compatible with our system, but of course we have process of what we implementing.. but the standard procedure not so because we are so small.</i>	I4_MD-SS Row: 150	
		business status	sales volume	<i>AHS: dier kalau volume naik... resource sure kene tambah nyer... kalau you ada resource pun...katalah you ada RM100ribu to spend, kata volume transaction 40 ribu sebulan.. you won't spend 100K</i>	I7_AHS-PTS Row: 91	
				<i>AHS: kalau kata volume dier increasekan...mau tak mau you kene carik duit untuk expend nak support (refering to security management)</i>	I7_AHS-PTS Row: 93	
				<i>AHS: so far takdelah.. i rasa issuenyer volume kan.. kalau orang crack pun ornag akan tengok site yang ada volume, if you talk about lelong.. i rasa dier ornag selalu kene ni</i>	I7_AHS-PTS Row: 443	
2	Organization Resources	technological	IT infrastructure	<i>AHS: technology gets easier.. market force, i really think yg sekarang kerajaan buat sekarang nih.. yang broad band penetration nih.. i really think that one will gonna help.</i>	I7_AHS-PTS Row: 167	Technology-characteristic
				<i>GX: connectivity is an issue.. AZ: do you think the technology are at par with whatever we want to implement in the business security management, meaning.. is for example.. if TM providing enough connectivity, Maxis giving it.. is Celcom providing it... GX: eemmm... laughs, the connectivity is not good here I mean.. I mean "sigh-mengeluh" ...AZ: so there is a problem in technology... GX: for example... we are having conferencing and we want to send a big file.. try sending a 3Meg file or whatever u know.. over your video conferencing.. it doesn't get delivered... until your conference.. well you know guys.. you know what faxing will be better... you know.. This are the challenges that we face and I believe the speed that we have here is just something that is really unacceptable.</i>	I5_NZA-GX Row: 26-30	
			physical tools	<i>GX: and CCTV to monitor the server room, make sure who goes in and who goes out</i>	I5_NZA-GX Row: 130	

ISSM Maturity: Qualitative Analysis Table

			<p>HS: ...you have to really use proper tools, proper expertise. The tools i use was quite new at the time but by time it gets old because the scammers know how to avoid, verification steps, they came out with new technologies iPhone, proxyIP</p>	I2_HS-TB Row: 254
			<p>SS: ...not just rely on SSL but we call it hash signature. Hash signature actually when we transact the data from our server o the gateway provider those are actually controlled by set of code, special code and it means that whoever hackers cannot hijack the transaction because it is already encrypted, that's another layer and another part is actually the firewall in the server. That more physical type of control. We rely on that kind of environment</p>	I4_MD-SS Row: 8
			<p>SS: that is the reason why we rely on third party server, because they have complete set of security..firewall..bla..bla.. their own.. that is why we don't have it here. Definitely we don't have expertise to manage that</p>	I4_MD-SS Row: 124
			<p>US: ...In terms of security implementation tu, because i said mostly dah ada dalam system dier, accept mcm this SSL..usually the vendor will advise so kitaorang just follow je.</p>	I6_DL-US Row: 36
			<p>HV: no what happen here of course we have Kaspersky... anti-virus tu standard all pc have antivirus one part of security issue lah, otherwise people will hack and system compromise. Because of our system...there is another thing that we have done we host it to a third party. Third party hosting, we don't have our machine here, we don't have anything. we host it at the third party</p>	I3_AR-HV Row: 67
			<p>HV: ...then we move to this new office just move dua bulan.. tak sampai. That is part of physical security you know...you know security has many part.. physical .. then logical .. and many2 part of security.. and this is part of the physical security we want to implement.. because kat sana not save banyak kes org masuk curi computer hilang.. banyak cases,</p>	I3_AR-HV Row: 145
			<p>HV: yes.. siapa ada kunci office, tak dating siapa pegang.. so ni dalah physical security in the office, make sure fire alarm jalan.. so that is part of security</p>	I3_AR-HV Row: 161

ISSM Maturity: Qualitative Analysis Table

	<p>logical tools</p>	<p><i>GX: ...so necessarily what is recommended by consultant is something that is workable, so we work within our means, building our own network, making sure we have our own internal system security, access control, a software to manage customer database, where they cannot take customer database, and copy them you know..</i></p>	<p>I5_NZA-GX Row: 4</p>	
		<p><i>GX: I think they should start at some point.. they should start somewhere even small. Not having network in your office is not acceptable. Start there. Start by having a document control system using the Microsoft available platform access control system and all that.. Start using access database for that matter, something simple</i></p>	<p>I5_NZA-GX Row: 74</p>	
		<p><i>GX: When I first heard about it the first time, when a guy came to us.. i say ohh this is complex, but I think let's take a simple step towards it, what is it we want to control, how do we control it, and then use what available tools available by Microsoft to manage security, access control and all that was basic, then se start to have logging in, passwords, simple ones,...</i></p>	<p>I5_NZA-GX Row: 100</p>	
		<p><i>GX: ..., so if you have security management that could managed, cause you know what type of information is being pulled out and when.. cause there is audit trail to tell u what document is being pulled out...</i></p>	<p>I5_NZA-GX Row: 130</p>	
		<p><i>HV: ...system ada password dier ada org yag key in kan.. so always segregation of duities must be very clear. That is very basic about securitylaa</i></p>	<p>I3_AR-HV Row: 53</p>	
		<p><i>US: change of password maybe, even your antivirus, update your virus definitions.</i></p>	<p>I6_DL-US Row: 167</p>	
	<p>process</p>	<p><i>SS: it is not secure the payment gateway..the rely on our system, what id o actually if I pass "A" to them they will pick "A" send to visa/MasterCard then bounce back to us, so actually the thing that control, the data transcribe actually the hash signature and SSL, I say that is very minimal.. that is why we need to create a fraud detection system.</i></p>	<p>I4_MD-SS Row: 116</p>	

ISSM Maturity: Qualitative Analysis Table

			<p>HS: ... I structure a new verification flowwhat happen when the order comes in and after the order got chargeback and the chargeback result ... once i did that I pull-up an automated system, system that for the order to go through. Pass certain criteria such as IP doesn't match, phone number doesn't match, previous chargeback, credit score.</p>	I2_HS-TB Row: 17 & 19
			<p>HS: Once you go in the website everything are track. One tool used it RATE. Rate does is, you have to integrate Rate into a payment gateway. What it does is, credit card is track and check with the record, what this guy has been purchasing, how it matches, IP, the bank, and bank number to verify.... There are two phases on control, one when the order comes through.</p>	I2_HS-TB Row: 21 & 23
			<p>AZ: beside Rate, have you had any other tools you have implemented over the web HS: have you heard social engineering? You create a fake identity for a purpose. You create fake identity to verify customer over the web. I do that all the time</p>	I2_HS-TB Row: 49-50
			<p>HS: Verification, yes very crucial</p>	I2_HS-TB Row: 27
			<p>HS:...Other business, they have to configure their own verification flow. And it is not easy to do that. If you ask me 1 year time. It took the company 1 year and a half to do that</p>	I2_HS-TB Row: 45
			<p>HS:...verification for customers is very important, they might not see the return at the same time, but by time they will not that is important. Don't really ignore security</p>	I2_HS-TB Row: 335
			<p>AZ: when you do/ implement verification flow, what actually makes you want to implement it, what drives you to do it?.... HS: to reduce fraud rate.</p>	I2_HS-TB Row: 56-57
			<p>KY: registered verified users...: so now we can track their payment and we can track their what they paid for and what not paid for,so we don't do it by ourself we work with a partner he is already verified and that eliminates a lot of our security concerns.</p>	I1_KY-SW Row: 76 & 78

ISSM Maturity: Qualitative Analysis Table

		<p>AZ: ...charge back yg bila org to dah bayar saylah dier beli 2 package dier bayar lepas tuh dier kata satu tak jadi..charge back to my credit card... HV: we have not happen before laa.. because very clear we are very clear.. when people ask for something , one thing that is very important is that we always send a quote, quotation issue will list amount you have to pay, what the item we charge you and the you sign on it, to indicate your acceptance or confirmation... AZ: so ada flow lahh</p>	<p>I3_AR-HV Row: 60-62</p>
non-technological	education-formal training	<p>AZ: education and knowledge is important... SS: yes.</p>	<p>I4_MD-SS Row:75-76</p>
		<p>HV: ...towards on how people understand it especially staff understanding security... AZ: ada grudge tak, mcm lecehlah susah lah buat nih HV: no takde... now tak de..</p>	<p>I3_AR-HV Row: 181-183</p>
		<p>AZ: how about having competence staff and training and awareness is it important for the business... HS: yes of course. You have to keep on sending , keep finding new field to venture in new technology to venture in and upgrade your staff just like how you upgrade your system</p>	<p>I2_HS-TB Row: 332-333</p>
		<p>AHS:...free tools banyak tapi orang tak tahu sebab takde education. Kalau dier nak buat I rasa education is the best. Tools banyak.. u nak free ada murah ada..mahal ada... Apa-apa basic tools... semua ada tinggal issuenya education</p>	<p>I7_AHS-PTS Row: 179</p>
		<p>AHS: As owner.. I know it is important. But as an owner you know how much you want to put into it. Because i think our need and requirement right now is consider quite small.</p>	<p>I7_AHS-PTS Row: 227</p>
		<p>AHS: ...: I rasa user education, contoh macam email system pejabatkan.. kita org google app. Kan, nak buat apa beli Microsoft exchange yang mahal2 tuh kan free</p>	<p>I7_AHS-PTS Row: 63</p>
		<p>AHS: Education is the best...</p>	<p>I7_AHS-PTS Row: 145</p>
		<p>US: of course training... but then again online pun banyak</p>	<p>I6_DL-US Row: 267</p>

ISSM Maturity: Qualitative Analysis Table

		<p><i>SS: well actually it looks complex but we simplify, that is our advantage laa.. because when we understand the subject , then we know how to solve in simple way.</i></p>	<p>I4_MD-SS Row: 74</p>
		<p><i>SS: ...so base on the knowledge and understanding and needs then you can do that, so that basic is good to give overall understanding</i></p>	<p>I4_MD-SS Row: 168</p>
education-informal (experience)		<p><i>KY: I guess it's ongoing process. I guess the first years it took was for us to really get business, that when we don't consider anything. The second year... we are in business for two year now.. the second year is when we start improving existing process.</i></p>	<p>I1_KY-SW Row: 114</p>
		<p><i>HS: it doesn't borders me and it is complex, there's a lot of experience you need from my.. i don't say i am experience but from what i'm knowledgeable in is investigating the cases thats why.. and the flow i've implemented was from my own experience and i spend about more than two years to tweak on every single steps of the flow so it could fits the .. you have to make it user easier and make us easier..... Over time when you see that this steps works you add in new product adding new product.. you see how it goes? So you have to go with a flow... you have to go with the technology.</i></p>	<p>I2_HS-TB Row: 119</p>
		<p><i>HS: Sometime it does not come to you right away.. it take few days to analyse the data, there a bunch of data there, so once you know the pattern of it, you have to make changes to you flow. It took a lot of time to do it but yes you have. ...when you see the sale is increasing charge back is decreasing you can see that is the correct way, just try an error laa</i></p>	<p>I2_HS-TB Row: 303 and 305</p>
		<p><i>US: for us.. sebab kita dah buat bende nih for almost 10years, with US kitaorang startkan.. so there are alot of things we learnt along the way.</i></p>	<p>I6_DL-US Row: 197</p>
		<p><i>AHS: kalau u nak cakap in any type dari day one dah ada dah, the very basiclah .. securing PC.. antivirus apa semua itu dari dayone dah ada kita</i></p>	<p>I7_AHS-PTS Row: 385</p>

ISSM Maturity: Qualitative Analysis Table

			<p>SS: it is quite some times because we do not have full concentration because when we have some free time we do it. Previously we provide solution for our customers on e-commerce hotel booking and some other site.</p>	I4_MD-SS Row: 42
			<p>HV: yeas, it is not susah, because i already in this area for many2 year you know to implement it easylah ,</p>	I3_AR-HV Row: 39
			<p>AZ: senang tak nak implement security, is it for you to have all these done.... HV: no to me easylah.. maybe because i have 20 years. So no big deal at all... AZ: so basically or you.. saylah you don't have this security back ground... HV: could be tough, could be i don't understand what this is all about</p>	I3_AR-HV Row: 124-127
		education-informal (understanding/a wareness)	<p>HV: back to the basic.. if you want to do e-commerce then you perlu buat... kalau u nak buat mcm biasa buat dtg office than up to youlah.. tapi if u want to be competitive.. your market is not Malaysia, the you have to do it.. if you need to do global.. u need to do e-commerce....if you want to do e-commerce you need to have securitylaa.. that is important.</p>	I3_AR-HV Row: 219
			<p>HV: easy because we don't burden ourself with the issue we burden the hosting company</p>	I3_AR-HV Row: 185
			<p>AZ: ... and one of the issue yg dier cakap lecehlaa.. complex sgt security ni... HV: because diorang tak paham... dia tak paham to me thats a key advantage you know, kalau org confident dgn kita punya website, the more people will come that basically....</p>	I3_AR-HV Row: 136-137
			<p>HV: ...how people understand it especially staff understanding security... AZ: ada grudge tak, mcm lecehlah susah lah buat nih... HV: no takde... now tak de.. dulu2 maybe.. younger people tak kisah.. sepuluh password pun tak pe.. inin ada password itu ada password.. it is not any issue already</p>	I3_AR-HV Row: 181-183
			<p>AZ: is it because mentality that you know.. not implementing security management.. not using it not adopting it... GX: I think it is AZ: or is it because of lack of training... GX: awareness... and also because IT people seem to make it complex.</p>	I5_NZA-GX Row: 17-20

ISSM Maturity: Qualitative Analysis Table

		<p>AZ: how about having competence staff and training and awareness is it important for the business... HS: yes of course. You have to keep on sending , keep finding new field to venture in new technology to venture in and upgrade your staff just like how you upgrade your system</p>	<p>I2_HS-TB Row: 332-333</p>
		<p>PTS: ...Apa yang diaornag boleh buat on their own yang no cost.. maksudnyer mcm harderning the hosting punya,haa itu dierorang buat sendirilah, tak perlu cakap2.. dierornag buat jek.. itu no cost kan...kalau nak ada cost.. then kene wait for que lahhh, kalau tak senang je dier ornog buat sendiri..</p>	<p>17_AHS-PTS Row: 311</p>
		<p>AZ: ...problem with awareness, scare to use technology, why is that,... GX: I think.. exposure... exposure</p>	<p>15_NZA-GX Row: 21-22</p>
	staff/ PIC/ expertise	<p>AHS: security implementation.. kalau nak kirer laaa, i tak Nampak budget kat soal software ke kat apa sangatlah. Banyak tools dah ada.. issue nyer technical expertise jek.. banyak tools2 tuh kita nak run.</p>	<p>17_AHS-PTS Row: 463</p>
		<p>AZ: so itu jerlah yang penting sekarang nih... AHS: I Nampak man power and expertise laaa. I Nampak tools tu banyak yang free. Banyak opensource punya tools.. how good we are with this tools haa.. technical issues</p>	<p>17_AHS-PTS Row: 464-465</p>
		<p>AZ: [waiting] kalau ada expertise, ada PIC pun tak guna yeh... AHS: You cannot pay for that kind of PIC. I bagi tahu you.. ni yang kita punya teknologi kita punya nih. Orang yang memang buat development, IT support semua2 nih.. our so call IT department dua tiga empat orang nih. Their salary average is much higher than staff2 yang lain</p>	<p>17_AHS-PTS Row: 200-201</p>
		<p>AZ: who actually takes care of security in the company... SS: our own staff... AZ: so you basically have a particular person to look into this...SS: yes... we have our dedicated IT</p>	<p>14_MD-SS Row: 19-22</p>
		<p>HS: ...because you really have to find suitable person to handle this. It is really not easy to find someone...AZ: so you are talking about increase of resources here HS: yes and about strength... you have to really use proper tools, proper expertise.</p>	<p>I2_HS-TB Row: 252-254</p>

ISSM Maturity: Qualitative Analysis Table

			<p>AZ: so you think e-commerce also even though it is a small e-commerce you have to have point of contact for particular implementation or what we call security implementation... HS: yes correct , yes for security implementation, you need a proper person to handle this</p>	I2_HS-TB Row: 192-193	
			<p>SS: that is the reason why we rely on third party server, because they have complete set of security..firewall..bla..bla.. their own.. that is why we don't have it here. Definitely we don't have expertise to manage that</p>	I4_MD-SS Row: 124	
			<p>KY: They are knowledgeable in implementing any web based requirement whether it is security or another feature.....So we define the requirement, and they build it so its quite simple, I need to tell them what to do they do it laaa.... but I don't know how to do it laaa...they will figure it outlaa..</p>	I1_KY-SW Row: 94 and 96	
		standards and policy	<p>AZ: don't you thing when you have a business policies, procedures it will actually help you do.. ok this is how you do your work, in a way.. when we call simplify....AHS: betullah...</p>	I7_AHS-PTS Row: 232-233	
			<p>HV: in the tourism sector to me e-commerce to me is crucial to have security policy in placelaa simple because it involve payment , involve transactional services...</p>	I3_AR-HV Row: 47	
			<p>AZ: ...do you think that will help tak kalau ada security policy ... US: at this point, not really, at this point... tak because kita tak de banyak2 branch lagi kan. It is just here</p>	I6_DL-US Row: 9-10	
			<p>GX: We tried to implement a little bit of ISO 27001. Things that we saw that could be implemented, simple things.</p>	I5_NZA-GX Row: 130	
			<p>AZ: but do you think now it is important for you to base (refer to standards)... HS: yess.. you have guidance, you have assistance .. you should really appreciate it and use it because it will help you a lot</p>	I2_HS-TB Row: 200-201	
			<p>AZ: you rasa penting tak standard or procedure... SS: SOP yes...but it really play a big role if you work with biz staff.. kalau u small few people, then.. normally is not in writing basislaaa..more informal they understand what they should do..</p>	I4_MD-SS Row: 151-152	

ISSM Maturity: Qualitative Analysis Table

3	Technology Security management	assurance	lower and predict risk	<p>SS: ... so we have to use that detection system to manage that to minimise the risk</p>	I4_MD-SS Row: 32		
				<p>SS: ...It is not just protecting money transactions but also need to protect the user profiles</p>	I4_MD-SS Row: 6		
				<p>HS: but there is one thing you have to think.. you can't really kill it but, .. you can really kill it... but you can reduce it that's the fact.</p>	I2_HS-TB Row: 309		
				<p>HS: once you know how the thing goes you can almost predict how fraud coming in.</p>	I2_HS-TB Row: 143		
		proper work assignment	<p>HV: So that is the basic of security you know...because we difine security is a crucial issue so we know who is responsible for what, and who is supposed to do what , so we have to assign that properly...</p>	I3_AR-HV Row: 51			
			<p>HV: ...security means is a good definition of "who do what- who received what" because you wnat to be secure right.. you must know.. mcm kit punya pintu rumah laaa kalau nak jaga security rumah kita tahu siapa pegang kunci, who is responsible for that.</p>	I3_AR-HV Row: 51			
		categories / types	copyright issues	<p>AZ: problemnya bila expand tuh some of the problem mcm nih lah...the copyright issue come in... AHS: of course, mau tak mahu kita terpaksa laa...</p>	I7_AHS-PTS Row: 102-103		
				redundancy and data backups	<p>US: we do backups, the hosting itself buat back up, but on our side, my partner, my husband laa will do periodic backups. On that server so we have a mini server at home so they call, so we can have the latest one.</p>	I6_DL-US Row: 98	
					<p>HV: ...segregation of hosting... that is very importa.. the security part is is that we can stil operate in the event of something happen.. so sytem masih secure</p>	I3_AR-HV Row: 69	
					<p>AHS: ...Sekarang data lost is one big area we are worried now.</p>	I7_AHS-PTS Row: 247	
<p>AHS:masalah backup tak buat. So our focus this yeah is to setup up a so-call central storage punya server untuk, the idea is to back up everythinglah in this company.</p>	I7_AHS-PTS Row: 253						

ISSM Maturity: Qualitative Analysis Table

		availability	<p>GX: ...And I know that.. it gives me that comfort... AZ: meaning there is availability.. with security there is availability... GX: yeah...</p> <p>HV: haa.. pentinglaa, when you do business you cannot be down all the time</p> <p>HV: yahh, system secure, system reliable and availability is always there</p> <p>HV: cannot the system cannot down thats all, mesti ada.. 24x7</p>	<p>I5_NZA-GX Row: 54-56</p> <p>I3_AR-HV Row: 71</p> <p>I3_AR-HV Row: 79</p> <p>I3_AR-HV Row: 89</p>	
		data confidentiality	AZ:Data confidentiality dah sebut tadi.. do you think it is important tak for the website to be available always... US: yes..	I6_DL-US Row: 83-84	
		segregation of duties	HV: ...so always segregation of duties must be very clear. That is very basic about securitylaa	I3_AR-HV Row: 53	
		audit trail	HV: who is responsible for what, anything happen we know who to findlaa	I3_AR-HV Row: 55	
	perceptions	business and users	<p>AZ: ...does security implementation a trend, a fashion... SS: not that so.. security is a serious thing...trend is not so serious... trend is thing that capture your attention mcm fashion.</p> <p>AZ: ...do u thing implementing security management is a waste of money and time... SS: not.. not at all... no.. no.. yeah a simple one cost you few hundreds, but is ia a year.. you can compare and calculate how many ringgit per day only. But interms of the function that it give you .. takboleh ternilailah</p> <p>AHS: trend.. kalau applicable.. kita guna lah.. kalau tak takdelahh. I rasalahkalau nak jadi first on the block is not the priority now lahhh, we want to be maybe the.. maybe the first pergi.. dah make all the mistakes apa semua.. and then baru kita follow.</p> <p>AZ: mcm mana dengan risk? It influence you tak?... will that push you... influence you implement security managment... AHS: I rasa risk yang boleh menyebabkan kita cepat bila kita boleh quantify bila besar mana hilang, mcm data lost kita boleh quantify</p>	<p>I4_MD-SS Row: 59-60</p> <p>I4_MD-SS Row: 193-194 and 196</p> <p>I7_AHS-PTS Row: 285</p> <p>I7_AHS-PTS Row: 294-295</p>	

ISSM Maturity: Qualitative Analysis Table

				<p>AHS: ...kalau nak cakap pasal security is that...kalau nak cakap what is important they will tell you what is the most painful now. Painful mcm hilang data.. buku takleh keluar. They will put money onto that first.</p>	<p>I7_AHS-PTS Row: 269</p>
				<p>HS: It doesn't take a long time there are few phases, you have to take one by one to put it and not all businesses can use the same flow.</p>	<p>I2_HS-TB Row: 45</p>
				<p>AZ: do you think it is a waste of money for the small e-commerce to implement security, do you think it is a waste of money to come up with a flow to track?... HS: No it is not a waste of money...</p>	<p>I2_HS-TB Row: 34-35</p>
				<p>AZ: do you thing implementing security is wasting of money and time... HV: not it is not wasting of money and time.. for me it is a must.. i don't know other business. Like internet banking.. u have to do it.. you have to spend money.</p>	<p>I3_AR-HV Row: 212-213</p>
				<p>AZ: so you impement security tools procedure nih bukan lah sebab trend, bukan ikut orng bukanlah yehh... HV: no nothing to do with that</p>	<p>I3_AR-HV Row: 80-81</p>
				<p>US: i think for e-commerce it is quite a standard feature.. ya sooo. We implement that because for the admin part we want it to be secure sbb kita tak nak org ganggu kan..</p>	<p>I6_DL-US Row: 28</p>
				<p>AZ:do you think implemnetatoion of Security management is a waste of money and awaste of time for you and your business?... US: emmm no i think, you have to start it right laaa, because what we learn before was it effect you when it happens...</p>	<p>I6_DL-US Row: 264</p>
				<p>US: emmmmm, if there is a breach in security, then it will affect your productivity and your business, so how I see it, you need to invest some time before you implement (security)....</p>	<p>I6_DL-US Row: 264</p>
				<p>KY: as i said its insurance, you are putting your investment now so that in case something happens in future you are prepared to handle it</p>	<p>I1_KY-SW Row: 86</p>
				<p>KY: ...I think in certain industry you can consider it (security management) to be an investment not an insurance. In my industry however, it is an insurance</p>	<p>I1_KY-SW Row: 158</p>

ISSM Maturity: Qualitative Analysis Table

			<p><i>KY: I, for me, for us lah security is always a cost center. It is insurance, you're putting in money in the off charge and someday someone will scam you and you are then prepared.</i></p>	<p>I1_KY-SW Row: 54</p>
			<p><i>KY: I think is very hard to find, security management, I think, how and what I think about security is overhead. Is an additional process which is not necessary unless something bad happens. That is how I think about it simply, so it is a cost center. So it is a very very difficult task to trying to make sure that cost center, cost comes in terms of money, time and at the cost of my users convenience. If he has to jump through one hoop to complete its transaction than that is trouble to my users. And it is very hard to be able to cut all this down and yet have a level of security.</i></p>	<p>I1_KY-SW Row: 60</p>
			<p><i>AZ: ...When you implement security management, do you think about what kind of risk you will face before you implement it... GX: yeah.. I do, first thing is that .. what happen if it becomes obsolete, what if the choice I make become obsolete...(laughs) we just have to live with it.. you know, we evaluate.. well if it is time to become obsolete.. well it is time to reinvest</i></p>	<p>I5_NZA-GX Row: 123-124 and 126</p>
			<p><i>GX: ..., but unfortunately when people look at ITSM (security management), they think that it is an expensive thinglaa. Maybe because of the image that has been projected</i></p>	<p>I5_NZA-GX Row: 4</p>
			<p><i>GX: ...then I realize that when I have this connected, with a certain security system, those guy can connect I can see what are connecting to and I know what they are doing and this are being monitored. But that takes a lot of investment, so that is the issue we are struggling right now.</i></p>	<p>I5_NZA-GX Row: 88</p>
			<p><i>GX: When I first heard about it the first time, when a guy came to us.. i say ohh this is complex</i></p>	<p>I5_NZA-GX Row: 100</p>
			<p><i>GX: ...So this need of constantly putting IT (security management) as complex, i think is a culture that we have, that we haven't break through.</i></p>	<p>I5_NZA-GX Row: 20</p>

ISSM Maturity: Qualitative Analysis Table

			<p>AZ: when u implement any security tools and procedures in your business, do you find it challenging, do you find it wasting your time.. do you find it lengthy... GX: it's costly... AZ: not so much about time?... GX: because we hire a person to do that</p>	<p>I5_NZA-GX Row: 45-48</p>
			<p>GX: so I think it is about exposure and the age gap.. where we were not introduce to that. So when they want to adopt that it become difficult.</p>	<p>I5_NZA-GX Row: 22</p>
4	Environment	3rd parties	<p>SS: that is the reason why we rely on third party server, because they have complete set of security..firewall..bla..bla.. their own.. that is why we don't have it here. Definitely we don't have expertise to manage that</p>	<p>I4_MD-SS Row: 124</p>
			<p>HV: ...we host it at the third party so the third party is quite a big corporate a reliable company laa to make sure.. there is two part.. one of the thing is the website you see is also in the third party and another thing.. our email is also hosted in another third party. Two different hosting. The reason is that, one of the fundamental of security is to prevent system failure</p>	<p>I3_AR-HV Row: 69</p>
			<p>HV: so actually the standards and policy like ISO and so on tuh.. our hosting company should have thatlaa.. they are big organization.. they are certified hosting company.. they should have this to ensure the physical security of the computer system..all the things.. it should be there laaa. So all of them has implement security within themselves you know, now I am not going to invent a new one, so what I have is security procedure within the administration office , that's all, the physical security, the technical security is all implemented by the service provider, we don't spent time on that one</p>	<p>I3_AR-HV Row: 159</p>
			<p>SS: actually setup.. and comprehensive testing.. a month.. we can finish in one two day... reason why we try to get true experience by testing on daily basis. The implementation by SSL is simple. The job is done by our server operator.. they have to put in codes. For us we just have to actually make sure everything is in order, then we do the testing based on our preferred method</p>	<p>I6_DL-US Row: 110</p>

ISSM Maturity: Qualitative Analysis Table

				<p>AHS: ...Maksundryer the third party who will provide us the services, will have to provide us the security sendiri, as much as possible I tak nak buat in-house.. sebab I takde experts, tak de experts kat dalam</p>	<p>17_AHS-PTS Row: 227</p>
				<p>GX: ...You got to work on the good people you have and outsource the services to them. And we have done this and our business it all about that and we manage to run revenue worth of 4Million in less than 10 people in our company</p>	<p>15_NZA-GX Row: 8</p>
				<p>GX: ...we work with freelancers who actually manage our website and make sure that the online payment services are actually done</p>	<p>15_NZA-GX Row: 4</p>
				<p>GX: ...so I have to hire a vendor.. so when you hire a vendor , your cost is very expensive. On the retainer fee will be expensive and if you decide not to have a retainer fee with the company, than you have to hire someone... that will be a capital cost for you, so at the end of the day we have evaluated options, and we find that outsourcing to a person outside where we have a contract of what they can do and cannot do, and then that is more cost effective...</p>	<p>15_NZA-GX Row: 6</p>
				<p>AHS: outsource memang issue.. usually stick to reputatble vendor, reputable platform...</p>	<p>17_AHS-PTS Row: 479</p>
				<p>AHS: secure.. lebih baik you outsource yang ada orang nak tengok dari inhouse yang incompetent</p>	<p>17_AHS-PTS Row: 485</p>
				<p>AHS: e-commerce we basically outsource</p>	<p>17_AHS-PTS Row: 245</p>
				<p>AHS: ..tapi advance level punya knowledge (of security) must outsource. Sebab imposible.. kalau you ada this kind of people dalam company, thank you very much.. memang baguslah nasib u baiklah kan...</p>	<p>17_AHS-PTS Row: 425</p>
				<p>AHS: common SMI, i rasa approach yang kene fikir is macam tadi, outsource security...sebab u tahu fundemantelly you tak boleh nak buat kat dalam company, can you afford to hire...“gaji berapa ribu?”</p>	<p>17_AHS-PTS Row: 423</p>

ISSM Maturity: Qualitative Analysis Table

				<p>AHS: betul... faham yeh, okk their is their core, so company like SMI probably yes.. probably not depending on the business. Katalah company mcm kita orang terbit buku..., yang buat tayar.. apa2 semua kan.. probably not, lebih baik outsourcekan kepada competent third party daripada dier buat kat dalam...</p> <p>AHS: then you terpaksa tengok service level agreement dengan dier orang lah...security websitelah they will pay you you security lah. Hosting.. hosting punya securitylah.. payment gateway, payment gateway security luarlah, you jangan buat sendiri, mcm I punya email systemkan.. google kan.. googlelah provide security</p>	<p>17_AHS-PTS Row: 431</p> <p>17_AHS-PTS Row: 205</p>
		open source and cloud computing		<p>GX: ...and then use what available tools available by Microsoft to manage security, access control and all that was basic, then se start to have logging in, passwords, simple ones, yeah when we talk about IS security.. why do we have to go to that level...</p> <p>AHS: apa tools lah kalau kirerlah kan... tools ka nada banyak kat luar sana, free tools banyak...Tools banyak.. u nak free ada murah ada..mahal ada.. apa.. apa basic tools... semua ada...</p> <p>AHS: I nampak tools tu banyak yang free. Banyak opensource punya tools.. how good we are with this tools haa.. technical issues</p> <p>AHS: ...Kalau boleh mcm cloud kan.. kalau boleh kita memang shiftout to cloud computing</p>	<p>15_NZA-GX Row: 100</p> <p>17_AHS-PTS Row: 179</p> <p>17_AHS-PTS Row: 465</p> <p>17_AHS-PTS Row: 479</p>
5	Environment government	support systems	<p>context-focused campaign</p> <p>smart partnership</p>	<p>HS: ...if they can only allocate or put one of their campaign or talk as security for e-commerce, I am sure will turn up...</p> <p>AHS: ...partner with this technology company, mintak dier orang support Malaysia.</p> <p>AZ: what you have to do buat joint-venture...AHS: buat smart partnership</p>	<p>12_HS-TB Row: 97</p> <p>17_AHS-PTS Row: 145</p> <p>17_AHS-PTS Row: 150-151</p>

ISSM Maturity: Qualitative Analysis Table

		soft loans	<p>GX: yeahh.. i mean.. you know.. let say the government say there is abuse of people taking grant and all that, well, just tell us that this is the appointed whatever.. university of whoever, that will come and implement this for us, prioritize the company that you believe could benefit from it...</p> <p>AHS: ...kalau kerajaan nak membantu, tak usah dari segi bagi grant sgt...I rasa the days of grant is over already. Grant day is over... Soft loan is good.</p>	<p>I5_NZA-GX Row: 52</p> <p>I7_AHS-PTS Row: 145</p>
		critical business context	<p>GX:because their return on the capital investment going to be slow and it is gonna be long term, so that support system is not correct here in Malaysia. We got to correct that first. Because I find that, you know we have grants and we have all this but every time we apply for it we don't qualify for that, you don't qualify for this.. and this ok.. we are not start-up.. you know you have all this grants for start-up.. but we are not start-up. Companies like me.. we are 8 years in business.. what are we? We are at growth stage.. so is the government prepared to deal with the growth of SME. You ask yourself why is our SME is not going outside. Ask again.. is the support system is good enough to support us to go outside?</p> <p>GX: ...But if you look at all the government grants financing that are being given out to companies, they have not tailored themselves to the service industries.</p>	<p>I5_NZA-GX Row: 62</p> <p>I5_NZA-GX Row: 80</p>
	legislation and guideline	mandatory/directive	<p>SS: it think it is good.. actually when government saya implement security.. it does not say to protect you but to protect the users, most of the regulation is to protect general public. It is good to have that. It will become standard implementation</p> <p>AZ: it is good ada directive dari government.. a clear directive will be good... SS: yes.. yes</p> <p>US: it has to be done to the vendors.. meaning if i were to give licenses for somebody to setup a website, the government has to have to make sure that your security systems mcm ni in the hosting...That guideline has to be imposed on the vendors.</p>	<p>I4_MD-SS Row: 146</p> <p>I4_MD-SS Row: 147-148</p> <p>I6_DL-US Row: 203</p>

ISSM Maturity: Qualitative Analysis Table

				<p>AZ: anything.. anything that you can think of, tak kirer lah model ker. Dosest have to be a physical tool. Doesn't have to be a technological tool. It can be just a procedure wise, it can be just a frame work model or anything.. do you see a need for that... US: I see a need for that, like i said based on the maturity of the company. Because security is important. I realized that Cuma depending on the level of the company punya resources dier focus dier.. tu semualah kan. So if you have the tool it should be based on certain number of website ker network ker, but if you have standards that people can use, to assess their security level, it would be good laa...</p>	I6_DL-US Row: 160-161
			monitoring system	<p>US: ...if there is no guideline...or there is no one monitor this people to do the right way of e-commerce business it can be very dangerouslaa, because people are sharing information freely in the internet, so i don't know how.. is there a way to monitor... to guide..</p>	I6_DL-US Row: 269
		readiness	expertise	<p>HS: They don't have the expertise</p>	I2_HS-TB Row: 87
				<p>HS: Correct. They don't have the man power, no resources and they don't take the initiative.</p>	I2_HS-TB Row: 11
			transparent	<p>GX: yeahh.. i mean.. you know.. let say the government say there is abuse of people taking grant and all that, well, just tell us that this is the appointed whatever.. university of whoever, that will come and implement this for us, prioritize the company that you believe could benefit from it ...</p>	I5_NZA-GX Row: 52
			technology savvy	<p>AHS: ...jangan buat bende bodoh yang menyekat kemajuan lah</p>	I7_AHS-PTS Row: 179
6	Environment technology vendor	support systems		<p>AZ: alright, so it was not influence by your users, it was not influence by anyone but... US: technology..</p>	I6_DL-US Row: 264
				<p>KY: eemm.. cybersecurity has a grants ...they are paying for consultant to look through, so they are experts and they kind of look at where we are weak, so we have applied for that and we will be call for interview.. I don't know whether I will get it, but they will advise us what to be done.</p>	I1_KY-SW Row: 128

ISSM Maturity: Qualitative Analysis Table

				<p>SS: I think like software providers could be yes... because they provide most of the solution and experience, SSL and all those come from them...</p>	<p>I4_MD-SS Row: 84</p>
				<p>GX: I think.. exposure...exposure...so because of that readiness is not being prepared, I think the environment here are not there...So I thing it is more on the environment that we have, has not encourage us to that level...</p>	<p>I5_NZA-GX Row: 22</p>
				<p>HS: No. When I was in off (office) u I don't care what users want, I just think about the company profit</p>	<p>I2_HS-TB Row: 143</p>
				<p>AHS: commercial force jek boleh and then technology...</p>	<p>I7_AHS-PTS Row: 165</p>
				<p>AHS: kecuali vendor mula buka mata, yang memang to go to or appoint SME/SMI punya market.</p>	<p>I7_AHS-PTS Row: 29</p>
				<p>AHS: I think you have to start daripada.. daripada manufacturer...bila manufacturer dah appoint reseller yang focus.. baru boleh jalan.. kalau tak takdak</p>	<p>I7_AHS-PTS Row: 39</p>
				<p>AHS: supplier tak sangatlah.. mcam i cakap kat u lah, supplier don't really support SMI lah kita banyak self-support i rasa banyak, you banyak look for forum ker apa kan... dalam internetlah self-support lah</p>	<p>I7_AHS-PTS Row: 407</p>
				<p>AHS: bgi diaorang SME nih kecil sangat, budget pun kecil margin pun small, we always go with the cheapest...</p>	<p>I7_AHS-PTS Row: 13</p>
7	Environment	influence		<p>AZ: ...like your particular company your users.. what do you call them gamers, this particular people by stuff, does all these users influence you implement a security tools or not. Do they have a lot of influence... HS: they do influence us...</p>	<p>I2_HS-TB Row: 328-329</p>
	User			<p>AZ: ...ok so did you get any support from anyone.. mcm u cakap tadi takde support.. from the government... tak yeehh.. ok, third party consultants.. other than hosting companieslaa...macam hosting company mmg tolong you because you actually buy from them... HV: takde...</p>	<p>I3_AR-HV Row: 156-157</p>

ISSM Maturity: Qualitative Analysis Table

8	Technology SM diffusion	relative advantage	simplify job task	<i>AZ: Do you believe, when you come up with this security flow, does it simplify your work, does it simplify?... HS: oh yes, from the fraud investigator yes, it makes it easier and faster...</i>	I2_HS-TB Row: 40-41
				<i>AZ: do you believe that when you implement security management it will simplify your business process, do you believe it will help u or not... SS: definitely...</i>	I4_MD-SS Row: 13-14
				<i>AZ: And these are effective using security management... GX: yeah.. we make decision.. some of the..you will be surprise...</i>	I5_NZA-GX Row: 15-16
				<i>AZ: ...Do you believe that security management can simplify your bsiness, in terms of running business every day?... GX: yeah of course, because we get export business through just our website and we deal with our partners overseas...</i>	I5_NZA-GX Row: 13-14
				<i>AZ: basically it will simplify your business because you know who takes care of what...HV: who is responsible for what, anything happen we know who to findlaaa...</i>	I3_AR-HV Row: 54-55
				<i>AZ: ...do you believe that security management can simplify your job every day tak?... HV: it should be...</i>	I3_AR-HV Row: 50-51
	enhance business- ROI/ business	<i>US: so I rasa, if you are at that point that you have customers, you are collecting customers information.. then i think you need, it is important to have... But ours dier punya alamat ada, email.. so the detail that you do not want other people to access then you need. Is important.</i>	I6_DL-US Row: 66		
		<i>AHS: dier kan semua nih (referring to security mangament question) is good and nicelah..</i>	I7_AHS-PTS Row: 87		
		<i>AHS: that is important kalau tak mahal sangat, kalau mahal sngat kita pun we stick with tried and true jeklah.. atau pun yang lebih reasonable. Nak carik yang advanve sangat pun takde point jugak. Because we are not that complex juga...</i>	I7_AHS-PTS Row: 369		
		<i>SS: ...you understand well how security can enhance your business then you implement it</i>	I4_MD-SS Row: 60		

ISSM Maturity: Qualitative Analysis Table

			<p><i>HV: we also partner with few other big companies.. ok when you partner with this kind of people.. of course they must have the confident to work with us .. do they have the proper setup no one.. do they have a so call system .. how secure will do with them in terms of my financial risk ...2009 bulan Sembilan initially start.. our ranking is very lowlah..i think ALEXA ranking very low... bottom, within 9 months our ranking goes up so now in the world we are 600,000 ranking, from 23millin ranking last year (2009)</i></p>	<p>I3_AR-HV Row: 54-55</p>
			<p><i>AZ: so you think it is very important for them to implement this (security)... HS: yes.. it has increase the sales...</i></p>	<p>I2_HS-TB Row: 248-249</p>
			<p><i>HS: It is not easy for customer to do it (abide to security management) but we have to do that (security management). One more thing we have to take care is refund rate. We have to balance chargeback(risk) and refund rate (dissatisfactory).</i></p>	<p>I2_HS-TB Row: 43</p>
			<p><i>AZ: ...the ROI still comes in?... HS: you can see the thing comes in when you see the sale is increasing charge back is decreasing you can see that is the correct way...</i></p>	<p>I2_HS-TB Row: 304-305</p>
			<p><i>HS: not immediately but after about a year then yes.. they see a result (ROI) they are quite satisfy with it</i></p>	<p>I2_HS-TB Row: 295</p>
			<p><i>GX: I think before we implement security management we are unable to detect customers segment....But when we implemented our portal on our website we started to build a database (referring to secureimplementation of website and database)...after a while we are able to analyse.....I get competitive advantage by implementing them.</i></p>	<p>I5_NZA-GX Row: 106 and 108</p>
			<p><i>AZ: An these are effective using security management...GX: yeah.. we make decision.. So this are the flexibility I believe, if i personally feel i'm challenge with, we have to grab it and run with it.. or we will be this...eeee the company that say I can't make it, this business is no longer viable for me.</i></p>	<p>I5_NZA-GX Row: 15-16</p>

ISSM Maturity: Qualitative Analysis Table

			<p><i>GX: But investing for technology (with security management).. i find that, for your customers for retention of your customers. That customers retention measurement. Customers have place where they can go to.. they feel they are taken care of..you know.. they will stay with you...</i></p>	I5_NZA-GX Row: 72
			<p><i>AZ: so basically you think technology is important to support security management and you also think security management bring positive value to your company... GX: yeah..</i></p>	I5_NZA-GX Row: 43-44
			<p><i>AZ: right how long did you wait to get revenue out of your (secure) website?... GX: I think, we started getting enquires through just the first year, but people going in and start swiping their credit card.. it took us three years, three to four years...</i></p>	I5_NZA-GX Row: 89-90
			<p><i>GX: ...we believe that some point or rather it is a long term investment that would bring in money but we struggle with the fact that it is not bringing in money fast enough</i></p>	I5_NZA-GX Row: 54
	enhance business- users		<p><i>AZ: ok right, when you implemented this particular security flow you say, does it bring any changes to the business?... HS: yes of course, more profit, a bit spike in refund rate and I think customers believe us more. We gain customer trust and customer were legit laa...</i></p>	I2_HS-TB Row: 242-243
			<p><i>AZ: so you really have to know to deliever it to your users in terms of packages...KY: correct. And we have done that very well, it's no longer a... if you sit in the users it represent benefit...</i></p>	I1_KY-SW Row: 143-144
			<p><i>GX: it is important.. first of all you must make your customer comfortable with you and you are supporting their business...</i></p>	I5_NZA-GX Row: 146
			<p><i>SS: ...one is actually protect us and two is to protect our customers</i></p>	I4_MD-SS Row: 52
			<p><i>AZ: so basically from point of view it is important to have security implementation and IT management together with it , to make sure your business and processes are in control... GX: to satisfy your customer.. I find it... AZ: do you think it should satisfy the business also not just the customer?... GX: to me is like if it satisfy the business and my customer is not happy with it, I have done it wrongly...</i></p>	I5_NZA-GX Row: 139-142

ISSM Maturity: Qualitative Analysis Table

			<p><i>KY: ok.. what we have done.. ok we try to combine security feature, it cannot come as , it cannot be interpreted as additional security measure to the end users. In web right users interface is everything. How the users feels when they use the website is the entire experience. So we can never package our security measures as one more step. How we package is one additional feature but that is how it mask the fact that this is a security measure. ... If you put forwards security as security, your users will run away. Website dynamics is very different from any other sort of business.</i></p>	I1_KY-SW Row: 142
			<p><i>SS: ok especially we talk about SSL again.. most of IT users know what SSL is, it's a secure site.. so every time you visit the website you verify and when they use SSL. From there people know that that site is secure... It gives a positive perception because along the way they go they can verify that cert is valid or not so from there you gain confidencelaa..</i></p>	I4_MD-SS Row: 54
			<p><i>SS: ...but if you want them to go to you then you have to implement, because there are many choice.. if you don't implement why do I go shop at your website without assurance of security, I can shop somewhere else... AZ: this is like a pull factorlah...SS: that is right...</i></p>	I4_MD-SS Row: 66-68
			<p><i>HV: ...when people do transaction they feel secure, they don't lose the money and they know where the money goes to laaa, not to do with technology..what is important is people.. our customer..they are doing business with us, they feel safe they can trust you, the money is there and whatever they do is there.. some people don't trust.. because when you masuk no credit card.. boleh harap ke tak.. dier takut2.. thats should not happenlaa.. because.. when they see your system.. they feel safe, confident, you are always there..</i></p>	I3_AR-HV Row: 107
			<p><i>AZ: ...complex sgt security ni... HV: ...to me thats a key advantage you know, kalau org confident dgn kita punya website, the more people will come that basically....</i></p>	I3_AR-HV Row: 136-137

ISSM Maturity: Qualitative Analysis Table

	complexity	ease of use	<p><i>GX:... Security management means to ensure whatever information that you have internally is being controlled and managed. How do we do that.. so we know manually how we control it and convert it into IT platform and that would actually help us..</i></p>	<p>15_NZA-GX Row: 100</p>
			<p><i>AZ: so kalau nak kata security nih menyusahkan pun tak jugak... AHS: tak jugak... selagi masuk akallah, reasonable and masuk akan then it is ok</i></p>	<p>17_AHS-PTS Row: 358-359</p>
			<p><i>GX: yeah.. at some point, but then again that system have to facilitate your business.. not make your business more complicated... so that is the point that people are so afraid off that when they use technology (security management) it makes life more difficult. In actual fact fix your process first....</i></p>	<p>15_NZA-GX Row: 76</p>
			<p><i>AHS: ehh kalau yang betul2.. memang complex... depending on the setup and the size lah. Kalau big operations memang complex. Kita tengok pun kita tahu complex. Nak kata SMI punya nak kata tak complex boleh buat.. sebenarnya can be complex lah. I think it can be complex. Memang kene ada dedicated PIC...AZ: but form your point of view .. from your own opinion, you rasa security menyusahkan tak... AHS: dier i rasa kene find the balance between security dengan user convience.. kalau terlampau focus on security sampai tak jadi tak user friendly, orang takkan pakai people akan find ways to over write. So i think is about findings the balance between the security implementation.. so dua nih kene ada balance...</i></p>	<p>17_AHS-PTS Row: 355-357</p>
			<p><i>AZ: ... do you think security is a tedious thing...SS: well, if you come from IT background it is straight forward.. security, the thing is you need to understand what kind of data section of your website you need to protect. Like our website.. not all is protected.. only on certain area especially on user data, admin, transaction. Only that. It is not complex, unless you don't understand what security is all about.. what SSL can do for you, how you need to protect your website from hackers.</i></p>	<p>14_MD-SS Row: 89-90</p>

ISSM Maturity: Qualitative Analysis Table

			<p><i>US: in terms of security, eemm... for me when i chose a design it is more about ease of use for our customer and for our side. In terms of security implementation tu, because i said mostly dah ada dalam system dier, accept mcm this SSL..usually the vendor will advise so kitaorang just follow je.</i></p>	I6_DL-US Row: 36
			<p><i>AZ: from your perspective ye.. do you think implementing security management nin tedious tak? Menyusahkan tak?... US: eemmm not really. Like i say.. most of it memang. Once with the technology.. because it is part and parcel already, nak ke tak nak you have to do it...</i></p>	I6_DL-US Row: 43-44
			<p><i>KY: ok.. what we have done.. ok we try to combine security feature, it cannot come as , it cannot be interpreted as additional security measure to the end users. In web right users interface is everything. How the users feels when they use the website is the entire experience. So we can never package our security measures as one more step. How we package is one additional feature but that is how it mask the fact that this is a security measure. Why we want you to register as a user is that we want to tell you what other new event coming up that you might like to attend. So like i said that why it is not easy to implement security. If you put forwards security as security, your users will run away.</i></p>	I1_KY-SW Row: 142
	ease of implementation		<p><i>US: no it like bundle up already... so when i assign the vendor to design, it is the design and ease of use.. the security system is part of it</i></p>	I6_DL-US Row: 50
			<p><i>HV: important thing is that IS security has already mature in the IT world... bende tuh dah mature.. u can use whatever available.. no need to buy... important to implement IT... tak boleh nak beli semuanya...</i></p>	I3_AR-HV Row: 191
			<p><i>HS: It doesn't take a long time there are few phases, you have to take one by one to put it and not all businesses can use the same flow...</i></p>	I2_HS-TB Row: 45
			<p><i>SS: yes... it will give ideas on basic implementation, because sometime we do not know what are the element we need to put in, when we want to implement.. say example, talk about server.. you need to have a firewall.. everybody knows you need firewall to protect server, of course on technical part itself it has so many level...</i></p>	I4_MD-SS Row: 208

ISSM Maturity: Qualitative Analysis Table

		<p>SS: ...because security has many level, there have actually many types.. when we talk about e-commerce , we talk about protecting the website, protecting the data and protecting the transactions, those are the three key area...</p>	<p>I4_MD-SS Row: 6</p>
		<p>US: at this point, not really, at this point... tak because kita tak de banyak2 branch lagi kan. It is just here kan.. to me... mcm in terms of password, mcm our POS system we have a passwordlahh only certain people can access it, even our website un to go to the admin site pun ada password... up to that level laa. But to go mcm.. because really do not have a lot of network you know. At the moment I don't see the need for ni.. if we were to implement it, we really do see so much difference.</p>	<p>I6_DL-US Row: 10</p>
		<p>SS: ...one is actually protect us and two is to protect our customers</p>	<p>I4_MD-SS Row: 52</p>
compatibility	legacy issues	<p>AHS: I rasa macam SMI ni tak risau sgt compatibility sebab kita tak banyak legacy issues. The good thing being SMI is that you can pretty much implement.. except mcm I dah ada SAP. Haa tuh takleh sentuh. Yang tuh maksub.. walaupun rasa mcam nak buang jek nak carik dengan bende lain...</p>	<p>I7_AHS-PTS Row: 365</p>
	existing tools	<p>HV: important thing is that IS security has already mature in the IT world... bende tuh dagh mature.. u can use whatever available.. no need to buy... important to implement IT... tak boleh nak beli semuanya...</p>	<p>I3_AR-HV Row: 191</p>
		<p>GX: When I first heard about it the first time, when a guy came to us.. i say ohh this is complex, but I think let's take a simple step towards it, what is it we want to control, how do we control it, and then use what available tools available...</p>	<p>I5_NZA-GX Row: 100</p>
		<p>GX: I think they should start at some point.. they should start somewhere even small. Not having network in your office is not acceptable. Start there. Start by having a document control system using the Microsoft available platform access control system and all that... Start using access database for that matter, something simple...</p>	<p>I5_NZA-GX Row: 74</p>

ISSM Maturity: Qualitative Analysis Table

			<p>AZ: so you mean is that, that particular technology is tweak able to your system, it cannot be complex, it has to fit , right...HS: easy...</p>	<p>I2_HS-TB Row: 68-69</p>
			<p>SS: well actually it looks complex but we simplify, that is our advantage laa.. because when we understand the subject , then we know how to solve in simple way.</p>	<p>I4_MD-SS Row: 74</p>
			<p>AZ: so you basically do security management according to the technology available today right, so you go with all this new tech.. follow like tweeter and stuff... GX: that is right...</p>	<p>I5_NZA-GX Row: 127-128</p>
			<p>AHS: apa tools lah kalau kirerlah kan... tools kan ada banyak kat luar sana, free tools banyak tapi orang tak tahu sebab takde education. Kalau dier nak buat I rasa education is the best. Tools banyak.. u nak free ada murah ada..mahal ada...</p>	<p>I7_AHS-PTS Row: 179</p>
			<p>AHS: security implementation.. kalau nak kirer laaa, i tak Nampak budget kat soal software ke kat apa sangatlah. Banyak tools dah ada.. issue nyer technical expertise jek.. banyak tools2 tuh kita nak run.</p>	<p>I7_AHS-PTS Row: 463</p>
			<p>AHS: ...I Nampak tools tu banyak yang free. Banyak open source punya tools.. how good we are with this tools haa.. technical issues</p>	<p>I7_AHS-PTS Row: 465</p>

APPENDIX E

PROTOTYPE MANUAL

INFORMATION SYSTEM SECURITY (ISSM) MATURITY SMI/E: MANUAL FOR ASSESSMENT

1. System starts with the “greeting screen-hello” [Figure 1]
2. Proceed to start link to begin the ISSM Maturity assessment for the SMI/E

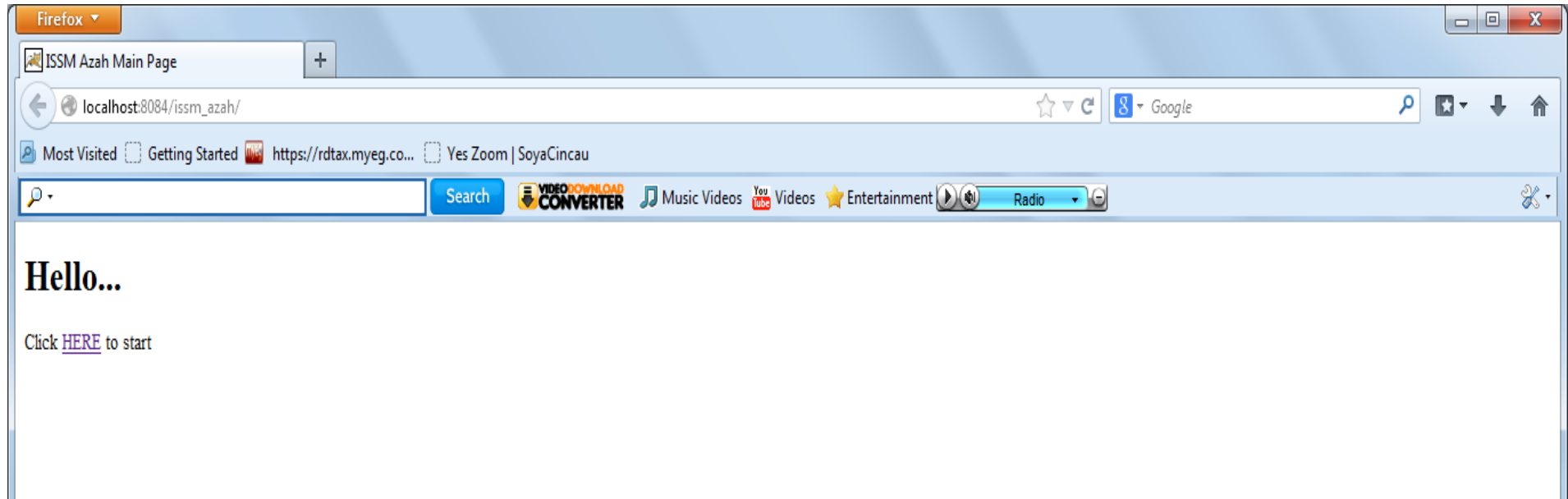


Figure 1: Greeting Screen for ISSM maturity system

3. System begins with the Business Demography information. All businesses are required to fill in all blank places before proceeding with the ISSM factors. [Figure 2]
4. The business demography is important because it is important to understand the level of business size and length.

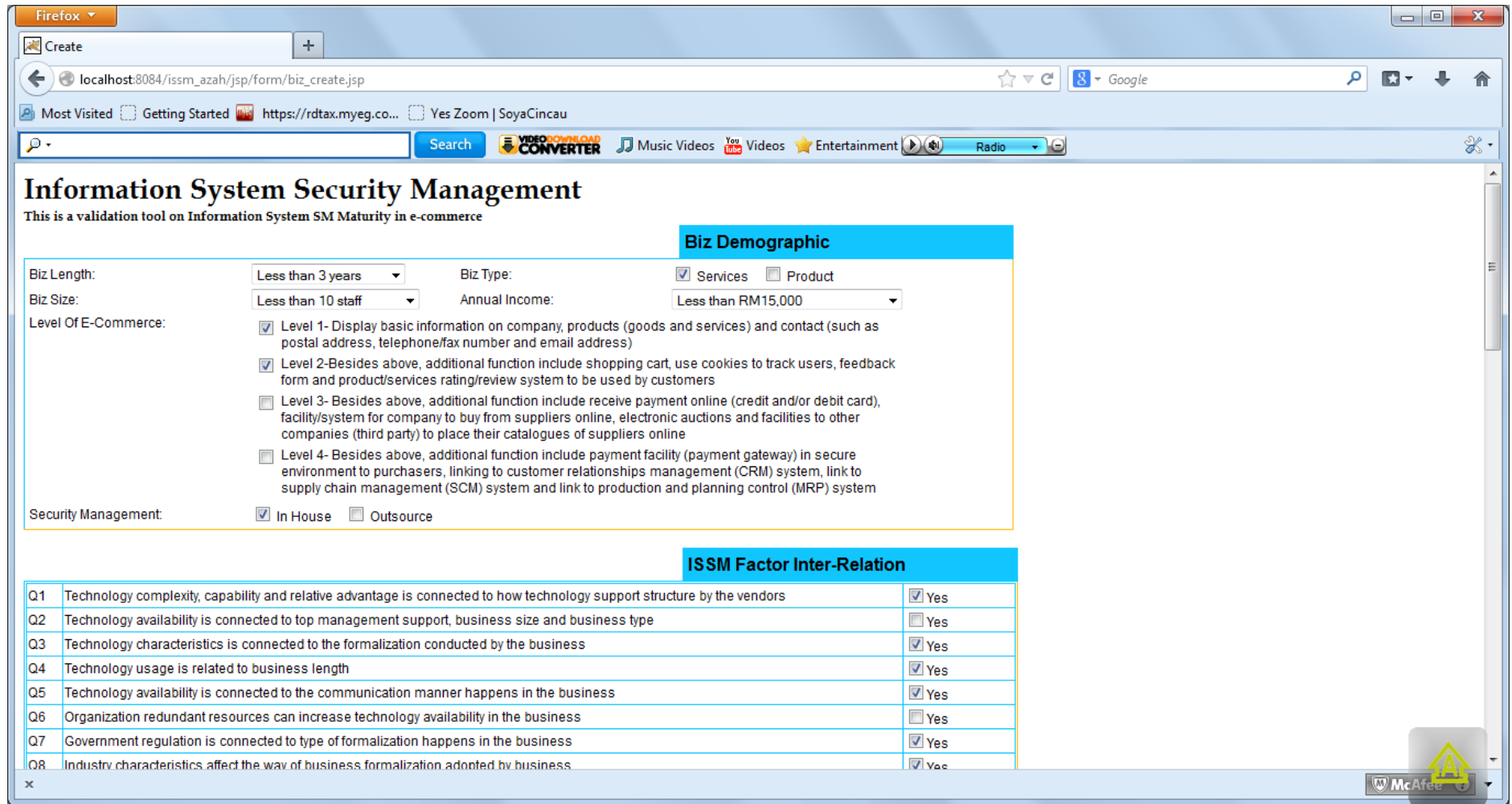


Figure 2: Business Demographic Screen

5. SMI/E are then required to identify their business position in terms of the factor inter-relation which has occurs in the business. [Figure 3]
6. SMI/E continues to identify factor dynamics involved in their business. These two identified factors were determined as part of the findings gathered during the research investigation results analysis. [Figure 3]

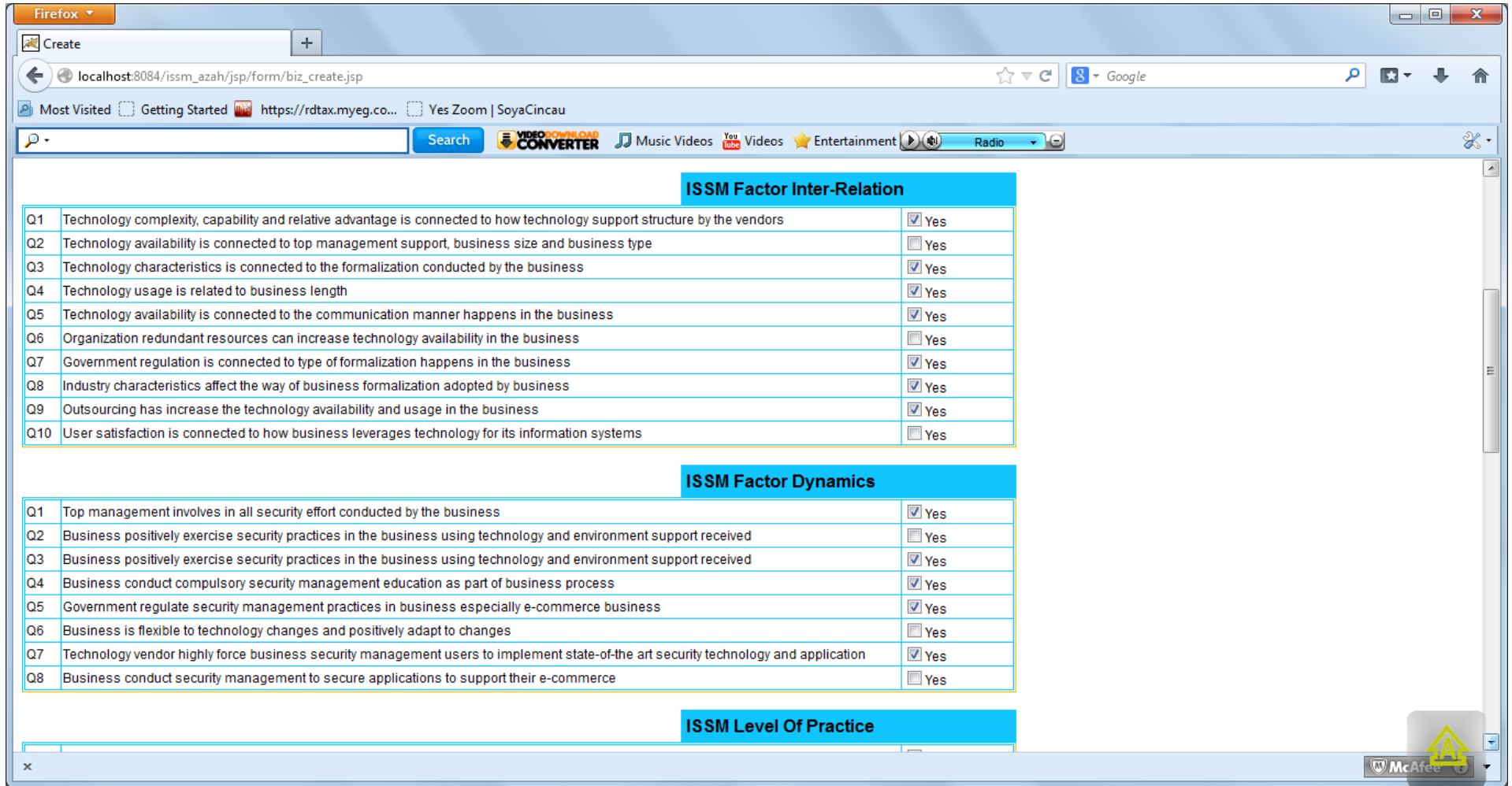


Figure 3: ISSM factor inter-relation and factor dynamic

- 7. Finally, SMI/E must end its assessment task by defining and ISSM practices being adopted and practised in the business. This information is crucial as it define the business ISSM implementation level and the well-being of security management of the business. [Figure 4a and 4b]

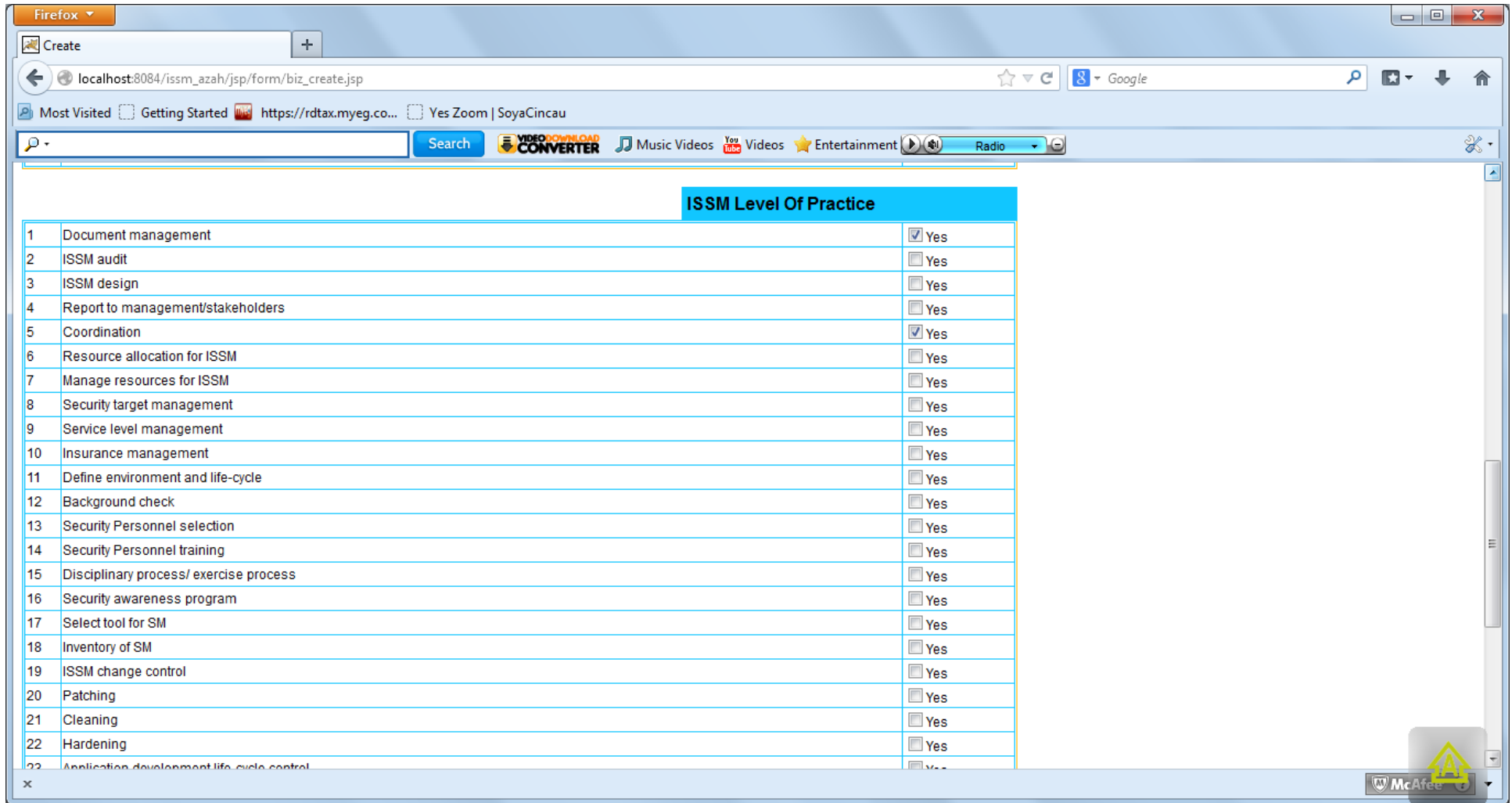


Figure 4a: ISSM level of practices

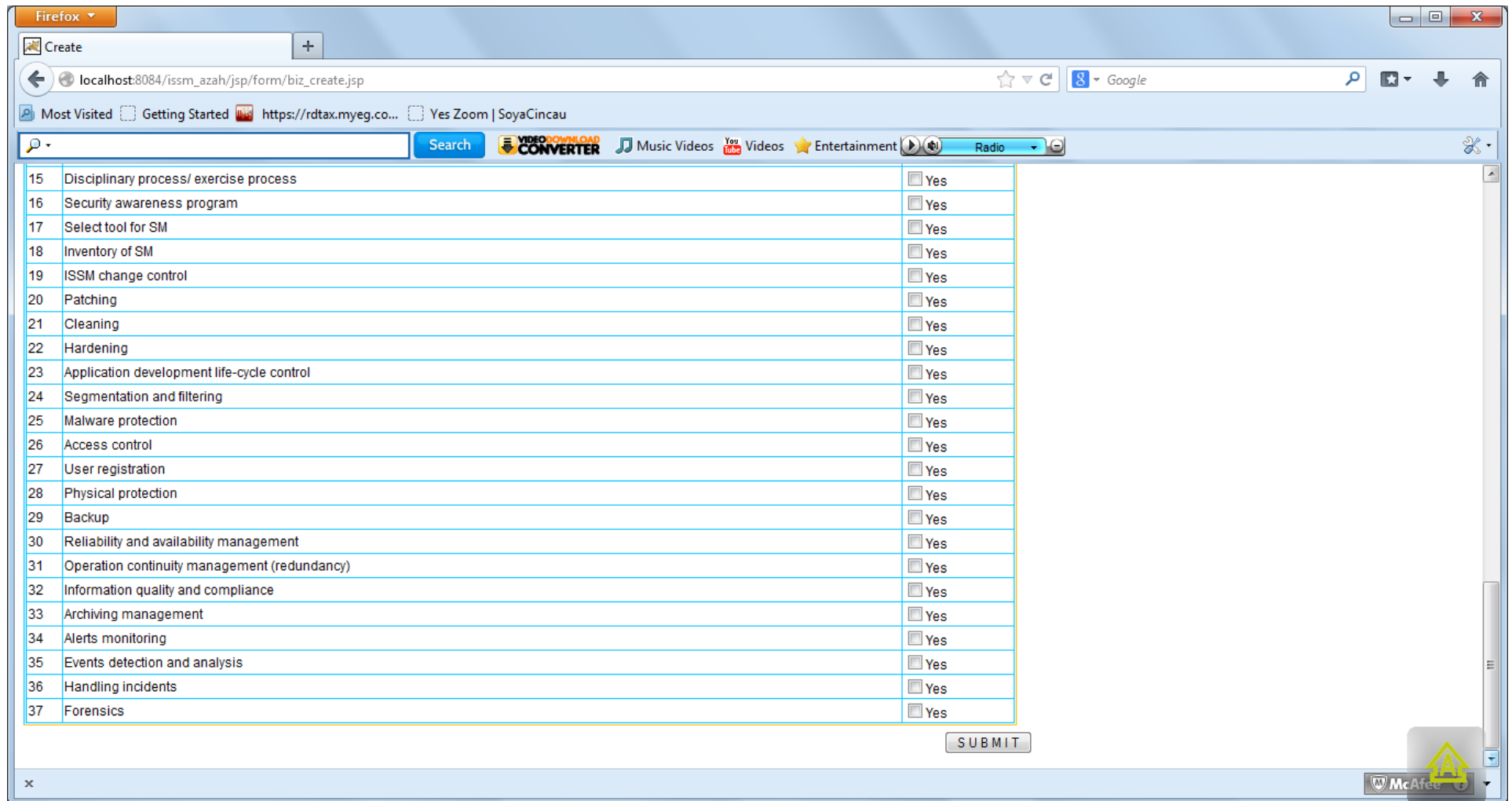


Figure 4b: ISSM level of practices

8. System then will assess all information input by the SMI/E. The system will assess the ISSM factor inter-relation status of the business in terms of percentage (%). [Figure 5]
9. Then, it will continue with the assessment of ISSM factor dynamics in-terms of percentage (%). [Figure 5]
10. Accumulation percentage (%) will be shown directly after these two results. [Figure 5]

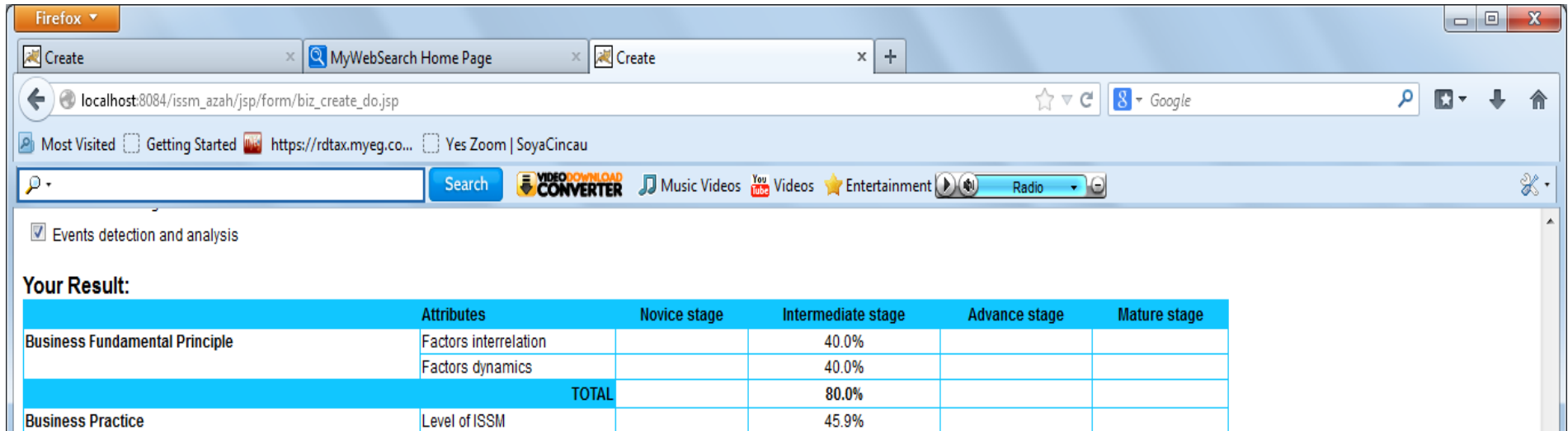


Figure 5: ISSM maturity results for SMI/E

11. The results does not end at accumulation percentage (%). As define in the research findings, to achieve ISSM maturity at certain level, both ISSM factor inter-relation and ISSM dynamics must be achieve concurrently. Hence, this system will calculate the results for ISSM maturity level through the factor inter-relation achievement and factor dynamics achievement though its average percentage (%). Though this, the business achievement is determined and the level of ISSM maturity of the business is achieved. [as shown in Figure 5]
12. There are four quadrant of Maturity level identified by the systems, which are the Novice, Intermediate, Advance and Mature. [Figure 5]
13. The business level of maturity in total may be slightly different from the calculation done in ISSM factor inter-relation and ISSM factor dynamics. Hence they may be possible changes from intermediate to novice, or advance to intermediate, if any factors are not achieve concurrently. This is because the determination of the ISSM maturity level is through concurrent ISSM factors achievement by the business, where each maturity quadrant has it determined score. [Figure 5]
14. Finally, system provides recommendation on ISSM practices required to improve business ISSM maturity level. [Figure 6]

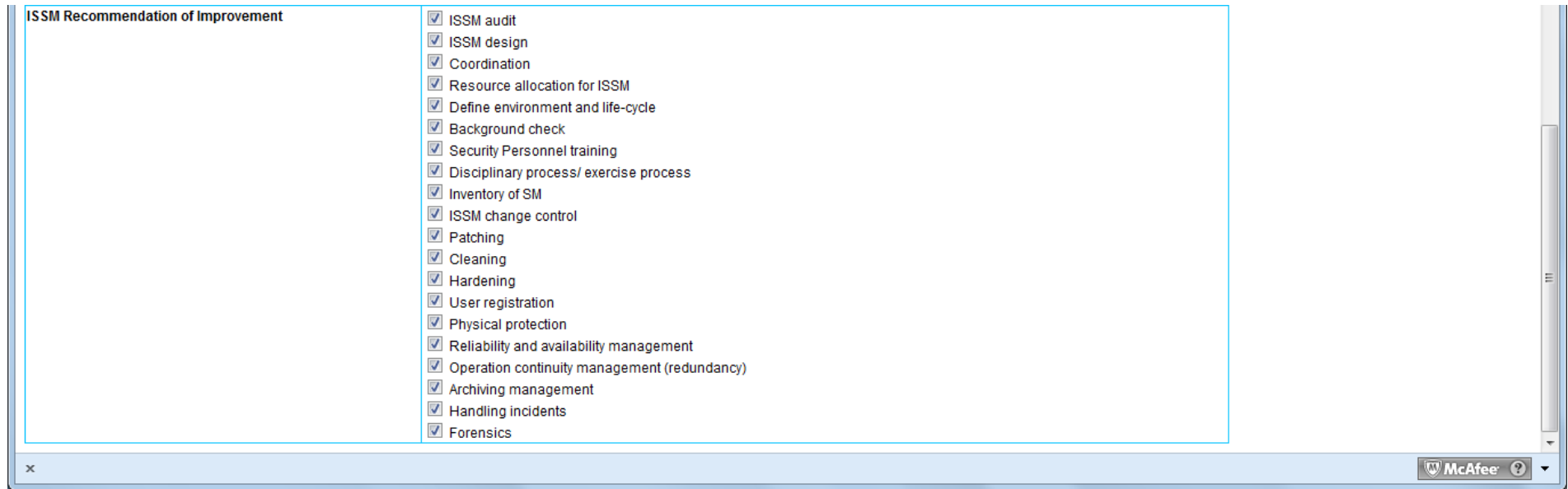


Figure 6: ISSM practices recommendation

APPENDIX F

ISSM VALIDATION AND EVALUATION FORM WITH EXPERTS

Information System Security Management (ISSM) Maturity -Validation Checklist

OBJECTIVE:

The objective of this validation is to compile and report the expert opinion on the model and system developed through the research findings. This validation activity is conducted to comply with external and internal examiner request. This activity was requested by the PhD examiners to gain validation from the expert, hence feed all expert comments and discussions for the purpose of PhD thesis corrections.

This research studied the socio-technical factors influencing the ISSM maturity in the SMI/E e-commerce context. You may find that the factors discussed were between technology, organization and environment factors rather than the detail of ISSM practices, which were often used and practiced in the business. These categorizations were part of the PhD findings, hence discussions and validation activities are based on the determined factors only.

A – Validation Details

Details of Validator

Name:	
Organisation:	
Position:	
Address of Organisation:	
Telephone Contact:	
Date of Validation:	
Signature of Validator:	

B – Expert Validation Objectives and Activities Checklist

Assessment activity	Y/N	Comment
The objective of the validation activity is clearly defined and conveyed.		
The written manual provided is appropriate.		
The validation conducted focuses on the issue of discussion. (Where issues covered the socio-technical factors believe to be the main influence of ISSM maturity of a SMI/E e-commerce)		

Document Name	Issued	Version	Owner
ISSM Maturity System Validation Checklist	2013	Version 1, 2013	Azah Anir Norman

C – Model Testing: Information System Security Management (ISSM) Maturity Assessment Profile

This section highlights the findings of the research. Two main contributors of ISSM maturity in SMI/E e-commerce is the influence of factor inter-relation and factor dynamics. Please rate how much do you agree with each of the statement below. Tick (✓) your answers.

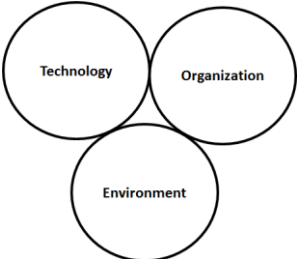
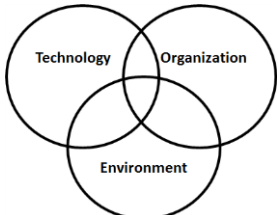

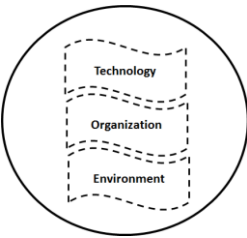
		Slightly agree	Moderately Agree	Highly Agree
No	Factor inter-relation	1	3	5
Ir1	Technology complexity, capability and relative advantage is connected to how technology support structure by the vendors			
Ir2	Technology availability is connected to top management support, business size and business type			
Ir3	Technology characteristics is connected to the formalization conducted by the business			
Ir4	Technology usage is related to business length			
Ir5	Technology availability is connected to the communication manner happens in the business			
Ir6	Organization redundant resources can increase technology availability in the business			
Ir7	Government regulation is connected to type of formalization happens in the business			
Ir8	Industry characteristics affect the way of business formalization adopted by business			
Ir9	Outsourcing has increase the technology availability and usage in the business			
Ir10	User satisfaction is connected to how business leverages technology for its information systems			

		Slightly agree	Moderately Agree	Highly Agree
No	Factor dynamic	1	3	5
Id1	Top management involves in all security effort conducted by the business			
Id2	Business can positively exercise security practices by having technology and environment support			
Id3	Top management decide fully on security management practices in the business			
Id4	Business conduct compulsory security management education as part of business process			
Id5	Government regulate security management practices in business especially e-commerce business			
Id6	Business is flexible to technology changes and positively adapt to changes			
Id7	Technology vendor highly force business security management users to implement state-of-the art security technology and application			
Id8	Business conduct security management to secure applications to support their e-commerce			

Document Name	Issued	Version	Owner
ISSM Maturity System Validation Checklist	2013	Version 1, 2013	Azah Anir Norman

D – Model testing: Information System Security Management (ISSM) Maturity Deterministic Profile

The factor inter-relation and factor dynamic tendency in a business define the overlapping socio-technical elements of a business. There are four overlapping scenarios to determine. Please tick (✓) which is the most appropriate representation of overlapping elements. Please comment on each representation.

NO	Overlapping scenario	Level of matureness of a business			
		Novice	Intermediate	Advance	Mature
1	 <p>Technology, organization and environment in a business has not shown any inter-relation and dynamics</p>				
2	 <p>Small inter-relation and dynamics between technology, organization and environment involved in a business</p>				
3	 <p>The inter-relation and dynamic of technology, organization and environment is seen highly correlated</p>				
4	 <p>There are holistic inter-relation and dynamic between all three factors. Business depend highly on these socio-technical elements for the security management success and effectiveness of the business</p>				

Document Name	Issued	Version	Owner
ISSM Maturity System Validation Checklist	2013	Version 1, 2013	Azah Anir Norman

E –Evaluation on the Information System Security Management (ISSM) Maturity Validation Tool Prototype

The system developed based on the input from section C. The systems will calculate the overlapping elements and provide results of the business maturity position. Please rate the assessment below.

System Usability	Y/N	COMMENT
1. System provides clear input for SMI/E to agree upon.		
2. The technical jargon displayed in the system is fairly easy to understand		
3. Business will not need to have high-level of security management understanding to use this system, hence provide business clear position of the business		
System output	Y/N	COMMENTS
1. The system calculated the business security management position clearly		
2. Through the result output business will be able to understand their security management maturity position		
3. Recommendation towards improvement is mentioned for business attention		
4. It is appropriate for the four segmentation of ISSM maturity for this business context based on the representation of the results		
System purpose	Y/N	COMMENTS
1. The purpose of the system is to provide level of maturity in terms of percentage is achieved		
2. Through the result business has an idea of the business security management status.		
3. The simple recommendation for improvement provides a guide to business on the security management area need to be improved.		

Document Name	Issued	Version	Owner
ISSM Maturity System Validation Checklist	2013	Version 1, 2013	Azah Anir Norman

REFERENCES

- Abu-Musa, A. (2010). Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security*, 18(4), 226–276.
- Aceituno, V. (2006a). ISM3: A standard for information security management. *ISSA Journal*, 22–25.
- Aceituno, V. (2006b). *ISM3 v1.20 published, a standard for advance information security management*. Retrieved from <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-04/msg00081.html>
- Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information systems research*, 9(2), 204–215.
- Ainin, S., & Noor Ismawati, J. (2003). E-commerce stimuli and practices in Malaysia. *PACIS 2003 Proceedings*, 38.
- AlAboodi, S. (2006). A new approach for assessing the maturity of information security. *Information Systems Control Journal*, 3, 36.
- Alam, S., & Ahsan, N. (2007). ICT adoption in Malaysian SMEs from services sectors: Preliminary findings. *Journal of Internet Banking and Commerce*, 12(3), 11.
- Al-Awadi, K., & Saidani, M. (2010). Justifying the need for a data security management plan for the UAE. *Information Management & Computer Security*, 18(3), 173–184.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276–289.
- Alfawaz, S. (2011). Information security management: a case study of an information security culture.
- Andam, Z. (2003). *E-commerce and e-business.[online] Kuala Lumpur, Malaysia: Undp-apdip, e-asean task force*. Retrieved from [http://dl.is.vnu.edu.vn/bitstream/123456789/233/1/eprimer-ecom\[1\].pdf](http://dl.is.vnu.edu.vn/bitstream/123456789/233/1/eprimer-ecom[1].pdf)
- Anderson, E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security*, 27(1), 22–29.
- Aris, N. M. (2006, 4-5 September 2006). *SMEs: Building blocks for economic growth*. Department of Statistics, Malaysia.
- Ayala, I. D. C. L., Vega, M., & Vargas-Lombardo, M. (2013). Emerging threats, risk and attacks in distributed systems: Cloud computing. In *Innovations and advances in computer, information, systems sciences, and engineering* (pp. 37–51). Springer.
- Bagozzi, R., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the academy of marketing science*, 16(1), 74–94.
- Bank Negara, M. (2005). *Status and performance of Small and Medium Enterprises (SME)*. Retrieved from http://www.bnm.gov.my/files/publication/sme/en/2005/chap_2.pdf
- Barlette, Y., & Fomin, V. (2008). Exploring the suitability of IS security management standards for SMEs. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 308–308).
- Baskerville, R. (1988). *Designing information systems security*. John Wiley & Sons, Inc.

- Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, 25(4), 375–414.
- Baskerville, R., & Myers, M. (2002). Information systems as a reference discipline. *MIS Quarterly*, 1–14.
- Baskerville, R., & Myers, M. (2009). Fashion waves in information systems research and practice. *MIS Quarterly*, 33(4), 647–662.
- Boudreau, M., Gefen, D., & Straub, D. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 1–16.
- Brancheau, J., Janz, B., & Wetherbe, J. (1996). Key issues in information systems management: 1994-95 sim delphi results. *MIS Quarterly*, 225–242.
- Brancheau, J., & Wetherbe, J. (1987). Key issues in information systems management. *MIS Quarterly*, 23–45.
- Burhanuddin, M., Arif, F., Azizah, V., & Prabuwno, A. (2009). Barriers and challenges for technology transfer in Malaysian Small and Medium Industries. In *Information management and engineering, 2009. ICIME'09. international conference on* (pp. 258–261).
- Burrell, G., & Morgan, G. (1994). *Sociological paradigms and organisational analysis*. Heinemann.
- Caralli, R., Stevens, J., Willke, B., & Wilson, W. (2004). *The critical success factor method: establishing a foundation for enterprise security management* (Tech. Rep.). DTIC Document.
- Cardholm, L. (2014). Identifying the business value of information security. *Approaches and Processes for Managing the Economics of Information Systems*, 157.
- Carnegie-Mellon, U. (1999). *Systems security engineering capability maturity model (sse-cmm)*. Carnegie Mellon University. Retrieved from SystemsSecurityEngineeringCapabilityMaturityModel(SSE-CMM) carnegie
- Cassel, C. M., Hackl, P., & Westlund, A. H. (2000). On measurement of intangible assets: a study of robustness of partial least squares. *Total Quality Management*, 11(7), 897–907.
- Cerf, V. (2001). A brief history of the internet and related networks. *Internet Histories*.
- Chang, S., & Ho, C. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345–361.
- Checkland, P. (2000). Soft systems methodology: A thirty year retrospective. *Systems Research and Behavioral Science*, 17, S11–S58.
- Chen, X., Li, S., Ma, J., & Li, J. (2011). Quantitative threat assessment of denial of service attacks on service availability. In *Computer Science and Automation Engineering (CSAE), 2011 IEEE International conference on* (Vol. 1, pp. 220–224).
- Chin, W. W. (1998a). The partial least squares approach for structural equation modeling.
- Chin, W. W. (1998b). The partial least squares approach for structural equation modeling.
- Cohen, F. (1987). Computer viruses: theory and experiments. *Computers & security*, 6(1), 22–35.
- Creswell, J., & Clark, V. (2007). *Designing and conducting mixed methods research*. Wiley Online Library.
- Crosby, P. (1979). *Quality is free: The art of making quality certain* (Vol. 94). McGraw-Hill New York.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions

- for behavioral information security research. *computers & security*, 32, 90–101.
- D'Arcy, J., & Hovav, A. (2009). Does one size fit all? examining the differential effects of is security countermeasures. *Journal of business ethics*, 89, 59–71.
- Da Veiga, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361–372.
- Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207.
- DeLone, W. H., & McLean, E. R. (1992). Information systems success: the quest for the dependent variable. *Information systems research*, 3(1), 60–95.
- DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of management information systems*, 19(4), 9–30.
- Denning, D. (1976). A lattice model of secure information flow. *Communications of the ACM*, 19(5), 236–243.
- Denning, D., Denning, P., & Schwartz, M. (1979). The tracker: A threat to statistical database security. *ACM Transactions on Database Systems (TODS)*, 4(1), 76–96.
- Denzin, N., & Lincoln, Y. (2005). *The sage handbook of qualitative research*. Sage Publications, Incorporated.
- Dhillon, G. (1995). *Interpreting the management of information systems security*. Unpublished doctoral dissertation, The London School of Economics and Political Science (LSE).
- Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125–128.
- Dhillon, G., & Backhouse, J. (2001). Current directions in is security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127–153.
- Diamantopoulos, A., & Siguaw, A. J. (2006). The error term in formative measurement models: Interpretation and modeling implications. *Journal of Modelling in Management*, 1(1), 7–17.
- Dictionaries, O. (2011). *Dictionary* (Vol. 2011) (No. 22 October).
- Dictionary, M. W. C. (2011). *Merriam-webster*.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6), 644–654.
- Dlamini, M., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, 28(3), 189–198.
- Dong, T.-P., Cheng, N.-C., & Wu, Y.-C. J. (2014). A study of the social networking website service in digital content industries: The Facebook case in Taiwan. *Computers in Human Behavior*, 30, 708–714.
- Dzazali, S. (2006). Social factors influencing the information security maturity of Malaysian Public Service Organisation: An empirical analysis. *ACIS 2006 Proceedings*, 103.
- Dzazali, S., Sulaiman, A., & Zolait, A. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, 26(4), 584–593.
- Economist, T. (2003). *Return of dotcom*. The Economist. Retrieved from <http://www.economist.com/node/2187144>

- Efron, B., & Tibshirani, R. (1993). *An introduction to the bootstrap* (Vol. 57). CRC Press.
- Eickelmann, N. (2004). Measuring maturity goes beyond process. *Software, IEEE, 21*(4), 12–13.
- Ein-Dor, P., & Segev, E. (1978). Organizational context and the success of management information systems. *Management Science, 24*(10), 1064–1077.
- Eloff, J. (1988). Computer security policy: Important issues. *Computers & Security, 7*(6), 559–562.
- Eloff, M., & Von Solms, S. (2000a). Information security management: a hierarchical framework for various approaches. *Computers & Security, 19*(3), 243–256.
- Eloff, M., & Von Solms, S. (2000b). Information security management: an approach to combine process certification and product evaluation. *Computers & Security, 19*(8), 698–709.
- Farn, K., Lin, S., & Fung, A. (2004). A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces, 26*(6), 501–513.
- Fisher, K., Broadbent, A., Shalm, L., Yan, Z., Lavoie, J., Prevedel, R., . . . Resch, K. (2014). Quantum computing on encrypted data. *Nature communications, 5*.
- Fitzgerald, K. (1995). Information security baselines. *Information Management & Computer Security, 3*(2), 8–12.
- Fomin, V., & Vries, H. (2008). ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption. In *EUROMOT 2008 Conference, Nice, France*.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 39*–50.
- Fraser, P., Moultrie, J., & Gregory, M. (2002). The use of maturity models/grids as a tool in assessing product development capability. In *Engineering Management Conference, 2002. IEMC'02. 2002 IEEE International* (Vol. 1, pp. 244–249).
- Furnell, S., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet research, 9*(5), 372–382.
- Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security issues in online social networks. *Internet Computing, IEEE, 15*(4), 56–63.
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information systems, 16*.
- Ghozali, I. (2008). *Structural equation modeling: Metode alternatif dengan partial least square*.
- Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal, 23*(4), 367–376.
- Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine de Gruyter.
- Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8*(4), 597–607.
- Goodhue, D., & Straub, D. (1991). Security concerns of system users: a study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13–27.
- Greene, J., Caracelli, V., & Graham, W. (1989). Toward a conceptual framework for mixed-method evaluation

- designs. *Educational evaluation and policy analysis*, 11(3), 255–274.
- Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems. *Computers & Security*, 16(8), 709–719.
- Guba, E., & Lincoln, Y. (1985). *Naturalistic inquiry* (Vol. 75). Sage Publications, Incorporated.
- Haenlein, M., & Kaplan, A. (2004). A beginner's guide to partial least squares analysis. *Understanding statistics*, 3(4), 283–297.
- Hair, J. (1998). *Multivariate data analysis: With readings*. Prentice-Hall.
- Hair, J., Anderson, B. B., R.E., & Black, W. (2010). *Multivariate data analysis*. Pearson.
- Hair, J., Ringle, C., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice*, 19(2), 139–152.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (PLS-SEM)*. SAGE Publications, Incorporated.
- Heikka, J., Baskerville, R., & Siponen, M. (2006). A design theory for secure information systems design methods. *Journal of the Association for Information Systems*, 7(11).
- Henseler, J., & Chin, W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. *Structural Equation Modeling*, 17(1), 82–109.
- Hoffer, J., & Straub, D. (1989). The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review*, 30(4), 35–43.
- Hone, K., & Eloff, J. (2002). Information security policy: What do international information security standards say? *Computers & Security*, 21(5), 402–409.
- Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, 23(3-Part-2), 918–939.
- Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security—a neo-institutional perspective. *The Journal of Strategic Information Systems*, 16(2), 153–172.
- Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database*, 36(4), 68–79.
- ISF, I. S. F. (2003). *The standard of good practices for information security*. Information Security Forum ISF. Retrieved from http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf
- ISO/IEC. (2008). *Corporate governance of information technology*. ISO.
- ISSA, I. S. S. A. (2004). *Generally Accepted Information Security Principles (GAISP)*. Information Systems Security Association (ISSA).
- Ivankova, N., Creswell, J., & Stick, S. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods*, 18(1), 3–20.
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*.
- Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of consumer research*, 30(2),

- Kandias, M., Virvilis, N., & Gritzalis, D. (2013). The insider threat in cloud computing. In *Critical information infrastructure security* (pp. 93–103). Springer.
- Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139–154.
- Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: A case study. *MIS Quarterly*, 571–586.
- Kartiwi, M., & MacGregor, R. C. (2007). Electronic commerce adoption barriers in Small to Medium-sized Enterprises (SMEs) in developed and developing countries: A cross-country comparison. *Journal of Electronic Commerce in Organizations (JECO)*, 5(3), 35–51.
- Kaynak, E., Tatoglu, E., & Kula, V. (2005). An analysis of the factors affecting the adoption of electronic commerce by SMEs: Evidence from an emerging market. *International Marketing Review*, 22(6), 623–640.
- Kock, N., & Verville, J. (2012). Exploring free questionnaire data with anchor variables: An illustration based on a study of it in healthcare. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, 7(1), 46–63.
- Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management*, 41(5), 597–607.
- Kowalski, S., Pavlovska, K., & Goldstein, M. (2013). Two case studies in using chatbots for security training. In *Information assurance and security education and training* (pp. 265–272). Springer.
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *computers & security*, 28(7), 509–520.
- Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840–847.
- Kvale, S., & Brinkmann, S. (2008). *Interviews: Learning the craft of qualitative research interviewing*. Sage Publications, Incorporated.
- Lavrakas, P. (2008). *Encyclopedia of survey research methods* (Vol. 1). Sage Publications, Incorporated.
- Lawshe, C. H. (1975). A quantitative approach to content validity1. *Personnel psychology*, 28(4), 563–575.
- Lessing, M. M. (2008). Best practices show the way to Information Security Maturity. In *6th National Conference on Process Establishment, Assessment and Improvement in Information Technology (improveit 2008)* (p. 1–9).
- Ling, C. Y. (2001). Model of factors influences on electronic commerce adoption and diffusion in Small & Medium-sized Enterprises. In *Doctoral consortium of the 9th european conference on information systems. bled. slovenia*.
- Loch, K., Carr, H., & Warkentin, M. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 173–186.
- Lynham, S. (2000). Theory building in the human resource development profession. *Human Resource Development Quarterly*, 11(2), 159–178.
- MacCallum, R. C., & Browne, M. W. (1993). The use of causal indicators in covariance structure models: Some practical issues. *Psychological bulletin*, 114(3), 533.

- Mansor, N., & Amri, A. A. (2010). The application of e-commerce among Malaysian Small Medium Enterprises. *European Journal of Scientific Research*, 14(4), 591–605.
- MasterCard. (2008). *Online shopping in Asia/Pacific patterns, trends and future growth*. Retrieved from http://www.mastercard.com/us/company/en/insights/pdfs/2008/Asia_Pacific_Online_Shop.pdf
- Maxwell, J. (1998). Designing a qualitative study. *Handbook of applied social research methods*, 69–100.
- Maxwell, J. (2004). *Qualitative research design: An interactive approach*. Sage Publications, Incorporated.
- Mayes, K., & Markantonakis, K. (2014). Information security best practices. In *Secure smart embedded devices, platforms and applications* (pp. 119–144). Springer.
- Melenovsky, M., & Sinur, J. (2006). BPM maturity model identifies six phases for successful BPM adoption. *Gartner Research, Stamford*.
- Merriam, S. B. (1998). *Qualitative research and case study applications in education. revised and expanded from "case study research in education"*. The Education Resource Information Center (ERIC).
- Miles, M., & Huberman, A. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage Publications, Incorporated.
- Mingers, J. (2001). Combining is research methods: Towards a pluralist methodology. *Information systems research*, 12(3), 240–259.
- Mingers, J., & Brocklesby, J. (1997). Multimethodology: Towards a framework for mixing methodologies. *Omega*, 25(5), 489–509.
- Mohamad, R., & Ismail, N. A. (2009). Electronic commerce adoption in SME: the trend of prior studies. *Journal of Internet Banking and Commerce*, 14(2), 1–16.
- Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), 2366–2375.
- Monfelt, Y., Pilemalm, S., Hallberg, J., & Yngström, L. (2011). The 14-layered framework for including social and organizational aspects in security management. *Information Management & Computer Security*, 19(2), 124–133.
- Mora, J.-D., & Barnes, N. G. (2011). Online media in fast-growing companies: Adoption, usage and relation to revenues. *Marketing Management Journal*, 21(2).
- Morgan, D. L. (1998). Practical strategies for combining qualitative and quantitative methods: Applications to health research. *Qualitative health research*, 8(3), 362–376.
- Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, 22(11), 594–597.
- Mumford, E. (1994). New treatments or old remedies: is business process reengineering really socio-technical design? *The Journal of Strategic Information Systems*, 3(4), 313–326.
- Mumford, E. (2000). A socio-technical approach to systems design. *Requirements Engineering*, 5(2), 125–133.
- Murine, G., & Carpenter, J. (1984). Measuring computer system security using software security metrics. In *Proceedings of the 2nd IFIP International Conference on Computer Security: A global challenge* (pp. 207–215).
- Myers, M., & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and organization*, 17(1), 2–26.

- Nasir, R., & Ponnusamy, V. (2007). An exploratory study on the level of trust towards online retailers among consumers in the United Kingdom and Malaysia. Available at SSRN 1079663.
- Neuman, W. (2009). *Understanding research*. Pearson/Allyn and Bacon.
- Niederman, F., Brancheau, J., & Wetherbe, J. (1991). Information systems management issues for the 1990s. *MIS Quarterly*, 15(4), 475–500.
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. McGraw, New York.
- Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within turkey. *International Journal of Information Management*, 30(6), 567–572.
- Parker, D. (1997). Strategic values of information security in business. *Computers & Security*, 16(7), 572–582.
- Paynter, J., & Lim, J. (2001). Drivers and impediments to e-commerce in Malaysia. *Malaysian Journal of library and Information science*, 6(2), 1–19.
- Petter, S., & Gallivan, M. (2004). Toward a framework for classifying and guiding mixed method research in information systems. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference* (pp. 10–pp).
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623–656.
- Podsakoff, P., MacKenzie, S., Lee, J., & Podsakoff, N. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, 88(5), 879.
- Prananto, A., McKay, J., & Marshall, P. (2003a). The spectrum of e-business maturity in Australian SMEs: A multiple case study approach to the applicability of the stages of growth for e-business model. In *11th european conference on information systems (ecis)*.
- Prananto, A., McKay, J., & Marshall, P. (2003b). A study of the progression of e-business maturity in Australian SMEs: Some evidence of the applicability of the stages of growth for e-business model. *Proceedings of the PACIS, Adelaide*, 68–80.
- Ramayah, T., Yan, L., & Sulaiman, M. (2005). SME e-readiness in Malaysia: Implications for Planning and Implementation. *Sasin Journal of Management*, 11(1), 103–120.
- Ramdani, B., Chevers, D., & Williams, D. A. (2013). SMEs' adoption of enterprise applications: A technology-organisation-environment model. *Journal of Small Business and Enterprise Development*, 20(4), 735-753.
- Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). Pfires: a policy framework for information security. *Communications of the ACM*, 46(7), 101–106.
- Ringle, C., Wende, S., & Will, A. (2005). SmartPLS 2.0 (m3) Beta. Hamburg: <http://www.smartpls.de>.
- Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
- Rogers, E. (1995). *Diffusion of innovations*. Simon and Schuster.
- Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data*. SAGE Publications, Incorporated.
- Ruighaver, A., Maynard, S., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *computers & security*, 26(1), 56–62.

- Russell, D. (2002). In search of underlying dimensions: The use (and abuse) of factor analysis in personality and social psychology bulletin. *Personality and social psychology bulletin*, 28(12), 1629–1646.
- Russell, R. (1990). Innovation in organizations: Toward an integrated model. *Review of Business*, 12(2), 19–25.
- Sage, A. (2009, 26 October 2011). *Study predicts U.S. e-commerce comeback by 2010*. Reuters.
- Sahama, T., Simpson, L., & Lane, B. (2013). Information Security Discipline, Science and Engineering Faculty, Queensland University of Technology, Brisbane, Australia. In *e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference* (pp. 249–253).
- S'anchez, L., Villafranca, D., Fernandez-Medina, E., & Piattini, M. (2006). Practical approach of a secure management system based on iso/iec 17799. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference* (pp. 8–pp).
- Schlarman, S. (2002). The case for a security information system. *Information systems security*, 11(1), 44–50.
- Sematech, N. (2012). *e-handbook of statistical methods*.
- Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612–613.
- Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, 22(2), 63–75.
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41.
- Siponen, M. (2002a). *Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm*. University of Oulu.
- Siponen, M. (2002b). Towards maturity of information security maturity criteria: Six lessons learned from software maturity criteria. *Information management & computer security*, 10(5), 210–224.
- Siponen, M. (2005). An analysis of the traditional is security approaches: Implications for research and practice. *European Journal of Information Systems*, 14(3), 303–315.
- Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49(8), 97–100.
- Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database*, 38(1), 60–80.
- Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270.
- Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.
- SIRIM, D. o. S. M. (2007). *Information technology-security techniques-information security management systems-requirements*. SIRIM Berhad.
- Sohail, M. S. (2003). Service quality in hospitals: More favourable than you might think. *Managing Service Quality*, 13(3), 197–206.
- Stacey, T. (1996). Information security program maturity grid. *Information Systems Security*, 5(2), 22–33.
- Stats, I. W. (2011). *The Internet Usage Statistics* (Vol. 2011) (No. 25 October).

- Stats, I. W. (2012). *Internet Usage in Asia* (Vol. 2012) (No. 27 October).
- Stoll, M., & Breu, R. (2013). Information security measurement roles and responsibilities. In T. S. Elleithy & K. (Eds.), *Emerging trends in computing, informatics, systems sciences, and engineering , lecture notes in electrical engineering* (p. 11-23). New York: Springer Science+Business Media.
- Straub, D. (1986). Computer abuse and security: Update on an empirical pilot study. *ACM SIGSAC Review*, 4(2), 21–31.
- Straub, D. (1990). Effective is security: An empirical study. *Information Systems Research*, 1(3), 255–276.
- Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems*, 13(24), 380–427.
- Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22, 441–470.
- Straub Jr, D., & Nance, W. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 45–60.
- Tan, K. S., Chong, S. C., Lin, B., & Eze, U. C. (2009). Internet-based ICT adoption: Evidence from Malaysian SMEs. *Industrial Management & Data Systems*, 109(2), 224–244.
- Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). Sage Publications, Incorporated.
- Taylor, M., & Murphy, A. (2004). SMEs and e-business. *Journal of Small Business and Enterprise Development*, 11(3), 280-289.
- Teubner, R., & Klein, S. (2007). Planning and designing web-based electronic commerce: A case study in the insurance industry. *Australasian Journal of Information Systems*, 6(1).
- TheStar. (2011, 21 April). *Online shopping trend rising in Malaysians, rm1.8bil spent in 2010*. Star Publications.
- TheStar. (2013, 28 September). *Maxis wants to be prepaid leader*. Star Publications.
- Thompson, B. (2004). *Exploratory and confirmatory factor analysis: Understanding concepts and applications*. American Psychological Association.
- Thompson, S. (2013). Helping the hacker? library information, security, and social engineering. *Information Technology and Libraries*, 25(4), 222–225.
- Thong, J. Y., Yap, C.-S., & Raman, K. (1996). Top management support, external expertise and information systems implementation in small businesses. *Information systems research*, 7(2), 248–267.
- Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation*. Lexington Books (Lexington, Mass.).
- Torres, J., Sarriegi, J., Santos, J., & Serrano, N. (2006). Managing information systems security: Critical success factors and indicators to measure effectiveness. *Information Security*, 530–545.
- Trauth, E., & Jessup, L. (2000). Understanding computer-mediated discussions: Positivist and interpretive analyses of group support system use. *MIS Quarterly*, 24(1), 43–80.
- Trist, E. (1981). The evolution of socio-technical systems. *Occasional paper*, 2, 1-67.
- Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001). Embedding security practices in contemporary information systems development approaches. *Information Management & Computer Security*, 9(4), 183–

- Tsohou, A., Kokolakis, S., Lambrinouidakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, 18(5), 350–365.
- Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application*, 11(2), 5–40.
- van Niekerk, B., & Jacobs, P. (2013). Cloud-based security mechanisms for critical information infrastructure protection. In *Adaptive Science and Technology (ICAST), 2013 International Conference* (pp. 1–4).
- Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476–486.
- Von Solms, B. (2005). Information security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99–104.
- von Solms, B. (2006). Information security—the fourth wave. *Computers & Security*, 25(3), 165–168.
- Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371–376.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101.
- Webster, J., & Watson, R. (2002). Analyzing the past to prepare.
- Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of it security management. *Information Management & Computer Security*, 17(1), 4–19.
- Wirtz, B. W., Piehler, R., & Ullrich, S. (2013). Determinants of social media website attractiveness. *Journal of Electronic Commerce Research*, 14(1).
- Wold, S. (1974). Spline functions in data analysis. *Technometrics*, 16(1), 1–11.
- Wong, J. (2013). *Malaysia's Online Shopping Behaviour 2012*. (Vol. 2013) (No. 6 December). Openminds Resources.
- Wood, C. (1987). Information systems security: Management success factors. *Computers & Security*, 6(4), 314–320.
- Yeh, Q., & Chang, A. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, 44(5), 480–491.
- Yeo, A., Rahim, M., & Miri, L. (2007). Understanding factors affecting success of information security risk assessment: The case of an Australian Higher Educational Institution.
- Yildirim, E. E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in Small-and Medium-sized Enterprises: A case study from Turkey. *International Journal of Information Management*, 31(4), 360–365.
- Yin, R. (2008). *Case study research: Design and methods* (Vol. 5). Sage Publications, Incorporated.
- Zakaria, M., & Hashim, M. (2003). Malaysian SMEs perceptions of e-business: Some empirical evidence. In *Proceedings of the National Seminar on E-commerce, Kuala Lumpur, Malaysia* (pp. 31–38).

- Zhou, Y., & Jiang, X. (2012). Dissecting android malware: Characterization and evolution. In *Security and Privacy (SP), 2012 IEEE Symposium* (pp. 95–109).
- Zhuang, Y., & Lederer, A. (2004). The impact of top management commitment, business process redesign, and it planning on the business-to-consumer e-commerce site. *Electronic Commerce Research*, 4(4), 315–333.
- Zissis, D., & Lekkas, D. (2011). Securing e-government and e-voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), 239–251.
- Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & Security*, 26(3), 256–265.