

Role of the Boards and Senior Management within Formal, Technical and Informal Components: IS/IT Security Governance in the Malaysian Publicly Listed Companies

By

Nadianatra Musa

**BSc (Hons.), Universiti Teknologi Malaysia (UTM), Malaysia, 2000
MSc (Information Systems), University of Tasmania, Australia, 2003**

Submitted in fulfilment of the requirements for the Degree of
Doctor of Philosophy

**School of Accounting and Corporate Governance
Faculty of Business
University of Tasmania**

November, 2011

Declaration of Originality

This thesis contains no material which has been accepted for a degree by the University or any other institution, except by way of background information and duly acknowledged in the thesis, and to the best of the my knowledge and belief no material previously published or written by another person except where due acknowledgement is made in the text of the thesis, nor does the thesis contain any material that infringes copyright.

Nadianatra Musa

Date

Statement of Authority of Access

This thesis may be made available for loan and limited copying in accordance with the Copyright Act 1968.

Nadianatra Musa

Date

Statement of Ethical Conduct

The research associated with this thesis abides by the international and Australian codes on human and animal experimentation, the guidelines by the Australian Government's Office of the Gene Technology Regulator and the rulings of the Safety, Ethics and Institutional Biosafety Committees of the University.

Nadianatra Musa

Date

Acknowledgements

I would like to express my gratitude to all those gave me the possibility to complete the thesis.

Foremost, I would like to express my sincere gratitude to my supervisors, Associate Professor Trevor Wilmshurst, Dr Gail Ridley, Dr Vishv Malhotra and Professor Bob Clift for the continuous support of my PhD study and research, for their patience, motivation, enthusiasm and immense knowledge. Their guidance helped me in all the time of researching and writing this thesis. I have worked with a number of people who contributed in assorted ways to the research, I gratefully thank them for their insightful comments, their willingness to share bright thoughts which were fruitful for shaping up my ideas and research. It was great to collaborate with you all.

Besides my supervisors, I would like to thank my employer, the Universiti Malaysia Sarawak (Unimas) and the Ministry of Higher Education Malaysia for being my sponsor and supporter throughout my PhD study.

I thank my research colleagues and friends in University of Tasmania, Lynne Gerke, Shaari, Hazianti, Andrew, Nahar, Mahdi, Shaz for sharing various thoughts at the office and many places.

Especially, I would like to convey my special thanks to my husband, Abdul Razak Abang Othman and my daughter, Dayang Mashitah Abdul Razak, who have always stood by me when I need them, always supported me all the time in my life. I owe my deepest gratitude to my parents Musa Bidin and Masnah Sahni, my siblings and all family members for their encouragement, patience and supporting me spiritually throughout my life.

I am indebted to my friends, Dayang Hanani Abang Ibrahim, Dr Kartinah Zen, Halikul Lenando, Nazim, Rosita, Yanti, Nehran, Mariatun, Sabri Samson, Anjung, Rafeah, Joyce and Roziah for creating such great friendships and for their stimulating support throughout my writing and research. I thank the Malay Tassie Society (Tasmania) and Malaysia Hall-Melbourne (Melbourne), for being supportive and caring friends.

Finally, I would like to thank everybody who was important for the successful realisation of the thesis, as well as expressing my apology that I could not mention them personally one by one.

Abstract

In IT governance, there are two types of responsibilities, first is IT value governance and second is IT risk governance. The primary objective of this study is to examine the second type of responsibility, IT risk governance and specifically looking into the involvement of the board, senior management and all management levels in IS/IT security.

Prior research has shown a lack of involvement by the board and senior management in understanding IS/IT security problems, unbalanced implementation of IS/IT security within the formal, technical and informal components and lack of internal controls application over IS/IT security. The gap found in this study has lead to the development of two major research questions, Research Question 1-In what way does the involvement of Boards and senior management impact on the implementation of IS/IT security governance? and Research Question 2-How can directing and monitoring actions in the technical, formal and informal components of IS/IT security governance in corporations be implemented effectively and efficiently? The two research questions have steered the development of the conceptual framework, the model of IS/IT security governance and the research methods.

The IS/IT security governance model is an extension of the conceptual framework, the model prescribes several areas relating to the elements of the three components, formal, technical and informal and component interactions (Relationship Type 1-Formal/Informal, Relationship Type 2-Formal/Technical and Relationship Type 3-Technical/Informal) within Malaysian Publicly Listed Corporations. The model suggests IS/IT security ought to be included within risk management and internal controls practices, through ‘directing’ and ‘monitoring’ actions and exclusively emphasises the supervision role and the relationship between the supervisor (giver) and the holder of responsibility. Because the nature of study is sensitive and confidential; the study has adopted a triangulation method. Data were collected using interviews and a mail survey as primary sources and website analysis as a secondary source. 12 interviews were conducted with CEOs, CIOs, other senior managers and IT manager from eight companies of Group A (Top) and Group B (Middle) across different industries. Despite a low response rate for the mail survey, the data have high validity as interviews and responses involved appropriate people in leading organisations in Malaysia from Group A(Top) and Group B(Middle)- high profit and large market capitalisation organisations and experienced senior managers. Content analysis over 210 annual reports of website data from Group A, Group B and Group C was conducted.

The data from interviews, survey and website analysis have supported the model of IS/IT security governance. The findings from the interview data are consistent with the elements of formal, technical and informal components and component interactions; risk management and internal controls over IS/IT security and ‘directing’ and ‘monitoring’ actions over IS/IT security are supported. The results of the survey have shown that the respondents had similar perspectives as the model. The website analysis revealed that two factors may determine IS/IT security governance, the group type and industry type.

Table of Contents

Declaration of Originality.....	ii
Statement of Authority of Access.....	iii
Statement of Ethical Conduct.....	iv
Acknowledgements	v
Abstract	vi
List of Tables.....	xvii
List of Figures.....	xix
Chapter 1 Introduction.....	1
1.0 Background of study.....	1
1.1 Research Problems and Research Questions	3
1.2 Overview of the dissertation.....	7
Chapter 2: Literature Review.....	9
2.0 Introduction	9
2.1 The Need for IS/IT Security	10
2.2 IS/IT Security Incidents, Vulnerabilities and Threats.....	11
2.2 IS/IT security controls and security standards	17
a) IS/IT Security Controls.....	17
b) IS/IT Security Standard-17799/BS7799.....	20
2.3 IS/IT Security Requires a Governance Focus.....	23
2.4 An Holistic View of IS/IT Security Implementation.....	26
2.5 Evolving Perspectives on IS/IT Security	29
2.5.1 Corporate Governance, Boards and Senior Management.....	29
2.5.2 IS/IT and Business Risk.....	31
2.5.3 Corporate Governance, IS/IT Security Implementation and Adequate Internal Controls	34
2.6 Measuring the Efficiency and Effectiveness of Internal Controls over IS/IT Security Implementation.....	35
2.7 Components of IS/IT security.....	36
2.7.1 Technical aspect	36
2.7.2 Organisational aspect.....	37
2.7.3 Human aspect	37
2.7.4 Legal Aspect.....	39
2.8 Empowering Human Capital through Education, Training and Awareness	39
2.9 Creating a Security Culture	40
2.10 Other useful frameworks and regulations	41
2.10.1 The Committee of Sponsoring Organisations of the Treadway Commission (COSO).....	41
2.10.2 Sarbanes-Oxley Act.....	42

2.10.3 The Health Insurance Portability and Accountability Act of 1996 (HIPAA)	43
2.10.4 Malaysian Code of Corporate Governance	43
2.11 Summary.....	44
Chapter 3 A Conceptual Framework	45
3.1 Introduction	45
3.2 IS/IT risks and IT governance	50
3.3 IT risk governance.....	52
3.4 Formal, technical and informal dimensions of IT risk governance.....	53
3.5 Internal controls for IT risk governance across the formal, technical and informal dimensions	55
3.5.1 Directing Actions.....	56
3.5.1.1 Directing Actions: Formal dimension.....	56
3.5.1.2 Directing Actions: Technical dimension	57
3.5.1.3 Directing Actions: Informal Dimension	58
3.5.2 Monitoring Actions.....	58
3.5.2.1 Monitoring Actions: Formal dimension.....	59
3.5.2.2 Monitoring Actions: Technical dimension	59
3.5.2.3 Monitoring Actions: Informal dimension	60
3.5.3 Summary.....	60
3.6 Developing a model of IS/IT security governance	61
Chapter 4 A Model of IS/IT Security Governance: The Role of the Boards and Senior Management within Formal, Technical and Informal components	64
4.1 Introduction	64
4.2 The Three Components of IS/IT Security Governance	65
4.2.1 Formal component.....	65
a) IS/IT security vision.....	66
b) IS/IT security management strategy	67
c) IS/IT Security Policy	70
d) IS/IT Security Standards	70
4.2.2 Technical component.....	71
a)Technological Areas.....	71
b) IS/IT Security Procedures	74
4.2.3 Informal component	75
a) Employee values	76
b) Organisational values.....	77
4.3 A model of component Interaction	78
4.3.1 Relationship-Type 1 (RT1).....	79

4.3.2 Relationship-Type 2 (RT2).....	81
4.3.3 Relationship Type 3 (RT3).....	82
4.4 Risk Management and Internal Controls: Relationship with the three components and interaction model....	83
4.4.1 Relationship between Risk Management and Internal Control.....	84
4.4.2 Stages of Risk Management and Monitoring.....	87
a) Stage 1: Risk Identification	87
b) Stage 2: Risk Analysis and Assessment	87
c) Stage 3: Risk Mitigation.....	87
d) Monitoring and Review.....	88
4.4.3 Risk Management and Internal Controls	89
4.4.3.1 Risk Management and Internal Controls: Formal component	89
4.4.3.2 Risk Management and Internal Controls: Technical component.....	89
4.4.3.3 Risk Management and Internal Controls: Informal component.....	92
4.4.4 Risk Identification and Internal Control Application Process for the interaction of the three components model	94
4.4.5 Directing and Monitoring Actions over risks from Formal, Technical and Informal components and the model interactions.....	98
4.4.5.1 The directing and monitoring actions	98
4.4.5.2 The directing and monitoring actions: The Three Components and the interactions.....	99
4.4.5.2.1 The directing and monitoring actions: The Formal component and the interactions.....	100
a) Formal/Technical.....	100
b) Formal/Informal	101
4.4.5.2.2 The directing and monitoring actions: The Technical component and its interaction	102
a) Technical/Formal:.....	103
b) Technical/Informal	103
4.4.5.2.3 The directing and monitoring actions: The Informal component and its interaction	106
a) Informal/Technical	107
b) Informal/Formal	108
4.5 The directing and monitoring actions over three components and interaction through use of risk management and internal controls	110
4.6 Objectives, Conceptual Framework (Chapter 3) and IS/IT security governance model.....	112
4.7 Comparison between the IS/IT Security Governance Model and other existing security models	113
4.8 Summary.....	115
Chapter 5: Research Design and Methodology	116
5.0 Introduction	116
5.1 Research Design	116
5.2 Research Paradigm	117

5.3 Sample for study	120
5.3.1 Group Target Design	120
5.3.2 Sample analysis	121
5.4 Research Methods.....	121
5.4.1 Interviews	121
5.4.1.1 The development of the interview instrument	121
5.4.2 Questionnaire.....	125
5.4.3 Website Analysis	126
5.5 Before Analysis	127
5.6 Data Analysis.....	129
5.6.1 Data Analysis Process.....	129
5.6.1.1 Data Analysis Procedures for Qualitative Data	129
Software analysis.....	130
Manual content analysis	130
5.6.1.2 Data Analysis Procedures for Quantitative Data	130
Website Analysis	130
Mail Survey	131
Chapter 6 Website Analysis.....	132
6.0 Introduction	132
6.1 Sample Analysis	132
6.2 Demographic Analysis.....	132
6.2.1 Group A.....	133
a) Analysis according to Industry Sectors	133
b) Analysis according to section of Annual Report	134
6.2.2 Group B	135
a) Analysis according to Industry Sectors	135
b) Analysis according to section of Annual Report	136
6.2.3 Group C	137
a) Analysis according to Industry Sectors	137
b) Analysis according to section of Annual Report	138
6.3 Data Analysis Procedures	138
6.4 Data Analysis and Research Questions	139
6.4.1 Data Analysis and Research Question 1	139
6.4.1.1 Formal Component	139
a) IS/IT Security Vision.....	139
b) IS/IT Security Management Strategy	140

i) Risk Management.....	141
ii) IS/IT Security internal controls	142
iii) Organisational structure of IS/IT security	142
iv) Education and Training relating to IS/IT security	143
v) Audit.....	144
c) IS/IT Security Policy	145
d) IS/IT Security Standards	147
6.4.1.2 Technical Component.....	147
a) Technological Resources Areas.....	148
i) IT Infrastructure and Business Data and Information.....	148
ii) Business Information Systems.....	149
b) IS/IT Security Procedures	149
6.4.1.3 Summary.....	150
6.4.2 Data Analysis and Research Question 2	153
6.4.2.1 Component Interaction	153
6.4.2.1.1 The relationship between Formal and Informal components, Relationship Type 1.....	153
6.4.2.1.2 The relationship between Formal and Technical components, Relationship Type 2.....	154
6.4.2.1.3 The relationship between Technical and Informal components, Relationship Type 3	155
6.4.2.2 Summary.....	155
The relationship between Formal and Informal components, Relationship Type 1	156
The relationship between Formal and Technical components, Relationship Type 2.....	156
The relationship between Technical and Informal components, Relationship Type 3	156
Chapter 7 Data Analysis: Leximancer Software Analysis.....	157
7.0 Introduction	157
7.1 Concept Map.....	157
7.1.1 Concepts	157
7.1.1.1 Co-occurrence of Concepts.....	159
a) Concept: Policy	160
b) Concept: Controls.....	162
c) Concept: Issues.....	164
d) Concept: Internal	166
e) Concept: Management.....	168
f) Concept: Level	170
g) Concept: Risk	172
h) Concept: Implementation	174
7.1.2 Themes	176

7.2.1 Results (<i>Concepts</i> , Themes, Co-Occurrence) and Research Question 1	178
1) Policy relating IT/IS security.....	179
2) Policy, IT/IS security and internal controls	180
3) Security issues and risk management	180
4) Security issues, organisational structure and risk management.....	181
5) IT/IS Security Policy, educational aspects and informal aspects.....	183
7.2.1.1 Summary.....	183
7.2.2 Results (<i>Concepts</i> , Themes, Co-Occurrence) and Research Question 2.....	184
7.2.2.1 Formal Dimension	185
a) IT/IS security policies.....	185
b) Role of IT Committee and IT/IS security policy implementation	186
c) Training, other educational aspects and IT/IS security policy	187
7.2.2.1.1 Summary.....	189
7.2.2.2 Technical Dimension.....	189
a) Technical and IT/IS security policy.....	189
i) Monitoring Actions	189
b) Technical roles (in sharing issue)	190
7.2.2.2.1 Summary.....	191
7.2.2.3 Informal Dimension.....	191
a) culture and integrity of people.....	191
i) Implementation action	191
ii) Monitoring action	192
7.2.2.3.1 Summary.....	193
Chapter 8 Data Analysis: Manual Content Analysis of Interview Data	194
8.1 Introduction	194
Part 1.....	195
8.2 Data Source: background of interview participants.....	195
8.3 The development of results.....	197
Part 2.....	197
8.4 Data Analysis and Results	197
8.4.1 Themes	197
8.4.1.1 Formal Dimension Themes.....	198
8.4.1.2 Technical Dimension Themes	199
8.4.1.3 Informal Dimension Themes	200
8.4.2 Issues	200
8.4.2.1 Primary Issues and Secondary Issues	201

8.4.2.1.1 Primary Issue: Business Needs	201
8.4.2.1.1.1 Secondary Issues.....	203
1) Protection/Safeguarding of Information	203
2) Risk.....	205
3) Business/Strategic Goals	206
4) Compliance.....	207
5) Internal controls procedures and processes	209
6) Policy and informal factors.....	210
7) Governance in IT/IS	212
8) Responsibility of senior management	213
9) Role of Committee	213
10) Role of Department	215
8.4.2.1.2 Primary Issue: Policy Development.....	215
8.4.2.1.2.1 Secondary Issues.....	217
1) Role of IT staff	217
2) The role of boards	217
3) Role of other departments	218
4) Policy review by external party	218
5) Identification of policy development areas	218
8.4.2.1.3 Primary Issue: IS/IT Security Implementation	219
8.4.2.1.3.1 Secondary Issues.....	221
1. “the protection of IS/IT business assets”:	221
2. “policy process and roles”	222
3. “policy process, educational and informal factors” bold	224
4. “protection and controls”	226
5. “identification of security issues”:	227
6. “auditing IT policy”	228
7. “risk management”,	229
8. “policy achievement and internal controls”	230
8.4.2.1.4 Primary Issue: Monitoring	231
8.4.2.1.4.1 Secondary Issues.....	233
1. Monitoring actions.....	236
2. Protection.....	237
3. policy achievement and internal controls	237
8.4.2.1.5 Primary Issue: Shared roles in security issues	238
8.4.2.1.5.1 Secondary Issues.....	239

1) Technical roles	241
2) Governance role.....	242
8.4.2.1.6 Primary Issue: Security Issues and Budgets	242
8.4.2.1.6.1 Secondary issues.....	243
1. Security vision/IT vision	244
2. Security controls.....	244
8.4.2.1.6.2 Summary.....	247
Part 3.....	247
8.5 Relating the data to IS/IT Security Governance Model.....	247
8.5.1 Themes of the Model of IS/IT security governance and Research Questions	247
a) Formal Component Themes	248
b) Technical Component Themes	249
c) Informal Component Themes.....	249
8.5.2 Data Analysis and Research Questions.....	249
8.5.2.1 Data Analysis and Research Question 1	250
8.5.2.1.1 Formal Component Themes.....	250
a) IS/IT Security Vision.....	250
b) IS/IT Security Management Strategy	251
c) Risk Management	251
d) Risk Management and Internal Controls.....	254
e) IS/IT Security Policy	255
8.5.2.1.2 Technical Component Themes	256
8.5.2.1.3 Informal Component Themes	260
a) Employee Values.....	260
b) Organisational Values	261
8.5.2.2 Data Analysis and Research Question 2	261
8.5.2.2.1The relationship between Formal and Informal components, Relationship Type 1.....	261
8.5.2.2.2The relationship between Formal and Technical components, Relationship Type 2.....	263
8.5.2.2.3The relationship between Informal and Technical components, Relationship Type 3	264
8.5.3 Implementation and Monitoring Actions over the three components and interactions.....	265
8.5.3.1 The Directing and Monitoring actions: The Formal component and its interaction	265
a) Case: Company A.....	266
8.5.3.2 The Directing and Monitoring actions: The Technical component and its interaction.....	268
a) Case: Company E	268
8.5.3.3The Directing and Monitoring actions: The Informal component and its interaction.....	269
a) Case: Company D.....	269

Chapter 9 Mail Survey Analysis.....	271
9.1 Response Rate.....	271
9.2 Demographic Information	271
9.3.1 Additional Information on survey and Research Question 1	273
9.3.1.1 Formal component.....	273
a) Importance of IS/IT Security	273
b) IS/IT Security Policy	274
c) IS/IT security and internal controls	277
d) IT Steering Committee	279
e) IT/IS security and Risk Management	280
f) IS/IT Security Standard.....	280
g) Technical role by board and senior management	280
9.3.1.2 Informal component.....	281
9.3.1.3 Summary.....	282
9.3.2 Additional Information on survey and Research Question 2	283
9.3.2.1 Formal/Informal Relationship Type 1 (RT1).....	284
9.3.2.2 Formal/Technical Relationship Type 2 (RT2).....	286
9.3.2.3 Summary.....	287
Chapter 10: Conclusion, Limitations, Further Research and Recommendations.....	288
10.1 Introduction	288
10.1.1 Website Analysis	289
10.1.2 Interview Analysis.....	289
10.1.3 Survey Analysis	297
10.2 Limitations.....	300
10.2.1 Literature	300
10.2.2 Research methods	300
10.2.2.1 Interview and Survey	300
10.2.2.2 Website data	301
10.3 Recommendations for Future Research.....	301
10.3.1 Extension, Model on supervision roles.....	301
10.3.2 Extension, model of component interaction between formal, technical and informal components.....	301
10.3.3 Improving IS/IT security governance and involvement from all participants	301
10.3.4 Replication study of website analysis over annual reports	301
10.3.5 Improving IS/IT security training among internal employees	302
10.4 Recommendations for industry and practitioners	302
10.5 Contribution.....	304

Bibliography	305
Appendices	313
Appendix 5A: Cover Letter with Information Sheet	313
Appendix 5B: Cover Letter and Questionnaire	318
Appendix 5C: The link between survey and research questions.....	326
Appendix 5D: Sample of Malaysian Publicly Listed Companies with Market Capitalisation Figures (In Malaysian Ringgit-MYR).....	330
Appendix 6A: Foxit Reader.....	332
Appendix 7A: Leximancer and concept map.....	333
Appendix 8A (Sample-The details of secondary issues)	334
Appendix 8B: A sample of the transcripts.....	337

List of Tables

Table 2.1 Ranking of threats to IS/IT security (Whitman, 2003, p 93)	15
Table 2.2 Major security domains and number of controls (Baker et al. 2007).....	18
Table 3.1 Directing and Monitoring Processes over formal, technical and informal dimensions	61
Table 4.1 a) Examples of relationship between Risk Management and Internal Controls	85
Table 4.1 b) Examples of relationship between Risk Management and Internal Controls	86
Table 4.2: Risk Identification and Internal Controls for the component Interaction	97
Table 5.1 The group design of study using 2008's market capitalisation.....	120
Table 5.2: No of planned interview questions by Dimensions and Designation/Position Levels.....	123
Table 5.3 No of Planned of Listed Companies According to Group	123
Table 5.4 No of planned interviews to conduct according to group	124
Table 5.5 Number of sample for website data according to group	127
Table 6.1 No of sets of annual reports used for analysis in sample groups	132
Table 6.2 Analysis on Group A According to Industry Sectors	133
Table 6.3 Analysis on Group A according to Section of Annual Report.....	135
Table 6.4 Analysis on Group B According to Industry Sectors.....	136
Table 6.5 Analysis on Group B according to Section of Annual Report.....	137
Table 6.6 Analysis on Group C According to Industry Sectors.....	137
Table 6.7 Analysis on Group C according to Section of Annual Report.....	138
Table 7.1 Concepts and its frequency and relevance score.....	158
Table 7.2 The co-occurrence of the “policy” with other related <i>concepts</i>	161
Table 7.3 the co-occurrence between “controls” concept with others	163
Table 7.4 the co-occurrence between “issues” concept with others	165
Table 7.5 The co-occurrence between “internal” concept with others	167
Table 7.6 the co-occurrence and likelihood between “management” concept with others.....	169
Table 7.7 the co-occurrence and likelihood between “level” concept with others	171
Table 7.8 the co-occurrence between “risk” concept with others	173
Table 7.9 The co-occurrence between “implementation” concept with others.....	175
Table 8.1 Data source and background of participants	196
Table 8.2a The relation between themes and issues	198
Table 8.2b The relation between themes and issues	198
Table 8.3a The primary issue of ‘business needs’ and its secondary issues	202
Table 8.3b The primary issue of ‘business needs’ and its secondary issues.....	203
Table 8.4a The primary issue of ‘policy development’ and its secondary issues	216
Table 8.4b The primary issue of ‘policy development’ and its secondary issues.....	216
Table 8.5a The primary issue of ‘implementation’ and its secondary issues.....	220
Table 8.5b The primary issue of ‘implementation’ and its secondary issues	221
Table 8.6a The primary issue of ‘monitoring’ and its secondary issues	232
Table 8.6b The primary issue of ‘monitoring’ and its secondary issues.....	232
Table 8.7a The sub analysis of secondary issues over the primary issue of monitoring.....	234
Table 8.7b The sub analysis of secondary issues over the primary issue of monitoring	236
Table 8.8a The primary issue of ‘share roles’ and its secondary issues.....	239
Table 8.8b The primary issue of ‘share roles’ and its secondary issues	239
Table 8.9a The sub analysis of secondary issues over primary issue of ‘share roles’	240

Table 8.9b The sub analysis of secondary issues over primary issue of ‘share roles’	241
Table 8.10a The primary issue of ‘security issues and budget’ and its secondary issues	243
Table 8.10b The primary issue of ‘security issues and budget’ and its secondary issues	243
Table 8.11a The sub analysis of secondary issues over the primary issue of ‘security issues and budget’	245
Table 8.11b The sub analysis of secondary issues over the primary issue of ‘security issues and budget’	246
Table 9.1 Demographic characteristics of respondents	272
Table 9.2 Importance of IS/IT security	273
Table 9.3 IS/IT Security Risks by the Board of Directors	273
Table 9.4 IS/IT Security Risks by Senior Management	274
Table 9.5 IS/IT Security Risk a Business Risk	274
Table 9.6 IS/IT Security Risk, part of Corporate Risk Management Plan	274
Table 9.7 IT/IS security policy	275
Table 9.8 The Board of Directors responsibility over IS/IT Security Policies	276
Table 9.9 Senior Management accountability over IS/IT Security Policies	276
Table 9.10 Security issues IS/IT Security Policies Business Goals	276
Table 9.11 Security issues IS/IT Security Policies, Business Requirements	277
Table 9.12 Quality of processes over security controls	277
Table 9.13 IS/IT Security Policies involvement and personnel’s at all levels	277
Table 9.14 IT/IS security and internal controls	278
Table 9.15 Internal controls and IS/IT Security Policies	278
Table 9.16 The Board of Directors responsibility and internal controls over security risks	278
Table 9.17 The Board of Directors accountability and internal controls over security risks	278
Table 9.18 Senior Management accountability and internal controls over security risks	279
Table 9.19 IT Steering Committee in place	279
Table 9.20 IS/IT Steering Committee essential mechanism	279
Table 9.21 IS/IT Steering Committee plays role IS/IT security policies	280
Table 9.22 IT/IS security and risk management	280
Table 9.23 IT/IS security standards	280
Table 9.24 The Board of Directors accountability, technical roles	281
Table 9.25 Senior Management responsibility, technical roles	281
Table 9.26 The Board of Directors, monitor technical roles	281
Table 9.27 Human factor social issue	281
Table 9.28 Trust, integrity, ethicality	282
Table 9.29 Education, training and awareness	284
Table 9.30 Conduct of human factors and Code of Ethics	284
Table 9.31 The Board of Directors responsibility over human factors policy	284
Table 9.32 The Board of Directors accountability over human factors policy	285
Table 9.33 Senior Management responsibility, human factors policy	285
Table 9.34 Corporation policy, human factor, knowledge, culture, awareness	285
Table 9.35 The Board of Directors, monitor, human factor	285
Table 9.36 Senior Management responsibility, monitor human factor	286
Table 9.38 The Board of Directors accountability over policy, standards and procedures	286

Table 9.39 Senior Management responsibility over policy, standards and procedures	287
Table 9.40 Reporting mechanism and IS/IT security governance	287

List of Figures

Figure 2-2 The model of Corporate Governance Direct Control Cycle (Solms, 2006, p 409)	24
Figure 2-3. Organisational structure for IS/IT security (William, 2007, p 13).....	27
Figure 3.1. A general organisational structure IS/IT security governance framework for any types of organisation.....	48
Figure 3.2. Research Focus of this study and IT governance framework.....	51
Figure 3.3. Relationship between internal controls, risk management and IS/IT security governance	53
Figure 3.4 Formal, technical and informal dimensions of IT risk governance	54
Figure 3.5 Internal controls process and IT risk governance of IS/IT security over the formal, technical and informal dimensions	56
Figure 3.6 A model of IS/IT security governance	63
Figure 4.1. Formal Component of IS/IT Security Governance.....	66
Figure 4.2. Technological Areas of Technical component	71
Figure 4.3. Technical component of IS/IT Security Governance Framework	72
Figure 4.4. Informal component of IS/IT security governance conceptual framework.....	76
Figure 4.5. Relationships between Formal, Technical and Informal components.....	79
Figure 4.6. Formal component has a relation to Informal component.....	80
Figure 4.7. Relationship between risk management and internal controls.....	84
Figure 4.8 Relationship between risk management and internal controls for the relationships among the three components	94
Figure 4.9 The directing and monitoring actions over the three components and interaction through use of risk management and internal controls.....	111
Figure 4.10. Conceptual framework of IS/IT security governance.....	112
Figure 5.1. A triangulation method designs approach adopted in this study (Ticehurst and Veal, 2000)	118
Figure 5.2. Triangulation Method Designs approach taken in this study	119
Figure 5.3 The relationship between research questions, the developed conceptual framework and data type.....	128
Figure 5.4 Procedures for Qualitative Data	129
Figure 7.1 The visualisation of <i>concepts</i> on the map.....	159
Figure 7.2 The co-occurrence of the “policy” with other related <i>concepts</i> by its brightness of ray colour	162
Figure 7.3 The co-occurrence of the “controls” with other related <i>concepts</i> by its brightness of ray colour	164
Figure 7.4 The co-occurrence of the “Issues” with other related <i>concepts</i> by its brightness of ray colour	166
Figure 7.5 The co-occurrence of the “internal” with other related <i>concepts</i> by its brightness of ray colour	168
Figure 7.6 The co-occurrence of the “management” with other related concepts by its brightness of ray colour	170

Figure 7.7 The co-occurrence of the “level” with other related <i>concepts</i> by its brightness of ray colour	172
Figure 7.8 The co-occurrence of the “risk” with other related <i>concepts</i> by its brightness of ray colour	174
Figure 7.9 The co-occurrence of the “implementation” with other related <i>concepts</i> by its brightness of ray colour	176
Figure 7-10 The <i>concepts</i> within the data set	178
Figure 10.1 Formal component themes of model and supporting data, manual content analysis.....	291
Figure 10.2 Technical component themes and supporting data, manual content analysis.....	291
Figure 10.3 Informal component themes of model and supporting data, manual content analysis	292
Figure 10.4 The component interaction across multiple companies (cases), the results of manual content analysis and supporting data	293
Figure 10.5 The directing and monitoring actions over the Formal component and its interaction and supporting data: by single case (company A)	295
Figure 10.6 The directing and monitoring actions over the Technical component and its interaction and supporting data: by single case (company E).....	296
Figure 10.7 The directing and monitoring actions over the Informal component and its interaction and supporting data: by single case (company E).....	297
Figure 10.8 The results of survey of formal themes and supporting data	299
Figure 10.9 The results of Informal themes and supporting data	299

Chapter 1 Introduction

1.0 Background of study

Over the past forty years or so, computers have replaced many of the manual systems of recording the activities of business and governmental organisations all over the world. More recently, the advances in technology have admitted millions of users to the Internet which has changed the environment in which our economic, social and political activities are conducted.

One outcome of these changes is the massive publicity that follows the discovery of any fraud in either the public or private sector and the occurrence of any technical break-down in computer systems, for example, in the reports and post-event analyses of such frauds as Enron and etc.,(Wood, 2002) it was never made absolutely clear whether these events were triumphs of outright dishonesty or whether the existing regulatory and recording systems were flawed which made it easier for the perpetrators to operate their schemes. Several corporate disasters received world-wide publicity and have stimulated research in many disciplines ranging from philosophy to labour relations but this investigation has been prompted by the confusion in the literatures relating to the business disciplines and Information Technology/Information Systems (IT/IS).

The academic literature and media reports (see Ch 2) relating to the use of computers in business consider serious frauds by employees against the corporation and by executives against shareholders and other stakeholders and, often without much evidence, attribute blame to technical problems in the computer systems or to misunderstandings of business problems by computer-related staff. On the other hand, authors in the IT/IS field contend that there are very few unresolved technical problems but that management and general staff are unwilling to accept their responsibilities for the operation of the computer systems. In addition, management and other users of the systems are unwilling to accord special status to IT/IS staff and expect the new systems to function at least as well as the systems that they replaced.

Some protagonists claim that the Board of Directors is responsible for the detailed operation of the computer systems and, therefore, must ensure that Board members are aware of what is going on and establish policies and procedures to ensure that the systems operate as planned. Other protagonists take the view that system designers, programmers and IT staff ought to be sufficiently well informed

about the specific business environment to be able to advise the Board about potential problems and currently available solutions.

Overall, the literature reflects a mixture of blame-shifting and lack of knowledge about what and why others in the organisation are required to do and how performance is monitored. At one level, this could be described as competition for status among different groups of employees. At another level, it could be seen as the lack of a theory which identifies problems, responsibilities and relationships among the various groups.

In most countries, corporate statutes and rules (mandatory or voluntary) about powers and responsibilities in corporations (corporate governance) place responsibility on the Board of Directors acting as a Board (Australian Stock Exchanges Group, 2012 & Securities Commission Malaysia, 2000). However, these documents do not provide much guidance about recognising potential problems or about preventative measures. Even so, it is apparent that knowingly tolerating dishonesty or incompetence within the corporation is likely to be regarded as negligence. Thus, there is an array of case law, management models and standards (see Ch 2) suggesting how Boards of Directors ought to operate.

As this researcher's interest lies in how IT/IS fits into the overall governance model, this investigation has been restricted to the role, responsibilities and potential of IT/IS in ensuring the best possible outcome for each corporation. It is expected that the development of a model for IT/IS security governance will contribute to the resolution of the turf wars referred to earlier and will improve the practice of this aspect of corporate governance. It is also expected that this model will provide a basis for the development of a more general corporate governance model that will be applicable to all organisations using computers.

Up to date, there has been no literature found in Malaysia that discussed the involvement of the boards and senior management in IT/IS security governance within Malaysian Publicly Listed Companies. There was a mutual lack of understanding of the interactions of IS/IT security problems among the board and senior managers and other line business managers including the interaction between the board and the IT Department, Accounting and Finance Department, Manufacturing Department and Human Resources Department. There is evidence that the major IS/IT security failures and incidents were caused by employees. For example, many existing employees do not bring IS/IT security problems to the notice of their heads of department or section for further strategic decisions.

The literature suggests that if the board and senior managers do not understand IS/IT security problems, the implementation of security controls may be less effective.

This study shows that boards and senior management do not always understand the IS/IT security problems and their implications for organisations. Vulnerabilities and threats were found to be the major cause of security incidents (Bishop, 1996). Failure to understand how security vulnerabilities and threats work in the organisation may affect the way that they protect their IS/IT assets and business information. If the IS/IT assets and business information of the organisation are vulnerable and exploited, it can lead to the failure of confidentiality, integrity and availability.

IT/IS security governance has increased in corporations to ensure that confidentiality, integrity and availability of business information are in place. If the confidentiality, integrity and availability of business information are compromised, corporations may incur direct losses and indirect losses to business (Su, 2006; Farahmand, 2003). For example, in the case of Enron and its auditors, Arthur Andersen, the senior management were shown to be involved in establishing “off-balance sheet” activities which helped to improve financial performance and increased its stock price (Wood 2002). The evidence has shown that corporate fraudulent behaviour was the major reason to the collapse of Enron. Even though the human aspect was a major factor of the Enron collapse it is believed that the board and senior managers did not understand how the security vulnerabilities and threats may lead to a variety of security attacks.

In another example, up to 70 percent of IT/IS security incidents are believed to be the result of internal users either through ignorance or stupidity and intentional acts (McIlwraith, 2006). This shows that there may be a lack of awareness by the boards and senior management in the implementation of IT/IS security governance within Malaysian Publicly Listed Companies. In order to address this problem, this study aims to examine the awareness of IT/IS security governance and its internal controls application within Malaysian Publicly Listed Corporations.

1.1 Research Problems and Research Questions

The research problems are now identified in detail followed by the research questions. There are three research problems prompting in this study.

Research Problem 1: Lack of involvement of the board and senior management in understanding IS/IT security problems

The first research problem is that IT/IS risk in relation to confidentiality, integrity and availability of business information is not seen as important at the board and senior management level (Amitava 2002; Kritzinger, Solms et al. 2003; Kizirian & Leese 2004; Force 2004; Knapp et al 2006; Posthumus & Von Solms 2006; Rastogi & Solms 2006).

Boards and senior management have left IS/IT security issues to be resolved at the IS/IT people/expertise level rather than at governance level. IS/IT security governance involves diverse people at different levels from top to bottom in order to achieve business goals. IT/IS security risk is also a business risk to corporations. This is due to the fact that the huge investment in IT/IS infrastructure and resources may expose business information internally and externally to risks if not identified, assessed and mitigated.

Research Problem 2: Unbalanced implementation of IS/IT security within the Formal, Technical and Informal components¹

It has been identified in the literature that there is a lack of informal aspects being governed by corporations relating to IT/IS security (Siponen & Oinas-Kukkonen 2007). The literature in IT/IS security has shown much work was focused on technical implementation, formal things such as management involvement, certification, standards and assessment but not much on people issues. As mentioned earlier, the majority (up to 70%) of IT/IS security incidents were the result of employee actions. There are two forms of actions; intended action and unintended action. Intended action can be malicious attacks (e.g., virus, worm, spyware, Trojan horses), intrusion of data and social engineering attacks (e.g., fraud). Unintended action can be human error, ignorance of the situation and stupidity, lack of integrity, trust, ethicality and lack of training, education and awareness. Security incidents, predominantly either by intended or unintended actions, have caused financial losses (e.g., data loss) and non-financial losses (e.g., business reputation, loss of confidence by investor) to corporations. IT risks vary. In spite of technical and formal aspects, boards and senior management are also responsible for IT risk caused by people issues. This is due to the fact that IT/IS security is not merely a technical issue but also a people and governance issue (Dhillon & Backhouse, 2000). As for that, a dynamic balance among the technical, formal and informal components is required within IT/IS security governance implementation (Torres, 2006, Mishra, 2007).

Research Problem 3: Lack of internal control applications over IS/IT security

¹ For definitions of these components see Section 4.2.

The third research problem identified in this study is a lack of internal control application in achieving policies relating to IT/IS security in corporations (Baker 2007, Siponen 2006 & Roger 2004). Corporations have internal controls in place to ensure procedures, regulations and laws are followed, transaction are properly documented, fraud, waste and abuse are minimised, unapproved transactions are not processed and desired outcomes are achieved in order to ensure that things go as intended. However, in the literature there is not much discussion on the importance of internal controls within the IT/IS security domain, in particular, in the areas of confidentiality, integrity and availability of business information. The literature also shows that IT/IS security in corporations is more concerned with the existence of security standards or security controls in place rather than the quality of implementation. For example, many corporations implement encryption technique to protect business data transferred via networks (e.g., internet/intranet), wireless systems and mobile phones from being intercepted by intruders. But what is the quality of the implementation? Does it follow the procedures? Does an outcome achieve security objectives and business goals? Has the process been checked, reported and communicated to higher levels and from higher levels to the bottom level?

These three research problems have lead to the development of two major research questions.

Research Question 1

In what way does the involvement of Boards and senior management impact on the implementation of IS/IT security governance?

Research Question 2

How can directing and monitoring actions in the technical, formal and informal components of IS/IT security governance in corporations be implemented effectively and efficiently?

In this study, a triangulated approach is adopted to answer the two posed research questions. Data were collected in three phases, phase 1 is a website analysis, phase 2 is an interview and phase 3 is a mail survey. Secondary data from the website were collected in Phase 1 and primary data from interviews and mail survey were collected in Phase 2 and Phase 3. The sample population of this study was divided into three, Group A-Top 100, Group B-middle 101-524 and Group C-Bottom 100, which was based on the market capitalisation recorded in 31 December 2008 by Bursa Malaysia. Throughout this study, all the three phases, Phase 1, Phase 2 and Phase 3 are sourced from the sample of the three groups.

A website analysis over the 210 annual reports of Malaysian Corporations was used in the first phase of data collection, the sample population of this study was taken from the annual reports of the three groups of companies, Group A, Group B and Group C. The study used the Foxit Reader program to discover texts and to highlight sentences that corresponded to the topics sought.

Interviews were conducted in the second phase of data collection. The interview schedule (questions of interview) was based on the themes/topics developed in the conceptual framework (Chapter 3) and predominantly governed by research questions 1 and 2. These semi-structured interviews were conducted with 1) boards of directors, represented by the CEO or Managing Director, 2) senior managers, represented by the Chief Information Officer/Chief Finance Officer and related designations and 3) junior managers, represented by the IT Manager, involved with IS/IT security.

A mail survey was employed in the third phase of data collection, respondents were boards of directors, senior managers and junior managers and represented all groups, Group A, Group B and Group C, within a number of industry background.

Respondents for the interviews and mail survey were selected from boards of directors, senior managers and junior managers.

Overall, findings indicate that the data of this study supported the themes developed in the IS/IT security governance model (Chapter 4), mainly supported most elements of the three components, formal, informal and technical and most component interactions. The findings from sample population also discover that Malaysian corporations have incorporated and included the issue of IS/IT security within their risk management and internal controls applications. The corporate governance components, namely, 'directing' and 'monitoring' actions, were found to be important actions in IS/IT security governance. The supervisory role between the giver (the supervisor) of responsibility and the holder of responsibility was vital for IS/IT security governance. The study answered both research questions 1 and 2, the results of the across-cases analysis and single-case analysis supported the elements of IS/IT security governance in three components of formal, informal and technical and the relationship of three component interactions over Relationship Type 1-formal/informal, Relationship Type 2-formal/technical and Relationship Type 3-technical/informal. The findings revealed that 'industry type' and 'group type' have an influence on the IS/IT security governance practices in the sample population of Malaysian publicly listed companies.

1.2 Overview of the dissertation

This study comprises 10 chapters.

Chapter 1 (Introduction) provides the general background of the study. It also presents the research problems and research questions. The chapter also outlines the structure and the organisation of the dissertation.

Chapter 2 (Literature Review) describes the literature on the role of boards and senior management in the effective application of internal controls to ensure that the corporation's directives, IS/IT security policies, standards, procedures, guidelines and administrative practices are properly implemented. First, the chapter addresses topics on the need for IS/IT security in these areas: 'IS/IT security incidents, vulnerabilities and threats', 'IS/IT security controls and security standards', 'IS/IT security requires a governance focus' and 'a holistic view of IS/IT security implementation'. Second, the chapter reviews the evolving perspectives on IS/IT security with regard to 'corporate governance, boards and senior management', 'IS/IT and business risk', 'corporate governance, IS/IT security implementation and adequate internal controls', 'empowering human capital through education, training and awareness' and 'creating a security culture'. The chapter ends by presenting other useful frameworks and regulations including the following topics 'the Committee of Sponsoring Organisations of the Treadway Commission (COSO)', 'Sarbanes-Oxley Act', 'the Health Insurance Portability and Accountability Act of 1996 (HIPPA)' and 'Malaysian Code of Corporate Governance'

Chapter 3 (Conceptual Framework) presents a conceptual framework covering specific issues relating to IS/IT risks governance, the formal, technical and formal dimensions of IT risk governance, internal controls for IT risk governance across the formal, technical and informal dimensions within the directing and monitoring actions. Then, a model of IS/IT security governance is developed from a combination of those discipline areas. Finally Chapter 3 provides the main motivation of this study: the discovery of the risk governance and internal controls management practices in Malaysian corporations.

Chapter 4 (Model of IS/IT security governance) The model was developed further based on Chapter 3. The chapter discusses substantial reviews of the role of boards and senior management within the formal, technical and informal components. Firstly, the model prescribes the elements of the three components of formal, technical and informal. Secondly, the model converts the interaction among the three components into three types of relationships, Relationship Type 1-Formal/Informal, Relationship Type 2-Formal/Technical and Relationship Type 3-Formal/Technical. Later, risk

management and internal controls over the three components and component interactions are discussed, including the directing and monitoring actions. Finally, comparisons are made between the IS/IT security governance model and the other existing security models.

Chapter 5 (Research Design and Methodology) justifies why the triangulation approach was selected in this research methodology. In this chapter, the combination of qualitative and quantitative methods used to acquire data for answering research questions posed in this study are described.

The data analysis chapters present the results of web data, interview data and survey data. The results of analysis are presented in four chapters, Chapter 6 (Web Analysis), Chapter 7 (Leximancer Software Analysis), Chapter 8 (Manual Content Analysis) and Chapter 9 (Survey Analysis).

Chapter 10 (Conclusions, limitations, further research and recommendations) reports the major conclusions in this study. The major conclusions address whether the data supported the model and research questions of this study. The chapter also provides the limitations and further research and recommendations.

Chapter 2: Literature Review

2.0 Introduction

Identifying the literature specific to this topic was quite difficult. There are numerous journal articles, conference papers and books relating to IT/IS security but a library search in that field revealed few specifically on this topic, although several authors made passing references to corporate governance. There are also substantial bodies of literature relating to security, internal control and corporate governance in the business disciplines such as management and accounting. However, again, library searches revealed very few articles, conference papers, etc. that dealt specifically with matters relating to IT/IS security.

The material identified as relating to IT/IS security and to corporate governance was read and promising references in the bibliographies of the documents were followed up. It was disappointing to discover that a very high proportion of the literature reviewed in IT/IS and in the relevant business disciplines was technical, theoretical or merely statements of opinion; very little of it was supported by empirical investigations of any kind. As a consequence, assessing (critiquing) the validity of these statements was very difficult.

As noted elsewhere in this thesis, the preponderance of technical or opinion pieces indicated a general malaise and indicated some topics that could be investigated but did not present any models that could be tested. Also, because of their nature, these papers gave no indications of methodologies or data-collection methods that were likely to be successful in this field.

Thus, what follows is perhaps better described as a report on the relevant literature rather than as a severe critique of competing models. However, some of the opinions and suggestions are utilised in Chapters 3 and 4 which are devoted to the development of a model for IT/IS security governance.

IS/IT security has become an essential part of business activity over the past three decades. This has come about in an attempt to ensure that confidentiality, integrity and availability of IS/IT assets and business information are in place. Some authors claim that due to lack of security awareness, the board and senior management do not understand the real IS/IT security problems faced by the lower levels relating to confidentiality, integrity and availability (Posthumus et al., 2004). With lack of security awareness, the interaction between the top to lower levels and the bottom such as operational level to upper level, creates a gap. The IS/IT security problems are referred to when the confidentiality, integrity and availability of IS/IT assets and business data have been compromised (Baskerville, 1988).

Today, the responsibilities and the roles for IS/IT security are no longer dominated by IT personnel. Rather there is now a broader integration of specialists in decision making since IS/IT applications have been used as a strategic tool for achieving business goals.

2.1 The Need for IS/IT Security

Businesses today rely on their IS/IT to conduct day-to-day activities. If IS/IT systems and business data are compromised, this could lead to corporation's financial losses and non-financial losses such as corporate embarrassment (Williams, 2007). However, the author did not conduct any empirical studies to support this argument.

Businesses also undertake strategic planning for creating value from IS/IT. For example, the implementation of an Electronic Resource Planning (ERP) system in organisations requires strategic planning. This planning aims to bring some benefits (O'Leary, 2000) such as:

- provides integrated systems by sharing data across various departments including between sales and marketing, production, operations, shipping, financial and purchasing departments;
- streamlines business processes and workflows;
- improves efficiency and productivity levels;
- lowers costs (ERP systems use two databases); and
- improves customer service.

However, the huge investment in IS/IT such as ERP has exposed organisations to IS/IT risks, including the security vulnerabilities of IS/IT. The protection of critical IS/IT used in business has grown in importance with the rapid development of business transaction applications such as ERP. Attention to the security of IS/IT has increased in importance. This is because of the need to offset vulnerability to attacks that could result in direct losses and indirect losses to business.

Direct financial losses may result when security is breached (Su, 2006). As cited by Su (2006), the CSI/FBI conducted a survey for the 639 respondents who have experienced using computer systems and reported that the total losses for 2005 were about US\$130 million which averages about US\$203,000 loss per respondent. Importantly, Su (2006) has developed a conceptual framework for achieving the relationships between business vision, critical impact factors and business drivers. But in Su's paper the relationship between business vision, critical impact factors and business drivers was illustrated using examples only and no data collection was conducted in validating the framework.

Indirect losses could compromise “*public reputation, brand image, goodwill in the market place, public and customer confidence in the accuracy of reporting, fraud resistance of business activities and the ability to meet the requirements of the regulators*”(Farahmand et al, 2003, p 350). According to Farahmand et al (2003), indirect costs are more serious than financial losses because these hidden costs are difficult to quantify. Farahmand et al developed a scheme for assessing possible damages caused by indirect costs but no empirical data supported this paper.

As a result of a huge investment in IS/IT, organisations need to identify, assess and mitigate the risks created by IS/IT just as they do with other organisational business risks to minimise business losses. In the report of Corporate Governance Task Force (2004) entitled, “*Information Security Governance: A call to action*”, risk is critical to businesses which primarily depend on IS/IT for supporting business operations. The high intensity use of IS/IT has lead to more vulnerability attacks and threats exposure to corporation’s business assets, resources and data. This has become a concern to organisations because an active vulnerability reflects a threat resulting from reliance on IS/IT applications (e.g., hardware and software), people and formal procedures (e.g., security policy, standards).

Over the last 30 years, there have been changing perspectives and trends on IS/IT security practices among corporations. The adoption of new practices such as IS/IT security controls, IS/IT security standards and governance focus was not only the result of technological and organisational dimensions but also of the human dimension. Therefore, the following sections will review the literature on incidents, vulnerabilities and threats, IS/IT security controls and security standards, governance focus for IS/IT security and a holistic view of IS/IT security implementation.

2.2 IS/IT Security Incidents, Vulnerabilities and Threats

This section will review the trend of IS/IT security incidents, vulnerabilities and threats from the 1970s until 21st century which encouraged corporations to adopt new practices to overcome IS/IT security issues.

An IS/IT security incident is a violation or imminent threat of violation of IS/IT security policies or standards of IS/IT security practices (Wiant et al, 2005). In the early part of the computing era in the 1970s, IS/IT security incidents were mainly associated with technical issues of computer systems such as operating systems (Madnick et al, 1973), access to computers and flow of information between or within a computer (Landwehr, 1981). The Formal Methods of Computer Security was

developed by Landwehr (1981) in order to improve “multi-level” mode, where some information on computer systems may have a classification higher than some computer users. Technical issues have caused some IS/IT security incidents since about the 1970s, which were the result of unresolved organisational vulnerability that led to attacks on IS/IT applications.

In the early 1980s the major cause of IS/IT security incidents was the design and development of IS/IT.

IS/IT security incidents were commonly the result of poor system design opening the systems to a variety of attacks including computer viruses (Fites, 1989), computer fraud (Dixon, 1992) and computer hacking and cracking (Hafner et al, 1991). Hafner et al (1991) stated that, in the 1960s to 1970s, a computer hacker was a respected and honoured person: he worked forty hours and stayed late just to refine a program until it could not be refined any more. But, in the early 1980s, the hacker was no longer a benign explorer but a malignant intruder.

Wood (1990) has proposed the principles of security design into the creation, enhancement and maintenance the IS/IT systems by computer system designers and system analysts. According to Wood, the lack of teamwork between system users, developers, experienced IS/IT auditors and IS/IT security specialists in the IS/IT development process has constrained the system development procedures. As noted by Wood, proper categorisation of controls is needed to facilitate the selection of controls from each category.

Vulnerability exists when the IS/IT no longer functions in the way intended (Bishop, Mate. et al, 1996). Bishop et al developed a technique to find vulnerabilities on the IS/IT systems and classified vulnerabilities into six categories, namely, nature of the flow, time of introduction, exploitation domain of the vulnerability, the effect domain, minimum number of components to exploit vulnerabilities and the source of the identification of vulnerability.

A defect, flaw or bug in the code of any program is an example of vulnerability which, if it is exploited, can lead to the failure of confidentiality, integrity and availability (Radianti, 2007).

The process of identifying the vulnerability is not a simplistic task due to the complexity of IS/IT applications, the number of potential vulnerabilities and their complexity (Bazaz et al, 2007). It has been reported in the literature that software vendors and corporations have offered rewards for

reported software bugs (Radianti, 2007). The reward system for the reported bugs is one way that organisations have started to deal with risk that is caused by IS/IT.

However, if not monitored effectively by the board and senior management, software vulnerabilities may expose business IS/IT assets and business data to risk. Even though the reward system for the reported bugs was efficient, Radianti (2007) argued that there is a “black market” for software vulnerabilities. To investigate how the “black market” was circulated, Radianti developed a system dynamics model to study the growth of the vulnerability black market. On the demand side, the system dynamics model by Radianti (2007) enabled users to detect the group of people willing to pay for secret knowledge about new vulnerabilities. While on the supply side of the system dynamics model, the hackers who developed scripts for malicious codes would sell the whole package to the highest bidder.

A presence of vulnerability in an IS/IT system encourages attacks to IS/IT applications potentially from malicious misuses such as social engineering attacks and the vulnerability software black market. Whitman (2003) highlighted the two most prioritised strategies that need to be conducted within organisations: first, is to understand the threats facing the IS/IT assets and business data and information; and second, to rank the identified existing threats in order to enable organisations to prioritise the threats according to the IS/IT security vision.

To understand better how the real organisations rank and prioritise the threats, Whitman (2003) conducted an online survey of IT executives including IS/IT Directors, Managers, Supervisors, Executive IS Directors like Chief Information Officer and Chief Technical Officer. According to Whitman (2003), respondents were asked: first, to evaluate each threat category on a scale of ‘very significant’ to ‘not significant’ and second, to identify the top five threats to their organisations. The results of the study have shown that the following threats were ranked in the top five; Deliberate Software Attacks (Rank No.1), Technical Software Failure or Errors (Rank No.2), Act of Human Error or Failure (Rank No.3), Deliberate Acts Espionage or Trespass (Rank No.4) and Deliberate Acts of Sabotage or Vandalism (Rank No.5). Clearly, the top five threats which were identified by Whitman (2003) suggest that the threats caused by human aspects (e.g., deliberate software attacks, act human error or failure, deliberate acts espionage and deliberate acts of sabotage) have predominantly triggered IS/IT security problems within organisations if compared with technical deficiencies (e.g., technical software or hardware failure).

If the Board and senior management understand more about the vulnerabilities and threats facing the organisation, this would help them to align security needs, prioritise threats and business vision. Business corporations should consider all forms of vulnerabilities and threats as potential risks that could degrade IS/IT. Vulnerabilities and threats need to be identified and addressed effectively to ensure that risks to organisational IS/IT are minimised (Farahmand et al, 2003).

Today, computer-based IS/IT systems are linked to the internet, a public network accessible by all. The online survey conducted by Whitman (2003) has provided evidence that many respondents used the Internet to support their business operations. Whitman (2003) showed that respondents used the Internet for the following purposes:

- 95% of survey respondents extensively used Internet to provide information;
- 81% use Internet to collect information;
- 60% to advertise;
- 55% to provide customer service;
- 46% to support internal operations;
- 45% to order goods and services;
- 38% to provide technical support;
- 36% to connect remote sites;
- 32% to extend internal networks;
- 27% to integrate value chain partners;
- and 18% to collect orders.

Interestingly, the online survey conducted by Whitman has shown that almost half the respondents use the Internet for supporting their internal operations. The higher the IT/IS systems being used by an organisation, the greater the exposure to attacks.

Nowadays, with the extensive use of Internet, the IS/IT systems and business data of organisations are exposed to security attacks and anonymous potential threats. Table 2-1 shows the ranking of threats relating to IS/IT security, where the most dangerous threats were predominantly caused by people's action. In Table 2-1, the majority of threats over IS/IT systems caused by people's action are serious. Therefore, a great amount of understanding about security problems and its impacts is crucial at the board and senior management level. Failure to understand the security threats and

vulnerabilities would lead to ineffective IS/IT security solutions, which may cause corporate risk management failure in dealing with security risks.

Threat Category	Weighted Ranking
Deliberate Software Attacks	2178
Technical Software Failures or Errors	1130
Act of Human Error or Failure	1101
Deliberate Acts of Espionage or Trespass	1044
Deliberate Acts of Sabotage or Vandalism	963
Technical Hardware Failures or Errors	942
Deliberate Acts of Theft	695
Forces of Nature	611
Compromises to Intellectual Property	495
QoS Deviations from Service Providers	434
Technological Obsolescence	428
Deliberate Acts of Information Extortion	225

Table 2.1 Ranking of threats to IS/IT security (Whitman, 2003, p 93)

Technological advancements have allowed corporations to adopt the internet to perform a range of business activities across time, space and organisational boundaries, such as E-Commerce and ERP applications. Software providers have enabled businesses to perform online services that use portals, web-based hubs, online market-places and industry-specific trading communities (Englund et al. 2000).

The increasing dependence on internet connectivity and capabilities has increased the scope of vulnerability since the internet-based IS/IT applications can be accessed from various sources both internal and external (Nachtigal, 2007). A model of a new Security Paradigm for E-Business developed by Nachtigal (2007) addresses the old parameters to the alternative one, which is called a process-based security paradigm. There are six sequential steps in the Security Paradigm for E-Business, namely, 1) business issues and definition, 2) business logic definition, 3) E-Business process security objectives analysis, 4) security designs, 5) security test and 6) the final security design. Importantly, the first step

of security paradigm has a similar concept to IS/IT security governance. The first e-process is identifying business issues and definitions and this stage is crucial for organisations because if the board and senior management do not understand the business goals and the business processes, the implementation of any security controls or security counter-measures would be less effective and less efficient.

Internal users can be referred to as personnel or authorised users normally engaged in supporting business operations (Farahmand et al, 2003). They may be considered as a threat when they exceed their privileges or authorities or commit errors. External users can be defined as anyone who is not engaged in supporting operations. They impact the productivity of the system either overtly or covertly (Farahmand et al, 2003). The variety of incidents and threats that have occurred in the past indicate potential threats to the security of IS/IT. These threats may increase the risk faced by organisations if the vulnerability is not addressed by their staff.

Since the internet has come to be increasingly used for commercial purposes, threats which reflect IS/IT vulnerability have continued to increase in both sophistication and magnitude (Ahlgren, 2005). Ahlgren (2005) identified several types of new computer security vulnerabilities such as foreign cyber attacks- a politically motivated IT attack, identity theft, cyber crime, phishing, malicious code, viruses, trojans, denial-of-service, spam, spyware, adware, botnets and web application attacks and mobile attacks.

The accessibility of corporate internet applications has exposed them to attack from external and internal sources, which may not be controlled by ineffective security policies. The ineffectiveness of security policies may result from technical deficiencies and has become clear now from deficiencies in the implementation and adaption of the policies. Inadequate governance control on the personnel responsible for IS/IT security policies, standards and procedures is increasingly being recognised as the main cause of these deficiencies (Dhillon et al, 2001). Dhillon et al. (2001) analysed the socio-philosophical aspects for understanding the IS/IT security domain using the interpretative paradigm of Burrell and Morgan (1979). Moreover, Dhillon et al also reviewed and identified the trend of IS/IT security directions to a greater holistic view, not from a narrow technical viewpoint only.

2.2 IS/IT security controls and security standards

a) IS/IT Security Controls

Having IS/IT security controls and security standards in place does not mean that the security of IS/IT is well managed (Baker, et al. 2007). As reviewed by Baker et al. (2007), previous studies were predominantly focused on the presence or the absence of security controls or security procedures but not on the quality of implementation. To understand better how the IS/IT security procedures have been implemented in managing IS/IT assets and business information security risk, Baker et al. (2007) has designed a web survey addressing 16 categories of general security domains. These 16 categories by Baker et al (2007) are presented in Table 2-2.

GENERAL SECURITY CONTROL DOMAINS	NUMBER OF CONTROLS
Antivirus software	4
Back-up and recovery	5
Business continuity/incident response	5
Employee training and awareness	6
Help desk/IT support training	4
Staff hiring and termination	4
Monitoring and logging	4
Network auditing and logging	6
Network security management	6
Passwords and access control	4
Physical security	9
Remote access security	4
Sensitive data handling and protection	6
System-level security	4
Technical documentation	4
Testing and review	5
Total	80

Table 2.2 Major security domains and number of controls (Baker et al. 2007)

Interestingly, the 16 general security control domains covered the three components of Technical, Formal and Informal. For example, controls like Antivirus software, back-up and recovery were identified as the Technical component. The examples of General Security Control Domains for Formal component are business continuity and incident response. While the Informal component was not represented exclusively by any of the 16 categories, it is presumed the Informal component has been incorporated within the implementation of both Technical and Formal components.

The demographic findings by Baker et al (2007) were that there were 349 respondents participating in the web survey which included Information Security Executives, Managers and Technical Specialists. The results show that the 10 top security domains were rated the highest in respect to implementation quality such as anti-virus software (technical), back-up and recovery procedures (operational), system level security procedures (technical) and accessible technical documentation (management). However, the lowest implementation quality ratings were predominantly presented by the management category such as Help desk/IT support training, business continuity/incident response, monitoring and logging procedures. The survey results have indicated that implementation quality was affected significantly by organisation size and industry. The study found larger organisations have bigger IT budgets for security controls and counter-measures. Industry type, like finance, was scored highly and education industry type, like education institutions, was scored lower for each of the 16 categories of general security domains, as identified earlier in Table 2.2 (Baker et al, 2007). Figure 2.1 shows the disparities among industry groups.

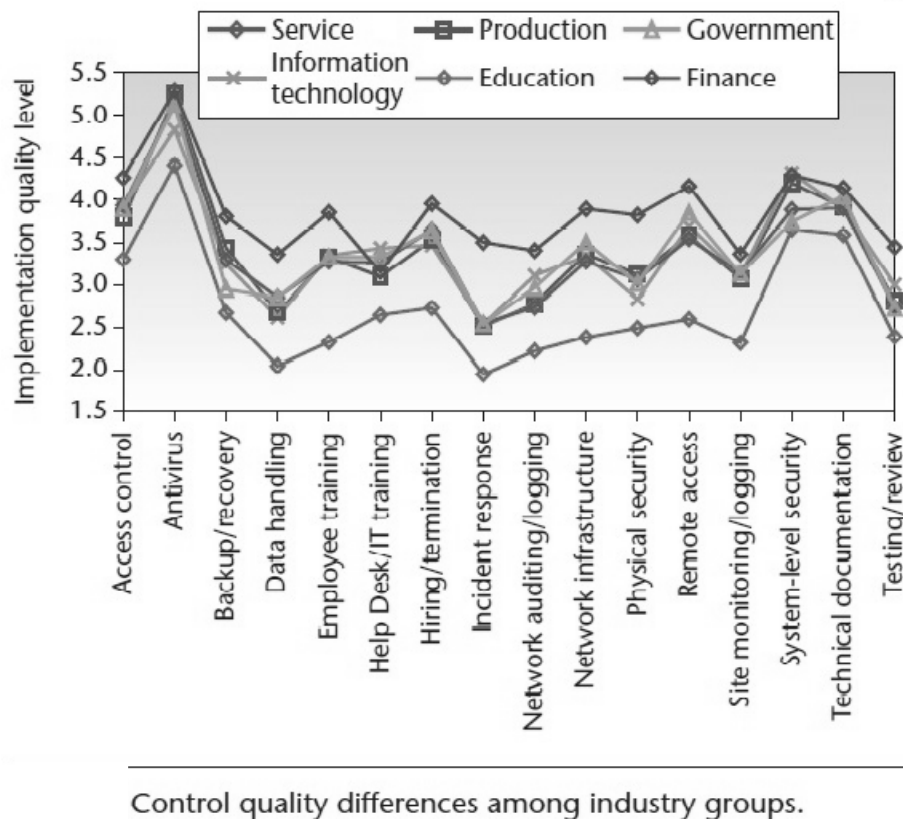


Figure 2.1 The security controls quality differences among industry groups (Baker et al, 2007, p 44)

For instance, the deployment of firewall technology is an example of an IS/IT security control that may be recommended by a security standard. However, the implementation of firewall technology is insufficient if there is no measure taken to assess how well the implementation is achieved by an organisation. The function of IS/IT security controls is to shield corporate vulnerability from various attacks from internal and external sources. If the IS/IT security control is not functioning well and IS/IT may be vulnerable and so increase business risk.

While IS/IT security controls provide security counter-measures, IS/IT security standards provide proper requirements which should be followed within the organisational IS/IT Security Policies and Procedures.

b) IS/IT Security Standard-17799/BS7799

The 17799/ BS7799 is an international standard for security management that can be used by small to large organisations. Historically, it was published by the British Standards Institution (BSI) in 1992 as an Industry Code of Practice. In 1995, the Code was up-graded to the UK Standard level, BS 7799. And finally in 2002, the standard was internationally recognised as 17799/ BS 7799-2:2002. The history has shown us the dramatic changes in the evolution of 17799/ BS 7799 over several years.

The purpose of the standard is to provide a framework for organisations in order to examine and improve the security of IT systems environments. In nature, the 17799/BS7799 standard is a comprehensive and risk-based approach. It allows organisations to decide the security needs (e.g., in terms of Control Objectives) which are based on the risk assessment they have conducted.

The 17799/BS7799 has covered ten key security areas including the scope of the standard, as follows:

1. Area: Security Policy

Standard: Demonstrate the management commitment to, and support for, IS/IT security.

2. Area: Organisational Security

Standard: Develop a management framework for the coordination and management of IS/IT security in the organisation: allocate IS/IT security responsibility.

3. Area: Asset Classification and Control

Standard: Maintain an appropriate level of protection for all critical or sensitive assets.

4. Area: Personnel Security

Standard: Reduce the risk of error, theft, fraud or misuse of computer resources by promoting user training and awareness regarding risks and threats to information.

5. Area: Physical and Environmental Security

Standard: Prevent unauthorised access to information processing facilities and prevent damage to information and to the organisation's premises.

6. Area: Communications and Operation Management

Standard: Reduce the risk of failure and its consequences by ensuring the proper and secure use of information processing facilities and by developing incident response procedure.

7. *Area:* Access Control Security

Standard: Control access to information to ensure the protection of networked systems and the detection of unauthorised activities.

8. *Area:* System Development and Maintenance

Standard: Prevent the loss, modification or misuse of information in operating systems and application software.

9. *Area:* Business Continuity Planning

Standard: Develop the organisation's capacity to react rapidly to the interruption of critical activities resulting from failures, incidents, natural disasters or catastrophes.

10. *Area:* Compliance

Standard: Ensure that all laws and regulations are respected and that existing policies comply with the security policy in order to ensure that the objectives laid out by senior management are met.

These ten areas of 17799/BS 7799 have covered many facets which range from technical, human, legal to business survivability.

Entrust (2003-2004) reported that the ten IS/ITO 17799/ BS7799-2:2002 chapters (which include 127 elements) were exclusively used by the Boards, the CEO, the CIO and the business unit executives in order to know the state of an organisation's IS/IT security, identify the top security issues and see the security progress made since the last reporting for future plans action.

Studies have shown that 17799/ BS 7799 offered several benefits to organisations. The many facets of 17799/BS 7799 have gained attention among businesses internationally to employ the standard. The standard, 17799/ BS 7799-2:2002, is seen as the best reference framework for IS/IT security management as it offers the combination of comprehensiveness and international level of acceptance within a business (Entrust 2003-2004). It is important to highlight that 17799/ BS7799-2:2002 is one of the standards which allow organisations to undergo a third party audit and become certified (Germain, 2005). Furthermore, Germain has compared 17799/BS7799 with several other

existing standards and the results of comparison indicated that only two standards, 17799/BS7799 and Common Criteria for IT Security Evaluation (ISO 15408), offered certification to organisations. While ISO15408 provides certification rather on the technical aspects of information systems, 17799/BS7799 covers a wider aspects of organisational and administrative matters.

Ezingear et al. (2005) found that 17799/ BS7799-2:2002 was primarily used as a marketing tool to generate customer confidence and attracted investors with well established procedures.

Businesses around the globe started to adapt 17799/ BS 7799-2:2002 as an IS/IT security standard. It is widely used by international organisations in places other than the UK such as Asia (including Japan, China, India, Taiwan, Korea), Australia (Waloff, 2002), Europe (including Germany, Italy, Netherlands, Finland, Hungary, Ireland, Norway, Sweden) (Osborne, 2006; Ezingear, 2005) and North America (Entrust 2003-2004).

However, 17799/BS7799 standard has limitations. The 17799/BS7799 standard is concerned with the existence of the processes rather than how effective is the implementation achievement of the goals towards the processes (Siponen, 2006). It focuses on the existence of processes rather than on how well the processes or activities are being accomplished. For instance, promoting user training and awareness regarding risks and threats to information is an example of IS/IT security standard. Organisations put more emphasis on setting up the training and awareness programme than ensuring the process achieves the procedures, regulations or laws and achieves the goal of IS/IT security. This may be due to insufficient internal controls over the standard processes. Since IS/IT security issues are predominantly social and people problems (Dhillon et al, 2000), adequate internal controls over the IS/IT processes are crucially important.

A limitation of standards arises from a compliance-led approach which has influenced the way people implement IS/IT security in organisations. A simplistic, compliance-led approach is not effective for IS/IT security because IS/IT security is not only a technological problem but also a social and organisational problem (Dhillon et al., 2000). It has been identified that the three security principles, namely, confidentiality, integrity and availability, were limited and applied to technical perspectives only, they were not applied to organisational and social aspects. Dhillon et al (2000) extended the security principles definition to human aspects including responsibility, integrity of people, trust and ethicality. However, no research and empirical study were conducted by Dhillon et al (2000) to validate the claim because it was rather a Technical Opinion paper.

As IS/IT security involves many disciplinary areas, the board and senior management have to be able to put in place effective mechanisms through IS/IT security controls and IS/IT security standards. An effective mechanism which is internal controls can be used to ensure the placement of IS/IT security controls and standards at any level within the corporation to achieve the corporation's goals. There is a lack of studies that emphasise how IS/IT security controls have been achieved, communicated and reported between and among the board, senior management and all employees.

2.3 IS/IT Security Requires a Governance Focus

In effective corporate governance, boards and senior management direct and control organisational IS/IT assets, resources and data to ensure their business objectives are achieved as intended. They need to ascertain if IS/IT security risks are managed appropriately including those of corporate IS/IT (Information Security Governance, 2006). In 2006, the IT Governance Institute published a report relating to Information Security Governance, which provides guidance to the Board and Senior Management and IT Security Professionals to assist them in IS/IT Security Governance responsibilities. Many IS Security Professional, Senior Managers and Academics from various industries and many countries such as USA, Britain, Canada, Austria, France, Italy and Australia, were involved in the publication. But, even though internationally recognised, it was rather a guidance and educational resource from a professional body, the IT Governance Institute, than a standard and the report did not include any empirical study for the validation process.

For many years, IS/IT security responsibilities have been dominated by IT people where IT people made decisions over IS/IT security including recognising, preventing and reacting to any threats to corporation's IS/IT (Solms, 2001). Solms has linked the logical relationship between information security and corporate governance. In corporate governance, the board and senior management who are accountable for the success or failure of organisations must be responsible for IS/IT assets and data but the paper was rather a technical opinion, there was no empirical research conducted to gain knowledge in the field.

Today, the responsibilities for security of IS/IT and the confidentiality, integrity and availability of information are involved by all three levels of activity in a company, the model of the Direct Control Cycle built by Solms covers strategic, tactical and operational management levels from the top to the bottom levels (Solms, 2006). As can be seen in Figure 2-2, across the three management levels, there are three distinct actions—Direct, Execute and Control- which take place in this model

because the core principle of corporate governance is *checks* and *prescribes* where the board and senior management are responsible for the key success or failure of a corporation.

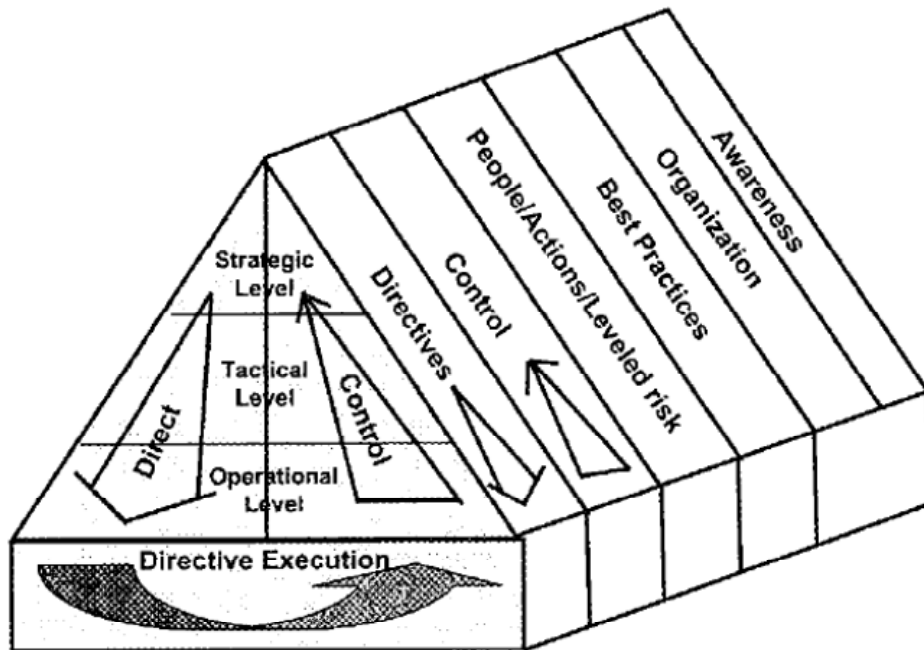


Figure 2-2 The model of Corporate Governance Direct Control Cycle (Solms, 2006, p 409)

The need for effective IS/IT security implementation and practice in corporations has been discussed in the literature for over a decade. The application of an effective mechanism of internal controls is necessary to measure the success or failure of certain IS/IT security controls. However, a mechanism of internal controls can be achieved through good corporate governance. Good corporate governance is critical for IS/IT security as it works through a top -down approach and confronts the corporation at the board and senior management level (Solms, 2001). Use of a top-down approach is useful for boards and senior management to create a security culture among all employees through IS/IT security policies, standards and procedures. Few articles have emphasized that IS/IT security requires a governance focus since IS/IT security is not solely a technical issue but also a governance (social and organisational) challenge (Conner B, et al. 2003; Solms, 2006).

Recent regulations such as the Sarbanes Oxley (SoX)(2002) and the Malaysian Code of Corporate Governance (2000) have been put in place as compulsory requirements for good business

practice in publicly listed companies in the USA and Malaysia. The implementation of SoX in the USA has positively changed the landscape of information security practices in US Stock Exchange Companies, after an empirical study conducted by Gordon et al (2006). The findings by Gordon et al show that the activities of IS/IT became more focused after the SoX was enacted. Boyle et al (2007) highlighted that even though SoX has some beneficial impacts it increases the costs to organisations such as auditing costs, governance and human capital costs and it lowers the investment by investors because of risk -taking concerns.

The aftermath of the 97/98 financial and economic crisis in East Asian countries forced the Malaysian Government to pass a new regulation on good corporate governance practices in 2000, the so-called Malaysian Code of Corporate Governance where the boards are responsible to manage corporate risks including the adequacy and integrity of company's internal control and management of information systems. The Malaysian Code of Corporate Governance places responsibility on the boards to manage corporate risks including those risks associated with the operation of the infrastructure. Minimising exposure to risk including identifying threats and acting to minimise exposure to vulnerabilities has become a major priority of the corporate boards of the publicly listed companies in the *Bursa Malaysia*. Up to date, there has been no empirical research to study the implications of the Malaysian Code of Corporate Governance implementation over IS/IT security.

Good corporate governance mechanisms are relevant to the practice of IS/IT security as they provide governance structure in corporations, as discussed next.

From a good corporate governance perspective, organisations have the capacity to direct IS/IT security on security matters like an organisational structure, roles and responsibilities for IS/IT security, all relate to IS/IT security (Williams, 2007). As highlighted in Williams' article, a corporate risk function (such as risk management, policy management, business continuity and incident response) is a vital need in the organisational structure for IS/IT security. This is because each employee is responsible to ensure that IS/IT are preserved against attacks.

Posthumus et al (2006) developed a framework which addresses the roles and responsibilities of individuals in corporations (Posthumus et al, 2006). Posthumus et al (2006) proposed that more integration of different specialists across departments is crucially needed to achieve IS/IT security governance. Even though the Posthumus et al framework was still at the theory grounding stage Posthumus et al had successfully addressed the importance of mutual interaction and consistent

security practices throughout departmental or sectional levels. However, if the board and senior management still do not understand their IS/IT security culture, security problems and their impacts, Posthumus's IS/IT security framework would not be beneficial to their organisations, no matter how comprehensive the Posthumus framework. This is because the Head of Department or Section in the organisation has a better understanding of the security culture and security problems, it is believed that, highlighting the mutual interaction between departments and sections in the organisation, needs to be taken care of (managed) and internally controlled (monitor).

While the roles and responsibilities of IS/IT security involve diverse people at different levels, Posthumus et al highlighted that an active involvement of the board and senior management is still critical to achieve IS/IT security governance. Posthumus et al have identified some of the roles that individuals need to play to resolve IS/IT security problems. The diversification of people and levels would bind them together collectively, requiring the involvement of the board, the CEO, line management, the CIO and his team, risk managers, audit committee members, security committee, auditors, compliance officers and all people within a corporation. As this framework was theoretically grounded, Posthumus et al did not draw on knowledge from the field.

Having clear roles and responsibilities for IS/IT security within an organisational structure helps business when dealing with IS/IT risk. Through an effective governance structure, the board and senior management will be able to minimise IS/IT risks by applying a mechanism of internal controls for measuring the success or failure of IS/IT security implementation.

2.4 An Holistic View of IS/IT Security Implementation

An holistic view of IS/IT security arises when IS/IT security is considered from two perspectives: the integration of different specialists; and a particular view of the nature of IS/IT security.

The first perspective requires the integration of different specialists including the corporate board, senior management and technical people to achieve an effective IS/IT security policy (Williams, 2007). In his technical opinion, Williams (2007) highlighted that the traditional IS/IT security function was no longer relevant in the new e-business trend, more integrated different functions are needed to identify, assess and mitigate the security risks including threats and vulnerabilities related to IS/IT assets and business information. A generally applicable framework for an organisational structure of responsibilities was established by Williams, depicting the security responsibilities of an Audit

Committee, Chief Executive Officer (CEO), Chief Information Security Officer (CISO), Chief Information Officer (CIO), Board roles, Human Resource Director, Non-Executive Directors and other directors. However, the William's framework was developed according to industry practices and was influenced by his important role in Information Systems Audit and Control Association (ISACA) and IT Governance Institute.

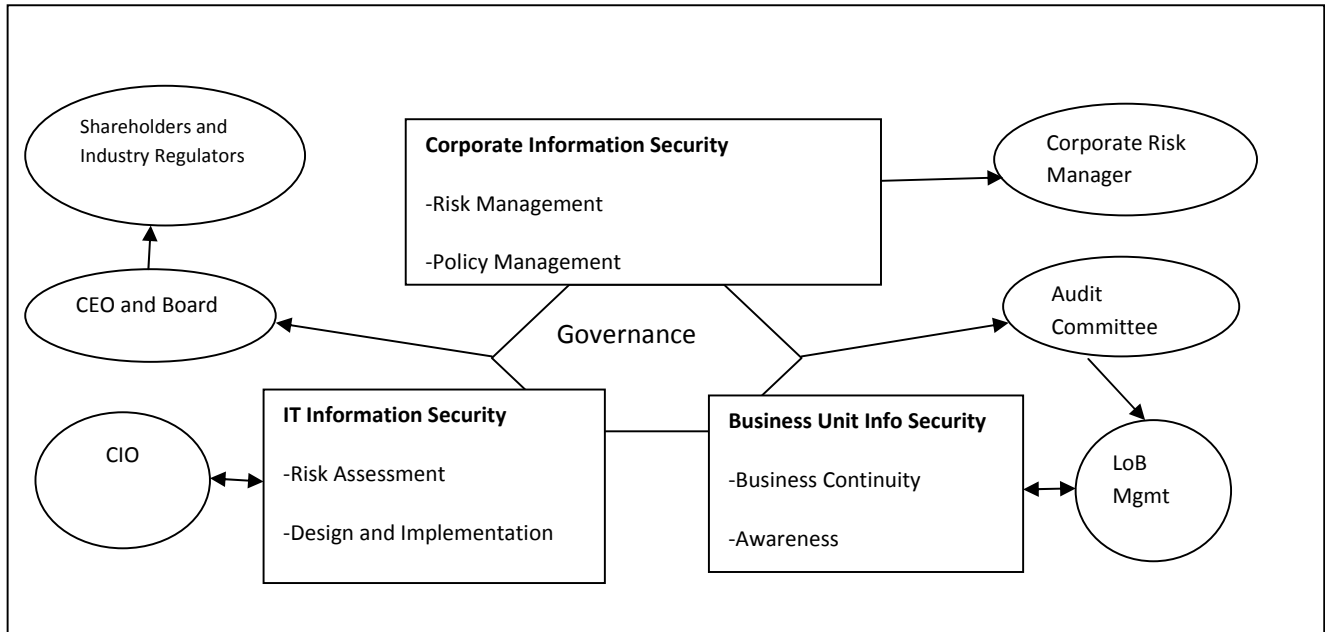


Figure 2-3. Organisational structure for IS/IT security (William, 2007, p 13)

IS/IT Systems have to be driven by people working together with other organisational employees at a broad level to accomplish a coherent IS/IT security implementation (Backhouse, J et al. 1996). Integrating different experts to achieve the common goal of IS/IT security is a challenging task because governance aspects such as culture and power need to be considered.

The informal component such as culture of the organisation plays a significant role in achieving IS/IT security governance and exclusively addresses the IS/IT security problems and issues. Culture creates differences where people tend to reject people who are different, such as management versus labour, field versus corporate and line versus staff (Labovitz et al., 1997). IS/IT security governance would not be successful if the board and senior management do not really understand the real security problems of an organisation which lead to bad security culture practices. Millions of IS/IT security problems relating to culture can be found in an organisation. For example, some employees do not read, understand and be aware of the security policy because the existing culture on security was not

entirely cultivated in the organisation. To address the culture differences and gaps among divisions, it is recommended that the security policy wordings should be read and understood by all employees and the job responsibilities have to be exclusively defined.

One of the impediments to creating an IS/IT security culture in organisation is the attitude of staff (Gaunt, 2000). Gaunt believes that the attitude of staff could be changed through formalised procedures and effective monitoring style by the board and senior management.

The second perspective is to view the nature of IS/IT security from three levels: the formal, informal and technical levels (Mishra et. al., 2007). The following description of the three levels is based on the work by Mishra (2007). The extended conceptual framework, Cyclical Nature of Information Systems Security Governance of Three Levels by Mishra was sourced originally from the “fried-egg” analogy for Information Systems Security developed by Dhillon in 2007. The formal level of Mishra’s conceptual framework focuses on how the corporation institutionalises organisational aspects such as IS/IT security policies, controls, culture, group behaviour and leadership style. On the other hand, the informal level covers personnel and human aspects of IS/IT security such as norms, values, personal beliefs and ethics, which lead to the acceptance of IS/IT security practices within businesses. In the technical level, formal controls are exercised through rules, procedures, operational details, monitoring and feedback of the security implementation. However, Mishra did not provide specific methods and guidelines showing how the feedback reports were assessed at the technical level (e.g., the IS/IT systems are working or not working), over the system implementation in the area such as operating systems, computer access, resources and the design and development of IS/IT.

Researchers have shown that many IS/IT security research studies were focused on the technical issues (Siponen, 2007). However, the IS/IT security literature on the informal aspects has received little attention from IS/IT security researchers.

A growing number of security researchers and practitioners has seen that human issues such as ethics problems, culture, social problems, human error and ignorance can jeopardise businesses that depend on IS/IT. Many IS/IT security technologies have been in place in organisations to control security risks such as security incidents but IS/IT security controls do not reduce information risk effectively (Blakley, 2002). This is because security problems are not merely technical problems but rather a more holistic perspective considering also organisational and human aspects.

2.5 Evolving Perspectives on IS/IT Security

2.5.1 Corporate Governance, Boards and Senior Management

Corporate governance comprises two important aspects, namely, directing and controlling (King Report, 2002; Solms et al., 2006). The first aspect, directing, is the process of providing strategic guidance on the way corporations should operate which normally happens via corporate policies, standards and procedures. The second aspect, controlling, is the process of ensuring corporations achieve their business goals, policies and procedures and comply with the country's laws and industrial regulations. Any form of security planning must reflect corporate governance characteristics.

The two aspects of governance, direction and control, can be used effectively to minimise the IS/IT risk (Solm, 2006). The Information Security Governance model by Solm (2006) explains that significant Direct and Control actions occur at all management levels including the Strategic Level, Tactical and Operational Level. However, as mentioned before in Solms (2006) paper there was no exploration on experience gained from the field to prove the said model.

Corporate governance practice within IS/IT security implementation is in demand. These were justified by the following IS/IT security researchers (Kizirian et al. 2004, Knapp et al. 2006, Posthumus et al. 2005). IS/IT security today has attracted a great deal of attention from corporation boards and senior management in directing and controlling IS/IT assets and resources.

Kizirian (2004) conducted case studies to investigate the security controls and management tone in the firm's IS audit working papers, Kizirian has confirmed that management sets the tone and direction of an organisation.

A combination of qualitative and quantitative methods was used by Knapp et al (2006) to investigate if the management has an effect on security culture and policy. Two hundred and twenty certified IS security professionals had answered the open-ended questions for the theory grounding part of their research. After the qualitative survey was conducted, sixty-eight certified IS security professionals answered the web survey. It was evidenced in Knapp's study that senior management support is a significant predictor for cultivating a security culture and enforcing policies.

A framework for the governance of information security developed by Posthumus et al.(2005) addresses how information security should be handled at senior management level. Posthumus has clearly defined the scope and characteristics of business information risk. Due to e-business demands,

the scope of business information risk has been extended to private networks and the Internet, to secure the line of communication between the organisation and its customer, suppliers and business alliances. The characteristics of business information risk which were confidentiality, integrity and availability have been incorporated into their Information Security Governance model but the model was not proved within a real world environment.

As IS/IT security is part of IT governance, the board and senior management are responsible for directing and controlling the IS/IT assets and business data. According to the IT Governance Institute report in 2003, IT governance has five major strategic domains, namely, 1) IT strategic alignment, 2) IT value delivery, 3) IT resource management, 4) IT risk management and 5) IT performance management (ITGI, 2003). This research study is focused on the fourth domain, IT risk management, specifically looking into IS/IT security.

IS/IT security governance underlies the IT governance concept by aligning the investment in IS/IT business directions with the risk associated with IS/IT security of IS/IT assets. In IT governance, the responsibilities and authorities are exercised by the board, senior management and IT management in the formulation and the implementation of IT strategy (Van Grembergen, 2002). It is presumed that IS/IT security governance holds similar responsibilities and authorities as well to IT governance. The alignment among business directions and IT needs is crucial in IT Governance.

An integration of skills is needed because IS/IT are driven by people across the corporation. In overseeing the interests of the stakeholders, IS/IT security requirements of IS/IT should be recognised at the corporation's board level.

The report published by the IT Governance Institute relating to IS/IT security governance presents some essential guidelines for boards to follow (ITGI, 2006). For example, these are, first, to place IS/IT security on the board's agenda, second, to identify an accountable and supportive IS/IT security leader, third, to review and approve IS/IT security policy and last, to assign IS/IT security responsibility to a key committee. However, without a proper direction in risk management and internal controls within the organisation, particularly to IS/IT security, no matter how good the guidelines provided by the IT Governance Institute they would not be successful and effective. This is because the interactions such as the Formal and Technical, Formal and Informal and Formal and Informal relationships have not been comprehensively explored by IS/IT security researchers. Lack of this

interaction would lead to poor implementation in risk management and internal controls relating to IS/IT security.

There are two key personnel involved in IS/IT security governance, the Chief Executive Officer (CEO) and Chief Information Officer (CIO). In corporations, the CEO is an agent of the board and, therefore, the shareholders. The CEO has a broad responsibility for steering the corporation in making profits, driving revenue and building shareholder value through achieving business objectives and goals (Bassett, 2006). According to the Corporate Governance Task Force (2004), the CEO is responsible for reporting compliance issues to the board and advising the level of acceptable risk. The CEO must also report on weaknesses of current practices and suggest IS/IT security plans for improvements. A CIO is, however, responsible for addressing the business and legal perspectives in the entire IS/IT security function. For example, the CIO advises the CEO on strategic planning efforts in preserving confidentiality, integrity and the availability of information bases in corporations. In conclusion, IS/IT security governance requires clear responsibilities and roles for a range of personnel.

2.5.2 IS/IT and Business Risk

If the board and senior management understand the vulnerabilities and threats of IS/IT in their organisation, this would help the organisation to identify, assess and mitigate the risks effectively.

Identifying the corporation's risks such as vulnerabilities and threats at governance level alongside other risks faced by the corporation is important. This can facilitate the board and senior management in dealing with the potential effects on the organisation and consequent impacts that might flow through to shareholders, the share price and competition (Institute, 2004).

Control Objective for Information and Related Technologies or COBIT is an IT Governance standard which is primarily used as an educational resource for CIO, senior management, IT management and professional controllers (ITGI, 2005). In 1998, the IT Governance Institute (ITGI) established the publication of COBIT (now is version 4.0). The standard aims to ensure the following goals are achieved: IT aligns with business objectives, IT enables the business and maximises benefits, IT resources are used responsibly and IT risks are managed appropriately.

COBIT is a standard framework to be used exclusively for supporting IT governance (COBIT, 2000). COBIT is organised into four domains which are: Planning and Organisation; Acquisition and Implementation; Delivery and Support; Monitor and Evaluate. Across these domains, there are 34 high-

level control objectives and 318 detailed control objectives to be identified for IT governance -related initiatives.

Even though it is not exclusively used for IT Security, it addresses the broad spectrum of IS/IT security governance within a wider IT Governance framework (Solms, 2005). As can be seen from the preceding sections, IS/IT security governance is an integral part of corporate governance, it involves all issues including management and governance issues in relation to IS/IT security.

As reported in the publication of IT Governance Institute (2005), COBIT provides a range of benefits as follows:

- better alignment, based on business focus;
- a view, understandable to management, of what IT does;
- clear ownership and responsibilities, based on process orientation;
- general acceptability with third parties and regulators;
- shared understanding amongst all stakeholders, based on a common language; and
- fulfilment of the COSO requirements for the IT control environment.

Hardy (2006) has conducted one case study at Unisys, a large IT services corporation in the US. Unisys conducts business in more than 100 companies with 36,400 employees. Unisys adopted COBIT in 2003 to achieve a standardised IT strategy across global operations. After the implementation of COBIT, Unisys has revolutionised some key attributes including communication, quality, consistency, credibility and maturity (Hardy, 2006). The success of COBIT was evidenced in Hardy's study of the Unisys organisation. The major success of Unisys was the improvement of IT processes, where the board and senior management of Unisys had successfully aligned the IT infrastructure with the company business goals. The Informal component, namely, commitment from all management levels including the board and senior management, has been identified as one of the critical success factors. Hardy found that they were responsible and accountable in the IT processes.

Furthermore, COBIT covers the entire roles of organisational structure which range from the boards to data operators (Hardy, 2006). Even though COBIT does not specifically address IS/IT security COBIT has provided ways for IS security researchers and professionals to improve the effectiveness of IT implementation in organisations. Therefore, the COBIT framework has become a necessary reference for IS/IT security governance nowadays.

A researcher found that the COBIT standard also has limitations. The complexity of tasks such as *how things must be done* is not shown in the publication of COBIT. It is rather looking at *what must be done* (Solms, 2005). More detail about the complexity of the task including guidance is needed because it might help IT people to understand the technical orientation of COBIT.

Having IT standards in place has offered many benefits but it is still dependent on the IS/IT direction by the board and senior management, whether the goal is to manage the IT processes effectively and efficiently or only to comply. COBIT is just an example and can be used as a reference for achieving IT processes at all layers of management.

Risk is the probability that an undesirable loss may result from actions (or inactions) of the firm (Blakley, 2002). It is an event which could reduce the value of the business were it to occur.

IS/IT risk is the same as any other business risk and needs to be taken seriously as the consequence of failure can involve substantial loss (Straub, 1998; Blakley, 2002; Radianti, 2007). The risk arising from security vulnerability of IS/IT should be addressed in a pragmatic and effective fashion as vulnerability opens the door to threats and attacks on the IS/IT.

The variety of incidents and threats that have occurred in the past indicate that the protection of IS/IT needs to be prioritised within corporate boards as risks such as system vulnerability would reduce the value of the business were it to occur (Blakley, 2002).

IS/IT risk exists when IS/IT assets are vulnerable to threats (Icove et al., 1999; Yeh et al., 2007). Yeh stated that there are two categories of assets: these assets may be IT led (software, hardware, data and networks) or non-IT led (personnel, physical and security regulations and policies). Both categories play a significant role in IS/IT security.

Normally, vulnerabilities occur in the event of the attacks such as denial of service attacks to critical parts of IS/IT including fundamental operating units, coordinating functions and controlling functions (Bhagwan et al., 2004). A recent study found that critical IS/IT assets such as networks and personnel have received inadequate protection in some corporations in developing countries in Asia (Yeh et al., 2007). Yeh et al. selected Asia because it was the region currently holding the largest number of developing nations.

2.5.3 Corporate Governance, IS/IT Security Implementation and Adequate Internal Controls

A part of the effective management of IS/IT risk includes attention to internal controls. Internal controls are important to the IS/IT security process to ensure the status of IS/IT security is reported so that the board and senior management can react to business risk effectively and efficiently (Solms, 2001). Solms successfully established the conceptual relationship between corporate governance, internal controls and information security but he did not validate the conceptual relation within the real world settings.

Internal controls are *ways, checks and balances, to provide assurance that things go as intended where procedures, regulations and laws are followed, transaction are properly documented, fraud, waste and abuse are minimised, unapproved transactions are not processed and desired outcomes are achieved* (Sinclitico, 2007, p 22). As reported by Sinclitico (2007) after 25 years *management controls* were finally done away with due to management failure to control the resources effectively and efficiently but good internal controls are still relevant today. The term internal controls has replaced management controls.

There are several ways to apply internal controls within IS/IT security implementation. The first approach is *measurability*, all types of directives such as security policies, procedures, and standards can be measured in some way (Solms, 2006). Even though the model of Corporate Governance Direct Control Cycle by Solms (2006) did not address internal controls specifically Solms highlighted the need to measure the IS/IT security processes and provided several ways to measure *what* and *where*. As noted by Solms, in an organisation, there are three management levels, strategic, tactical and operational. The operational level can be measured, monitored and reported through reports and low-level administrative documents, such as *logs of operating systems, databases and firewalls*. Later, the upper level, namely, tactical level, measurement relates to the level of compliance and conformance of IS/IT security policies, corporate standards and procedures, such as *Senior Managers reports*, to be brought up at Strategic Level. At the strategic level, measurement can be done via a set of directives from the board such as *compliance reports, security risk management reports* and any *conformance reports* relating to IS/IT security.

The second approach to applying internal controls to IS/IT security implementation is to use the general deterrence theory (GTD) which comes from the field of criminology. GTD includes four lines of sequential action, the first is deterrence, the second is prevention, the third is detection and the fourth

is remedy, these four lines were developed to reduce computer abuses in corporations (Straub et al. 1998).

In the IS/IT security risk planning model by Straub (1998) which uses GTD, counter-measures work according to lines of controls. In the first line—deterrence control—potential offenders are deterred in a passive approach through policies, guidelines and security awareness programmes. If potential offenders ignore deterrence control, the next line— prevention control—can be enforced actively through physical and procedural controls. If potential offenders successfully penetrate the first two lines, corporations can use detection control to gather evidence of misuse such as suspicious activity reports, systems audits and virus scanning reports.

Finally, remedy control is effected when there is non-compliance to the first three lines, which may involve *warnings, reprimands, termination of employment and legal action*.

The four lines of GTD controls are not meaningful if the board and senior management do not put a proper measurement system in place. The effective measurement system is important because it is the key to culture (Labovitz, 1997).

However, establishing effective internal controls depends on the involvement of the board and senior management as they are responsible for both the creation of business opportunities and the maintenance of the effective IS/IT security of the corporation (Varadharajan, 2007).

2.6 Measuring the Efficiency and Effectiveness of Internal Controls over IS/IT Security Implementation

Throughout the governance process, documents that are produced at all management levels can be analysed in order to determine the status of IS/IT security achievement. Measurement of IS/IT security needs to reflect all documents produced at all management levels from the strategic (e.g., strategic vision), tactical (e.g., security policies, organisational standards and procedures) to operational (e.g., sets of administrative guidelines and administrative procedures) (Solms, 2006).

The governance process is primarily exercised by people at the senior level and involves all management levels. Organisations may measure IS/IT security practices and apply internal controls to certify whether information assets are used responsibly as intended (Ghose, 2006). Internal controls can be applied to IS/IT security components and may be specified as measurements.

2.7 Components of IS/IT security

In this section, relevant components of IS/IT security will be described. The components are divided into four aspects based on the work by Yngstrom (2006) and Solms (2001). IS/IT security is a multi-dimensional discipline which requires a balanced attention between these four aspects, identified as, technical, organisational, human and legal. It does not concentrate on a single aspect. These four aspects will now be examined.

2.7.1 Technical aspect

Predominantly, before the advent of the IS/IT security management era, the IS/IT security literature was focused on the technical context (Siponen, 2007; Yngstrom, 2006). IS/IT security issues like operating systems, access to computer resources, the design and development of IS/IT and internet security were considered to be the major technical challenges in organisations.

Siponen (2007) conducted a survey, analysing the IS/IT security literature up to early 2001, secondary data were taken primarily from various conferences and journals across disciplines. The analytical framework was established in Siponen's work, four main issues were identified in the study, namely, 1) access to IS, 2) secure communication, 3) secure management and 4) development of secure IS. Siponen (2007) has shown that IS/IT security research was mainly concentrated on two major issues; access to IS and secure communication. The technical issues surrounding access to IS were *authentication methods (e.g., password and token-based authentication), access control and information-flow control models, memory protection of operating systems, anti-virus techniques, watermarking, imagesecurity, audit/intrusion detection, firewalls* (Siponen, 2007, p 71). Whilst, the secure communication issue was focused on technical issues like *Cryptographic techniques, including message encryption, digital signatures, steganography, watermarking, hash, virtual private networks, electronic cash, Intranet security, anonymity techniques*" (Siponen, 2007, p 71).

It was found in Siponen's work (2007) that technical issues had dominated security problems. This occurred due to many factors; it is believed that the mutual interaction between formal and technical, formal and informal, and technical and informal were missing and less taken care of. For example, the implementation of the technical component, such as intrusion techniques, was rather a stand-alone approach. The implementation of technical component, intrusion technique, might not have had an adequate interaction with the formal and informal components, e.g., the implementation of the intrusion technique might not align with IS/IT security risk management (formal component) and might get insufficient support from employees (informal component).

However, in more recent years, non-technical aspects have received greater attention as discussion has come to focus on information and the governance process (Mishra et al. 2007).

2.7.2 Organisational aspect

The organisational aspect is part of the formal component (formal procedures) that needs to be implemented in organisations. The successful implementation of the formal component is, though, still dependent on the mutual relationship with the technical and informal components. In IS/IT security, the organisational aspect covers components like organisational structure, job responsibilities, mutual communication between related roles and the involvement of senior management (Solms, 2001). To operationalise those components, organisations may apply strategies and approaches at each level, such as IS/IT security policy (Lineman, 2002-2005), policies regarding strategic vision, IT and business alignment, competition and legal prescriptions (Solms, 2006). Security researchers have addressed the need for the organisational aspect for several years to minimise the IS/IT security incidents and threats.

It has been discussed earlier that security risk is a business risk which needs to be taken into consideration within the formal risk management procedures of the corporation.

However, IS/IT security is not only an organisational problem but also a social problem (Dhillon et al, 2000). To resolve IS/IT security problems, Dhillon et al incorporated some additional human aspects; responsibility, human integrity, trust and ethicality into IS/IT security principles. Therefore, the human aspect also needs to be considered.

2.7.3 Human aspect

The human aspect of the informal component is often neglected by organisations. This could happen because organisations might have inadequate internal controls and risk management plans over informal aspects. Internal controls can be used by organisations to measure the efficiency and effectiveness of informal component operations such as the interaction between formal component (e.g., policy implementation) and informal component (e.g., the level of policy acceptance among employees) and between technical (e.g., security procedures such as firewalls implementation) and informal (e.g., poor culture practices).

In the literature, the informal component has been shown to be relevant to IS/IT security. Informal component relates to people (Torres, 2006) and may deal with people's integrity (Wood, 2002), culture and commitment (Gaunt, 2000; Hone, 2002a; Wood, 2002), education level (Solms,

2004; Whitman, 2003; Wood, 2002) and user behaviours (Stanton, 2004). Clearly, the informal component is a critical success factor in addressing security problems, where a greater understanding and mutual interaction between informal and technical/formal components exist.

A failure to address human aspects may expose organisations to business risks if not properly managed. For example, the case of Enron and its auditors (Andersen) in the US will illustrate this. Both companies shocked the stockholding public in the USA by their corporate fraudulent behaviour (Wood, 2002). In Wood's paper, senior management were allegedly involved in destroying/shredding documents required by the federal investigator, the Securities and Exchange of Commission. According to Wood, such fraudulent behaviour may bring losses to businesses including business reputation and business continuity. Wood (2002) claimed the incident of Enron and its auditors should have been brought to the attention of CEOs in organisations for future development and implementation of IS/IT security policies. The reason for this concern is because the boards of directors and senior management have responsibility to ensure employees need to be trained, educated and acquainted with IS/IT security policy. In some companies, the security solution is mainly focused on adopting IS/IT rather than understanding security concerns. It is important to highlight that the paper by Wood was rather a technical opinion, the paper was based on the perspective of a consultant's experiences in IS/IT security and policy development.

Dhillon (2000) underlines that security concerns are not only about the confidentiality, integrity and availability of data but also about human responsibility, integrity, trust and ethicality. Human aspects such as ethical (integrity), ignorance and stupidity are seen to be a serious threat to organisational IS/IT and might expose information assets to risks and vulnerabilities.

This section has illustrated how useful a multi-dimensional discipline is in dealing with security risks caused by human behaviour, human ethics (integrity), human ignorance and human stupidity and organisational IS/IT. *Facing pressures of organisational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understanding the security concern* (Dhillon, 2000, p 127). There are some solutions to be found through empowering human capital, which can be broken into two approaches; providing education, training and awareness and developing a security culture.

2.7.4 Legal Aspect

The legal aspect is an external factor to organisations. A legal factor is an input that needs to be considered by the Board and senior management in the development process of IS/IT security policy, standards and procedures. For example, governments have increasingly enacted laws relating to IS/IT security practices to be effected by small to large organisations (Posthumus, et al. 2004). Up to date, several laws have been enacted and used by organisations to minimise and deal with IS/IT security threats such as the Sarbanes Oxley Act, the Health Insurance Portability and Accountability Act, the Malaysian Code of Corporate Governance.

The increased number of IS/IT security incidents has encouraged organisations to take legal actions against internal employees and external users who misused or falsified business information with the use of IS/IT applications. An earlier section, 2.5.3, reviewed the four sequence line of actions that can be implemented to reduce computer abuses which are deterrence, prevention, detection and remedy. Legal, which falls into remedy, needs to be put into action if the first three lines are ignored by internal and external users. This shows that the legal aspect is still needed for governing IS/IT security practices in organisations today. For example, the ease of access to business information and services has encouraged the board and senior management to implement regulations relating to IS/IT security to minimise security incidents (Posthumus et al., 2004).

The involvement of the board and senior management is needed because they are able to create a security culture where the compliance with regulation or law works through a top-down approach (Solms, 2001).

2.8 Empowering Human Capital through Education, Training and Awareness

Effective security is not about identifying solutions that are more technical but about creating awareness, training and educating all computer users in the basics of computer security (Rudolph, 2000). Up to 70 percent of incidents are believed to be the result of internal users either through ignorance or stupidity rather than intentional acts (McIlwraith, 2006). Internal users should be aware that ignorance and stupidity may increase an organisation's business losses—through IS/IT security incidents. The reason is that ignorance and stupidity are threats to IS/IT which can be resolved through appropriate education, training and the raising of awareness (Brian, 2001).

While the link between education, training and awareness is significant, awareness is seen to be the fundamental requirement for good IS/IT security practices. Awareness of security of IS/IT is the

practice of making people aware of the important aspects of IS/IT security and encouraging them to act in a way that relates to organisational activities (McIlwraith, 2006). It has been emphasised in the Organisation for Economic Co-operation and Development (OECD) Guidelines, that awareness is one of the nine principles which warns that participants should be conscious of the configuration of available up-dates for their systems and to perform good practices to enhance security and the needs of other participants in organisations (OECD, 2002). According to the OECD, awareness can improve the way people handle IS/IT and might reduce the risks involved to low business risk level.

Raising IS/IT security awareness requires the involvement from the board and senior management. The board and senior management are the people who are responsible to cultivate the awareness of employees because they are mandated to deal with corporate risks— IS/IT risks. The directives from the board and senior management about both awareness programs and IS/IT security planning need to flow down to the bottom to ensure that IS/IT risks are minimised. The awareness program and IS/IT security planning should go hand in hand in proffering a means to change the situation. One of the reasons for ineffective IS/IT security is that senior managers often do not understand the security problems faced at the ground level and are not aware of the security counter-measures available to them (Straub, 1998). This example has shown that without awareness the security counter-measures might not be implemented successfully. That is why the relationship between awareness program and IS/IT security planning should be established in the first place before implementing security counter-measures anywhere. At this stage, the role of the board and senior management is crucial to ensure all employees are aware and act on any set of directives such as IS/IT security policies, standards, procedures or guidelines.

If employees have an adequate knowledge on IS/IT security needs, the creation of security culture can be developed naturally in an informal way because culture involves human behaviour. This is because human error is the root cause of problems during the technological implementation (Brian, 2001). To be more effective in IS/IT security, the causes of human error can be addressed through conducting both awareness training and IS/IT security planning.

2.9 Creating a Security Culture

Security culture is associated with organisational culture. An organisational culture is defined as *a complex pattern of beliefs, expectations, ideas, values, attitudes and behaviours in an organisation that binds members together and influence what they think about themselves and what they do*

(Hellreigle, D et al, 1998, p 546). Organisational culture is associated with the behaviour of employees. Security culture helps to create an impact on the operation of IS/IT through the daily practices of employee behaviour (McIlwraith, 2006; Ward, 2002). As the root of the majority of IS/IT security problems is human error, IS/IT security culture may act as a “human firewall” to protect organisational IS/IT and information assets (Zakaria, 2003).

Researchers have found ways that organisations can cultivate security culture by increasing analysis of employee security perception (Zakaria, 2005). This is because perception influences behaviour (Huczynski, 2001). A positive security perception can help employees apply security policies and procedures into practice (Zakaria, 2005). A negative security perception can lead employees to perform negative daily work routines which increase business risks. Zakaria has given one example of security perception which relates to employee perception on security tasks. In a case study reported by Zakaria, employees claimed that security tasks were supposed to be the responsibility of the IT/Computing Centre but not of others. This perception is an example of negative security perception. The negative perception about security tasks has led to bad corporate practice where IS/IT security is the responsibility of specific groups such as IT staff but not of all staff. Researchers report that security activities require the full involvement from all employees (Babiak, 2005; Force, 2004). Therefore, perception analysis can reveal either positive or negative perceptions that can be used by organisations to redesign their security awareness and training programmes within an organisation’s context (Zakaria, 2005).

2.10 Other useful frameworks and regulations

Apart from ISO 17799/BS7799 and COBIT, most organisations today have used different frameworks or combinations of frameworks as a guide in order to protect information assets and IS/IT from being hacked by internal users or external users. One major reference framework, namely, COSO, will be presented in the next section. This section also reviews the Sarbanes-Oxley Act (2002), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Malaysian Code of Corporate Governance (2000).

2.10.1 The Committee of Sponsoring Organisations of the Treadway Commission (COSO)

COSO is an example of an internal controls framework but is not exclusively used for guidance in IS/IT security practices and implementation. Since its release in 1992, there has been no up-dated version reflecting security environment or IT guidance (Entrust, 2003-2004). COSO is primarily used

in domains such as financial reporting and audit procedures by these following authors such as Campbell (2006), Swanson(1999), Sinclitico (2007), Armour (2000), W.R.K (2000), Rittenberg (2007) and McCuaig (2007). Organisations used COSO to examine whether certain objectives are achieved as intended by employing certain policies, standards and procedures with senior management's involvement.

COSO underlines the role of the board and senior management as the most needed component of a control structure (Swanson, 1999; Bedell, 2006; Rogers, 2004). In the COSO framework, the board and senior management involvement are considered to be "Control Environment", the foundation for all other components of internal control, providing discipline and structure. One study confirmed that the control environment is the most important component of internal controls in the eyes of auditors (O'Leary, 2006). Apart from COBIT, COSO has also emphasised that the involvement of board and senior management are required to achieve the objectives and mission of organisations effectively and efficiently.

2.10.2 Sarbanes-Oxley Act

The enactment of Sarbanes-Oxley Act (2002) was driven by a number of US corporate collapses such as Enron, WorldCom, Waste Management, SunBeam and Global Crossings (Boyle et al, 2007). Boyle et al. (2007) have emphasised that Enron and WorldCom had the largest impact on the economy. As a consortium of energy companies, Enron was allegedly involved with various manipulations of its financial reporting statements which allowed a significant over-statement of earnings. In a similar situation, WorldCom, a major telecommunication firm in the USA was purportedly involved with a series of fraudulent transactions totalling \$3.8 million in 2002.

In response to the above corporate scandals, the Sarbanes-Oxley Act was enacted covering internal controls, external financial disclosure, corporate governance and auditor behaviour (Boyle, 2007). Even though the Sarbanes-Oxley Act is not exclusively used for IS/IT, the empirical evidence found that the Sarbanes-Oxley Act is progressively making an impact on the voluntary disclosure of IS/IT activities by corporations (Gordon, 2006). However, even though the Sarbanes-Oxley Act offers many benefits in US corporations today, there are some drawbacks.

Boyle noted that the Act has had some effects in terms of financial and non-financial matters (Boyle, 2007). Further, Boyle added that, in terms of financial matters, the corporations are facing long-term liability such as auditing costs, compliance costs, governance and human capital costs. In

non-financial matters, the effects include the mismatch between auditors and corporations, the ambiguity of the quality of investor information and capital market efficiency. However, in general, the SoX has transformed the way people direct, control and practise their internal controls, external financial disclosure, corporate governance and auditor behaviour.

2.10.3 The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was enacted in 1996 on the advice of the U.S. Department of Health & Human Services (HHS) and established a set of national standards for the protection of certain health information and privacy in electronic form. The main purpose of the HIPAA is to ensure that the privacy and the security of individual's health information is properly protected electronically. The Act applies to all health plans, health-care clearinghouses and to any health-care provider in USA (Services, 2003). Even though HIPAA regulation has broad implications to the health-care industry, the level of understanding about security issues by executive management is frustrating (Jensen, 2007). Jensen et al identified that HIPAA was frequently treated as both tactical and operational issues, rather than governance and management issues. Lack of governance and management attention in IS/IT security would expose organisations to high risk level of threats and vulnerability attacks. Jensen found that organisational change such as culture and awareness are the most important challenge to the successful implementation of HIPAA regulation.

2.10.4 Malaysian Code of Corporate Governance

The incorporation of corporate governance practice in Bursa Saham (previously KLSE) listed companies was started in 1993 due to the mandating of audit committees by Bursa Saham's listing requirements (Haniffa, 2006). The corporate governance practices were later emphasised by the Malaysian Security Commission (SC) in 1993. It has been found that poor corporate governance was a major cause of the financial and economic crisis especially in East Asian countries like Malaysia, Thailand and Indonesia in the years 1997 and 1998 (Liew, 2006). That crisis saw a number of Malaysian "blue chip" corporate failures including Renong, UEM and KFC (Haniffa, 2006). The aftermath of 97/98 financial and economic crisis in East Asian countries forced the Malaysian Government to pass a new regulation on good corporate governance practices in 2000, the so-called Malaysian Code of Corporate Governance which was derived mainly from the Hampel Report and the Cadbury Report (Securities Commission Malaysia, 2000).

The Malaysian Code of Corporate Governance emphasises that boards have to be able to identify principal risks of all aspects of the business and the implementation of appropriate systems to manage these risks. Balancing between risks incurred and potential returns to shareholders is essential practice in corporate governance (Securities Commission Malaysia, 2000). In particular, according to the Malaysian Code of Corporate Governance boards are responsible to manage corporate risks including the adequacy and integrity of company's internal control and management of IS/IT. Even though the code is not specifically for IS/IT security, the good corporate governance practices corporations should be able to identify the risks that created by IS/IT.

2.11 Summary

The issues and ideas canvassed in this chapter are so disparate and lacking in support that the need to develop a model is clear. That model ought to attempt to specify the variables and reflect as far as is relevant the suggestions reported.

Chapter 3 A Conceptual Framework

3.1 Introduction

In order to develop a conceptual framework for IT/IS security governance it is necessary to consider the structure of organisations, the planned allocation of duties and the lines of authority. It is also necessary to consider the tasks and risks to be avoided or managed and whether those risks are organisation-wide or are restricted to specific functions. All these matters are discussed in this chapter before developing a conceptual model.

In IS/IT security governance, the trade-off between IS/IT security needs and financial support from the Board is vital to sustain and maintain the IS/IT investment in business. Corporate governance regulations reflect the legal relationships between shareholders and directors and the legal relationships between the Board of Directors and employees including the CEO.

Most countries have adopted the Anglo-American corporate structure with one Board supported by special purpose advisory committees such as risk management, audit and remuneration. The corporate governance regulations and listing requirements usually require a majority of independent directors on the Board and the predominance of independent directors on committees.

Strictly speaking, all directors, even executive directors, are elected by the shareholders but as the Board itself or even the CEO has control of the nomination of people to be elected there is some concern that the intent of the law may be frustrated. This was one of the concerns that prompted corporate governance regulations. In the Malaysian Code of Corporate Governance, the Board of directors has power to determine the Board's authority, Board size and committees, independent advice and company's management in accordance with the purpose, objectives and strategies of the company (Berhad, B.M, 2011).

Some countries, notably Germany and China, have adopted the two board system— a supervisory board is placed above the Board of directors which is charged with the running of the company.

The differences between the two systems have some effects on the distribution of power among individuals but, for the purposes of this thesis, the main interest is in the group which has effective control and decision-making power and, hence, has responsibility for whatever happens within the company.

Under either system, the Chief Executive Officer, whether called CEO, Managing Director, President or whatever, is employed to “execute” the decisions of the Board. To do this he is also a member of the Board although under corporate governance regulations his participation in some of the Board committees is restricted or even banned. The listing requirements, Paragraph 15.09, of the Malaysian Code of Corporate Governance states that “all of the Audit Committee members must be non-executive directors, and with a majority of them being independent directors” (Berhad, B.M, 2009, p 1503). Even though the CEO and Chief Financial Officer of Malaysian publicly listed companies are not allowed to be members of the Audit Committee, their inputs, where necessary, should be included in the meeting agenda, this was referred in Paragraph 15.19 of the listing requirements.

Most Boards nowadays have a risk management committee whose duty it is to identify and assess all risks facing the company and to advise on policies and procedures to avoid or to mitigate those risks. In some companies it seems that the handling of IT/IS risks is assigned to this committee but in others a separate committee has been set up. Again, for the purposes of this thesis the committee structure does not affect the responsibility of the Board but it may affect the channels of communication and how they operate (William, 2007). It appears that some authors in the IT/IS field see the risk management committee as the group to be informed.

It is presumed that although the organisational chart in Figure 3-1 is related specifically to Malaysian publicly listed companies, it is generally applicable to other types of organisation and other countries because any organisational chart is broadly similar to Figure 3.1.

In the typical corporation, the CEO has several subordinates comprising senior managers or executives who have specific functionalities in accordance with the nature of the business and industry type, such as Chief Operating Officer, Chief Marketing Officer, Chief Information Officer and Administrative Officer. Boards normally consist of a Chairman, Managing Director/CEO, Finance Director, Marketing Director and Non-Executive Directors, as illustrated in Figure 3.1. However, it is important to remember that the centre of all authority and responsibility is the Board, acting formally as the Board in a properly constituted meeting. Members of the Board as individuals have no powers unless they have been specifically given by the Board.

The Board of directors which is elected by the shareholders, has powers, authorities, responsibilities and accountabilities to oversee, not manage in detail, day-to-day business. Their responsibilities include,

determine the organisation's mission, select, support and review the executive and their performance, ensure effective organisational planning, manage resources effectively, determine and monitor the organisation's products, services and programs and enhance the organisation's public image (McNamara, 2011) (Online).

As addressed by McNamara, the guidelines given on Board's responsibilities are similar for profit and non-profit organisations. This chapter will present a generally applicable IS/IT security governance framework which can be adopted by any type of organisation. The aim of this conceptual framework is to provide ways to help the managements of corporations, particularly in the area of roles and responsibilities in IS/IT security governance. The following discussion is based on Figure 3.1.

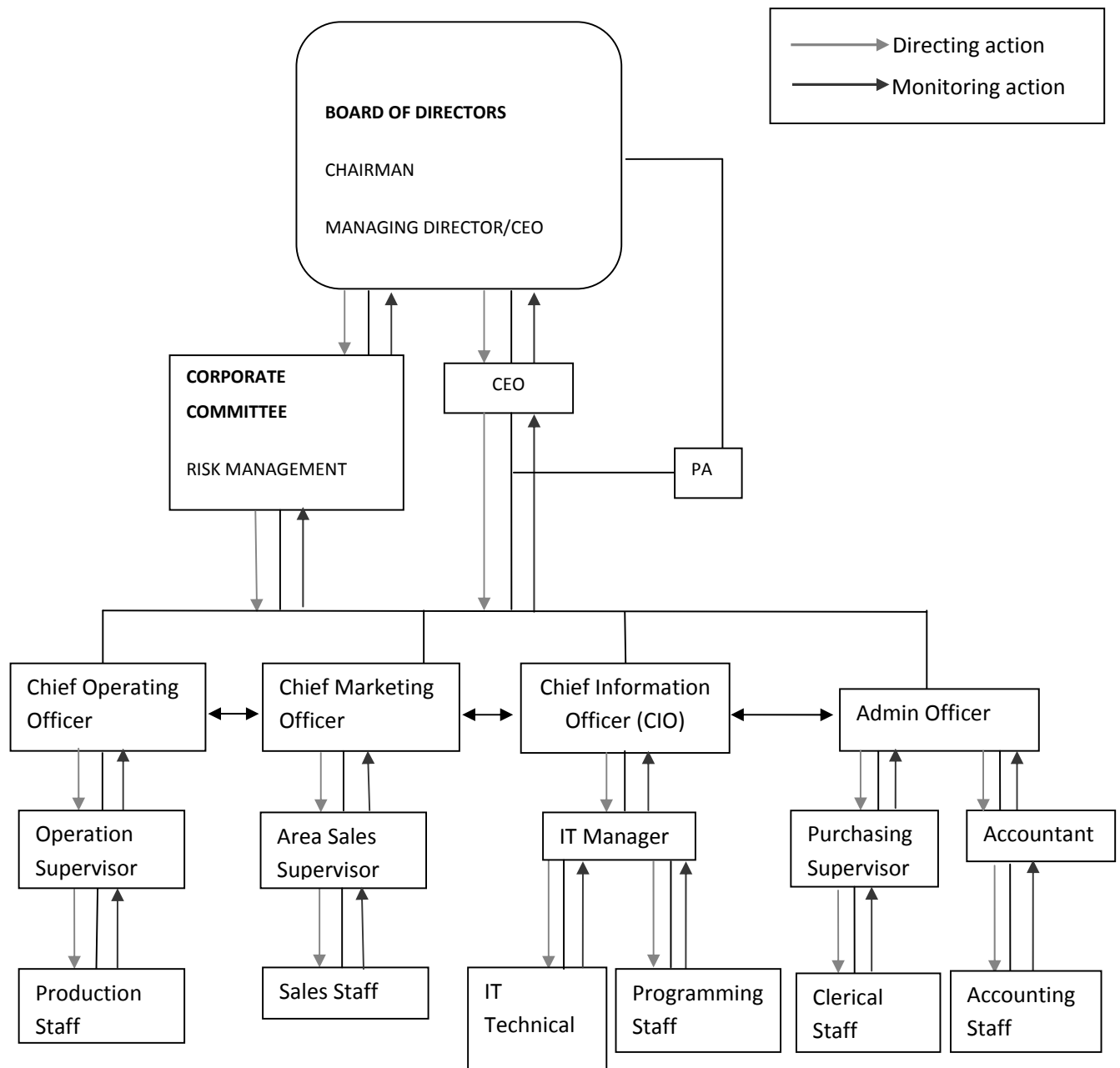


Figure 3.1. A general organisational structure IS/IT security governance framework for any types of organisation

The ultimate decisions on adopting IS/IT security controls and counter-measures are in the hands of Boards with reference to the cost-benefit analysis/return of investments results in respect to the responsibility and security requirements. To illustrate the importance of achieving security processes in terms of responsibility and security requirements within organisations, the model of “A

Responsibility Relationship between Two Agents” by Strens et al (2003) is considered, it requires identifying security requirements in the first place before delegating the responsibilities, where agents can be *people, an individual to a department or the whole of the organisation*. In Strens et al.’s model, the two agents of the relationship were identified as, first, *the giver of the responsibility* and second, *the holder of the responsibility*.

The authors stated that “equal consideration must be given to both human and technical issues if the design of the IT systems is to meet the real requirements of the organisation and be supportive of people in their works” (Strens et al., 1993, p 143). In their responsibility model, Strens et al (1993) proposed the two important factors, namely, responsibilities and obligations within IS/IT security implementation. Strens et al viewed that responsibilities cannot be delegated but obligations can be delegated, from *giver* to *holder*. As obligations such as security tasks are delegated the person to whom the tasks are delegated becomes responsible for their performance. This leads to the creation of a hierarchy or network in which the obligations delegated become more detailed as we move down from board level to the operational levels.

Strens et al., define responsibility as following criteria,

“a) who is responsible to whom;

b) the state of affairs for which the responsibility is held;

c) a list of obligations held by the responsibility holder (how the responsibility can be fulfilled);

d) the type of responsibility (these include accountability, blameworthiness, legal liability)”

(Strens, et al., 1993, P. 144).

As responsibility cannot be delegated the model by Strens et al imposes a duty on the person responsible to “supervise” the performance of the obligations. This, in turn, imposes a duty on the “operator” to provide appropriate information, e.g., to report. The set of relationships implied by Strens et al can be easily fitted to the organisational chart in Figure 3.1.

A responsibility relationship for certain tasks is discharged according to the “obligations” such as *directing, supervising and monitoring* (Strens et al, 2003, p 146). It is important to highlight that for Strens et al responsibility refers to *for a state of affairs* and obligation refers to *do something that will change or maintain that state of affairs* (Strens et al, 1993, P. 144).

Let us consider an example. In Figure 3.1, the IT Manager may have responsibility over the programmers for protecting the integrity of Accounting Information Systems from misuse, alteration and modification in the databases applications. In order to fulfil this responsibility, the IT Manager must discharge certain obligations such as to establish and apply security internal controls (e.g., network logs, log-on databases logs, transaction files) and monitor the intended activity. The identification of the responsibility and obligations over the relationship would help the person responsible (such as the IT Manager) to report back to the CIO, then to the CEO and ultimately to the Risk Management Committee and Audit Committee. After receiving managerial reports (including any proposals for improvement) from the management level, the Board or the relevant committee would revise the risk assessment and consider the needs for security mitigations according to the alignment between the use of IS/IT for business operations and the need for security controls/counter-measures over its risk. If there were a misalignment in the relationship, this may create gaps, the Board may perceive this as unnecessary and the security internal controls missions and risk management operational strategies can be frustrated. The financial constraints may not be the issue if the corporation has a clear IS/IT security mission to ensure the IS/IT investment is protected and maintained for sustaining growth and wealth creation (National Cyber Security Summit Task Force, 2004).

3.2 IS/IT risks and IT governance

IS/IT assets and resources need to be protected from all risks. Identifying, assessing and mitigating risks are associated with corporate governance. In effective corporate governance, the Board and senior management direct, control and monitor organisational assets and resources including IS/IT to ensure that their business objectives are achieved as intended (Corporate Governance Task Force, 2004). This process is referred to as Information technology (IT) governance, a sub-set of corporate governance.

Within IT governance there are two main responsibilities, IT value governance and IT risk governance. IT value governance concerns the wealth creation of the company and increasing shareholder value while IT risk governance relates to the security of information systems and IT infrastructures. IT risk governance is essential to ensure that organisations derive all expected and intended IT value benefits. Figure 3-2 demonstrates the focus of this conceptual framework: looking into IT risk governance and specifically examining how IS/IT security issues such as vulnerability and various threats are identified and minimised within Malaysian publicly listed companies.

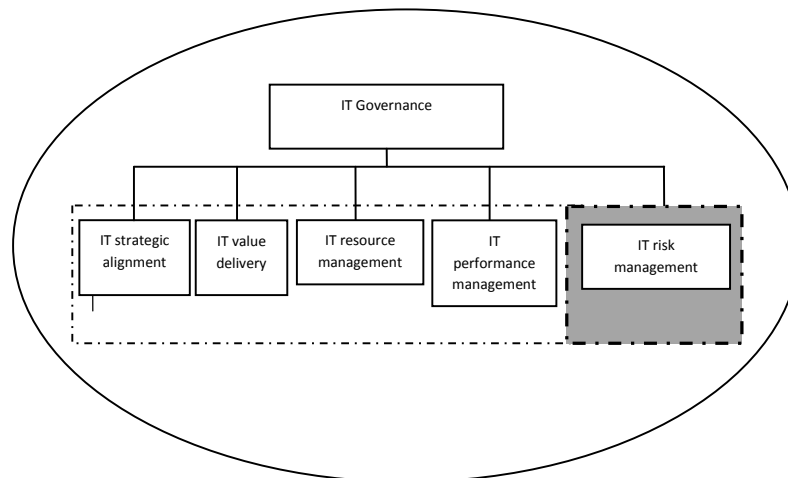


Figure 3.2 Research Focus of this study and IT governance framework (adapted from ITGI, 2003)

The IT Governance Institute identified five IT governance domains: IT strategic alignment, IT value delivery, IT resource management, IT performance management and IT risk management (ITGI, 2003}. The Institute identified the first four domains as belonging to IT value governance and the last as IT risk governance. This relationship is shown in Figure 3.2 above. When aiming to achieve IS/IT value benefits of the four IT governance domains, safeguarding IS/IT assets and resources is vital to minimise the risks to IS/IT.

Managing the IS/IT risks is an important aspect of IT risk governance. This is for the following two reasons: internal factors and external factors. Internal factors are internal to the technical dimension and involve risks from technical deficiencies and limitations of the software and hardware. While external factors are concerned with human issues, human threats could be risky to business because many security problems are social and people issues.

First, business losses caused by threats to and vulnerabilities of IS/IT may be critical. The literature review has suggested that if threats and vulnerabilities of IS/IT risks are not treated appropriately at the Board and senior management level, security incidents within organisations may continue.

As security of IS/IT is part of IT risk governance, the difference between risk and security needs to be understood first. A risk occurs when a certain system is vulnerable to attacks while security is a process of preserving and safeguarding assets or resources from being attacked. The importance of

addressing IT risk governance and ensuring that IS/IT security issues receive a high level of attention has been highlighted by a growing number of security incidents (Lin, 2006).

Second, risks that result from security threats and vulnerabilities of IS/IT may come from various sources: human threats, e.g., hackers, crackers, computer criminals, terrorism, industrial espionage and insiders; IS application vulnerabilities, e.g., coding problems and physical vulnerabilities, e.g., earthquakes, floods and fire (Dhillon et al., 2007). That is why the Board and senior management need to be actively involved in corporate risk management to ensure all potential types of IS/IT risks are identified, assessed and mitigated effectively.

3.3 IT risk governance

IT risk governance which involves IT risk management can be used to minimise or avoid security threats and so prevent IS/IT being vulnerable to attack. If potential security threats and vulnerabilities are not addressed and managed effectively by the Board and senior management, they may create risks affecting IS/IT. These risks may affect software, hardware, network and data (Yeh et al. 2007).

Internal controls and IT risk governance are essential parts of corporate governance to monitor the effectiveness of resources. To achieve effective corporate governance and minimise business risks, internal controls and IT risk governance are important mechanisms to ensure that resources are used and monitored so that potential security risks can be identified, assessed and mitigated simultaneously. The Board and senior management are formally responsible for internal controls because they have the power to make decisions on resources and activities, including the security of these resources (OECD, 1999). In other words, IS/IT security is the responsibility of corporate governance and the Board and senior management have oversight of those responsibilities.

In this conceptual framework, internal controls and IT risk governance work together in addressing potential threats and vulnerabilities at an organisational level. As can be seen in Figure 3.3, internal controls are a part of the corporate governance mechanisms. Internal controls can be used for directing and monitoring the use of IS/IT. Internal controls help to ensure that the security policy achieves its objectives. Throughout the IS/IT security process the establishment of IT risk governance needs to be in parallel with internal controls.

Internal controls and IT risk governance are important to the IS/IT security process in two significant ways: first, execute and implement directives; and second, monitor the implementation of directives. In the first process, the Board and senior management use internal controls and IT risk governance to ensure that the corporation's directives such as security policies, standards, procedures, guidelines, administrative rules and practices at all organisational levels are properly chosen and adapted to the organisation, implemented and enforced. While in the second process, IT risk governance and internal controls assist in monitoring the status of the IS/IT security achievement. The feedback reported to the Board and senior management allows them to react to the business risk early, effectively and efficiently (Sinclitico, 2007., COSO, 1992).

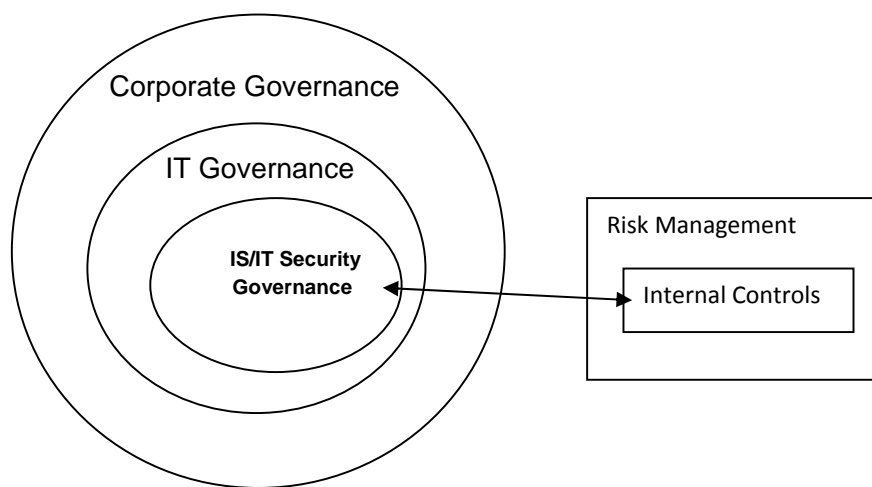


Figure 3.3. Relationship between internal controls, risk management and IS/IT security governance

IS/IT security is a sub-set of corporate governance. It provides strategic direction, achievement of objectives, IT risk governance and the internal controls of the corporate security program (IT Governance Institute 2006). IS/IT security governance in this study is defined as the role of the Board and senior management to establish effective internal controls and apply IT risk governance to ensure that the confidentiality, integrity and availability of IS/IT assets/resources are safeguarded (Baskerville, 1988, Parker, 1998, IT Governance Institute, 2006).

3.4 Formal, technical and informal dimensions of IT risk governance

In this conceptual framework, IS/IT potential risks are managed using three dimensions: the technical dimension, formal dimension and informal dimension (Dhillon, 2006, Mishra, et al, 2007).

In Figure 3.4, the formal dimension is concerned with organisational aspects such as strategic vision and the alignment between business goals and the security policy. The security policy includes

having clear security roles and responsibilities and other IS/IT security policies. The formal dimension also concerns the organisational structure and formal communications between related roles to achieve the secure operation of IS/IT.

The technical dimension mainly deals with the security of IS/IT areas and uses techniques and controls such as assets classification and control, communication and operations management, access control security (e.g., encryption, cryptography, filters, back up and disaster recovery) and system development and maintenance. The technical dimension is also concerned with how to minimise the vulnerability of systems to coding problems and physical threats (e.g., natural disasters).

The informal dimension covers personnel and human aspects such as norms, values, personal beliefs, people's integrity, trust and ethics, culture, commitment, ignorance and stupidity, the level of education and training and security awareness. These aspects facilitate the acceptance of IS/IT security practices within businesses. The informal dimension can be used to address the human threat issues including intended actions associated with hackers, crackers, computer criminals, terrorism, industrial espionage and the inappropriate actions of insiders. The informal dimension includes unintended actions such as mistakes and error.

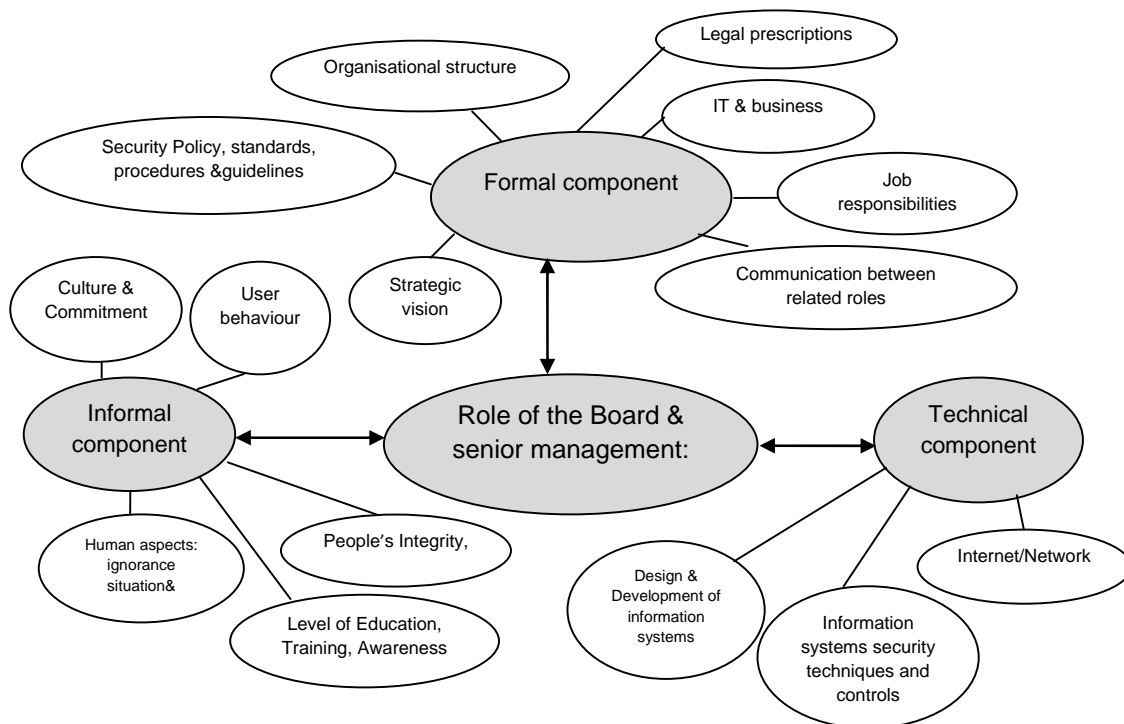


Figure 3.4 Formal, technical and informal dimensions of IT risk governance

The three dimensions of IT risk governance need to operate in a parallel way. The Board and senior management are responsible to balance these three dimensions in practice. Ignoring one of these dimensions such as the human aspect may indicate that corporate risk management is not functioning as well as it could be.

3.5 Internal controls for IT risk governance across the formal, technical and informal dimensions

Internal controls are important mechanisms to ensure that the alignment between business goals and security initiatives can achieve the corporation's objectives across the formal, technical, and informal dimensions of IT risk governance. Internal controls in the conceptual framework set out in Figure 3.5 are grouped into two major governance actions, namely, 'directing' and 'monitoring'. The directing actions and monitoring actions can be mapped out across the formal, technical and informal dimensions to achieve an effective implementation of IS/IT security governance (Solms et al, 2006). In the modified framework set out in Figure 3.5, directional arrows show that the Board and senior management can provide strategic direction and guidance to the formal, technical and informal dimensions within organisations. The monitoring arrows indicate how the Board and senior management can monitor the achievement of the actions which were produced in the directed activities. In the monitoring process, all direct activities are monitored to ensure any transactions that occur in the formal, technical and informal dimensions are properly aligned with the security needs as intended.

The framework in Figure 3.5 has been divided into two levels: internal elements and external elements. The internal elements show the boundary of power exercised by the Board and senior management in an organisation, while the external elements refer to the power of external parties exercised over organisations through laws and regulations.

The first level, which covers the internal elements organised according to the three dimensions, the formal, technical and informal, is examined in this study. In Chapter 2, in the formal dimension, elements involved include organisational structure for security, job responsibilities and communication between related roles, security policy, IT and business alignment policy. The following elements of the technical dimension were identified: information systems security techniques and controls and internet/network security. Elements of the informal dimension are human aspects, culture and commitments, level of education, training and awareness, people's integrity, trust and ethicality.

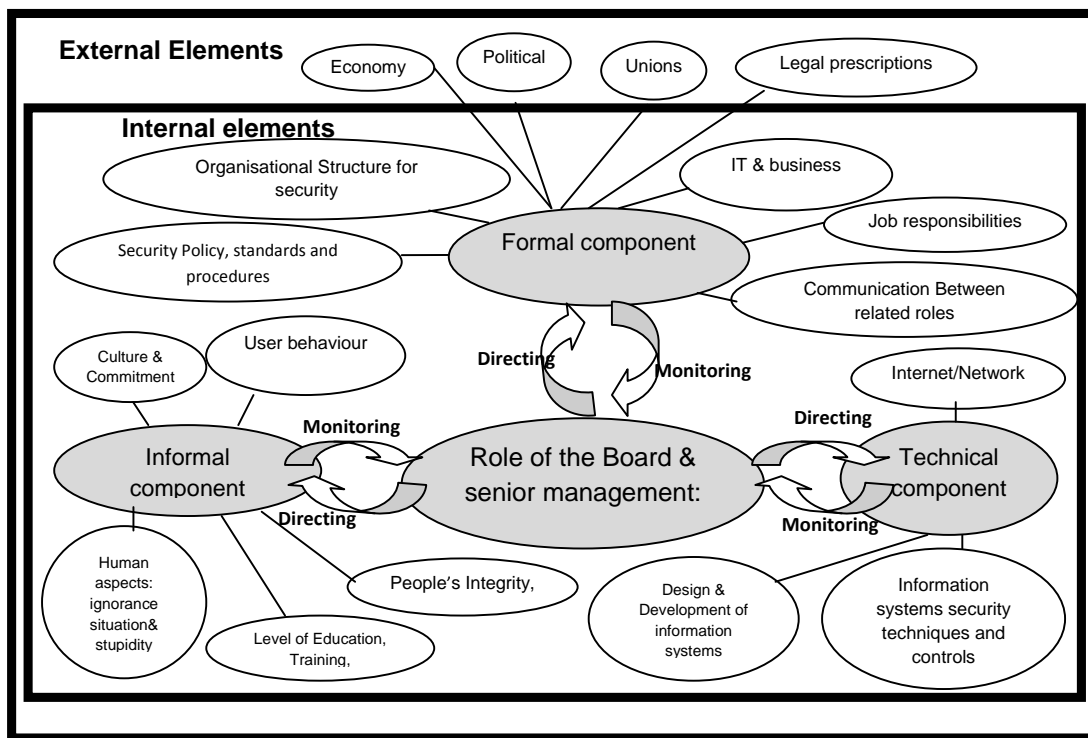


Figure 3.5 Internal controls process and IT risk governance of IS/IT security over the formal, technical and informal dimensions

In the following sections, the two major processes of directing and monitoring are discussed in detail and incorporated within the formal, technical and informal dimensions.

3.5.1 Directing Actions

In the directing actions, an arrow shows how the elements of each dimension are imposed by the Board and senior management. The monitoring arrows indicate that the Board and senior management have responsibilities across formal, technical and informal dimensions which are now discussed.

3.5.1.1 Directing Actions: Formal dimension

The establishment of an organisational structure for IS/IT security is needed for IT risk governance. To achieve this objective it is necessary to establish a clear IS/IT security role and responsibility for each employee. Having clearly defined roles and responsibilities will indicate who has the authority and is accountable for decision making in the IS/IT security process (Williams, 2007).

The Board and senior management are responsible and accountable to ensure that business risks including IS/IT risk are considered and addressed in a corporation's policies, standards and procedures. It is important to highlight the difference between responsibility and accountability. According to Dhillon, responsibility for security is a state of responsiveness that involves accepting judgments, acts and omissions. While, accountability is the preparedness to give an explanation to stakeholders for one's judgments, intentions, acts and omissions, when they are directed (asked) to do so, based on the actions of employees (Dhillon, 2007). Nowadays, employees can access data and other corporation information remotely at airports, cafés and other wireless hot spots. Increased ease of access brings potential security risks. Further, the Board and senior management have to be able to manage the communication of related roles to employees.

As IS/IT security is a continuous process, the communication channels between staff holding related roles should be re-evaluated from time to time. Finally, in achieving the alignment between IT/IS and business goals, the Board and senior management should ensure that the creation of IT value is protected at internal levels.

The three elements of the formal dimension were summarised as follows:

- establishment of clear roles and responsibilities for IS/IT security
- ensure that communication between related roles occurs in the security process
- implement an effective security policy, IT and business alignment policy

3.5.1.2 Directing Actions: Technical dimension

In the technical dimension of IT risk governance, the technical aspects of IS/IT security are shared among everybody within the company, particularly the Board and senior management but also including other related roles such as other line managers and lower-level employees. The Board and senior management are included in the technical roles because the risk created by IS/IT is a part of corporate risk which needs to be addressed at the governance level. The Board and senior management may impose requirements of security techniques and controls, design and development of IS/IT and internet/network aspects to ensure that the IT value is protected at the technical level.

As discussed earlier, internal elements identified in the technical dimension are summarised as follows:

- share responsibilities for the technical processes between the Board, senior management and related roles, which cover:
 - security techniques and controls
 - design and development of secure information systems
 - internet/ network security
- ensure that the business goals and security requirements are achievable.

3.5.1.3 Directing Actions: Informal Dimension

In achieving the alignment between the business goals and security requirements, the Board and senior management need also to incorporate human aspects within the IS/IT security process. Human aspects are a vital dimension in IS/IT security because security incidents predominantly result from human action rather than from organisational or technical problems. Human action can be divided into two parts, intended action (e.g., violations) and unintended action (e.g., mistakes and lapses) (Hurst, 1998). To minimise both types of human action happening, several elements can be monitored by the Board and senior management to discover the level of such practices. These elements include culture and commitments, level of education, training, awareness, people's integrity, trust and ethicality.

The role of the Board and senior management is to impose those elements into practices through collaboration with those people in related roles. The success of IS/IT security, therefore, depends on the Board and senior management's commitment.

The incorporation of human aspects into the security counter-measures may minimise the creation of risk from human action. Through effective internal controls and IT risk governance, the Board and senior management shape the behaviour of employees so that they are accountable and act with integrity, trust and ethicality. These behaviours are needed to prevent the employees committing unintended actions such as mistakes and lapses and intended actions such as violations.

3.5.2 Monitoring Actions

Monitoring actions include corporate governance responsibilities. Monitoring is observing and noting deviations from expected performance such as IS/IT systems performance, policy and procedures implementation and security culture of people within the organisation. Monitoring involves getting feedback (e.g., systems deficiencies, bugs, system performance) and reports (e.g., the

achievement of security internal controls, security incidents) and observing the security culture (e.g., unlocking the computer covertly), then the deviations must be reported to the level of management empowered to order appropriate corrections. However, if there are no clear policies or procedures on deviations, the monitoring task would be difficult, that is why the existence of formal, technical and informal dimensions and their interaction are significant in IS/IT security governance. Indeed, if there are no written policies and procedures in place, the corrective actions on unreasonable deviations could be hard to resolve because the management of the risk was not assigned to anyone exercising authority.

How directed activities are monitored in the formal, technical and informal dimensions is discussed in the following sections.

3.5.2.1 Monitoring Actions: Formal dimension

At the formal dimension when monitoring actions, the Board and senior management need to ensure that the alignment between business goals and security requirements is achieved. If this alignment has not occurred, it might indicate that the Board and senior management are not involved in the corporate risk management process. In this situation the Board and senior management may improve the alignment by getting more involved on the management of IS/IT risk. To do so, they can monitor whether the role and responsibility structures are well or ill defined. Having clear roles and responsibilities for IS/IT security in the organisational structure is a part of the risk management function (Williams, 2007).

3.5.2.2 Monitoring Actions: Technical dimension

Within the technical dimension, the Board and senior management play a significant role in monitoring the progress of implementation of IS/IT security controls. The following are examples of IS/IT security controls used by organisations: encryption, discretionary and mandatory access control, cryptography, filters, back -up, disaster recovery, audit log, verification, authentication and validation checks. Monitoring the security reports results of IS/IT security controls is part of the internal control applied in this process. The managerial entities (e.g., Risk Management Committee, CIO, IT manager) who are responsible for internal controls would promptly react and question the effectiveness of existing procedures and insist on improvement and perhaps even suggest that the Board revise the acceptable level of risk to ensure the objective of the procedure is achieved in an efficient and effective way (Solms et al, 2006). The application of internal controls and IT risk governance to the security

reports can be used to help the Board and senior management to ensure that resources are used and managed according to the business and security policy.

3.5.2.3 Monitoring Actions: Informal dimension

The informal dimension within IS/IT security governance can be monitored in a few ways: first through security behaviour; and second, through security failures and incidents. In the first way of monitoring, management can monitor the security behaviour of employees through feedback, security reports and communication during meetings. While in the second way, it can be monitored by looking at the security failures or incidents that occur in the corporation. For instance, if failures resulting from violations or social engineering attacks increase, the management may increase the awareness program amongst the employees. In the case of incidents caused by negligence due to poor performance, management may address the risk by conducting more training and educational programs to improve employees' skill and knowledge. Management may also change the duties of relevant individuals or dismiss them and/or move to tighten up employment practices and procedures.

3.5.3 Summary

Both directing and monitoring actions in the formal, technical and informal dimensions are needed in organisations. The directing and monitoring actions are important because by safeguarding information IS/IT can protect IT value from business losses such as gaining a bad reputation and monetary losses. To summarise this section, Table 3.1 shows how the directing and monitoring processes are incorporated within the formal, technical and informal dimensions.

Dimensions	Internal Controls: Role of the Board and senior management in IS/IT security governance	
	Directing	Monitoring
Formal Dimension	Define the importance of information systems security and its alignment to business goals, define clear roles and responsibilities to each employee involved	Define the importance of monitoring action against the directed activities, Define how monitoring action helps organisations to achieve risk management function
Technical Dimension	Define the need of security controls/counter-measures to incorporate in the risk management process, in order to resolve technological deficiencies	
Informal Dimension	Define the importance of human aspects to encounter human actions(either intended or unintended), security culture is part of this dimension	

Table 3.1 Directing and Monitoring Processes over formal, technical and informal dimensions

3.6 Developing a model of IS/IT security governance

The literature has shown the gap to be studied : management failure to understand the IS/IT security problems faced by lower levels of the organisation simultaneously in three dimensions, namely, formal, technical and informal dimensions. Apparently, in previous studies, the IS/IT security researchers were concerned with technical issues and not much with formal and informal issues (Siponen et al, 2007). This creates a gap in IS/IT security studies, as unbalanced IS/IT security implementation over the all three dimensions may not solve the IS/IT security issues in a holistic way because security problems are not only technical problems but also social, management and governance problems. The balance of IS/IT security implementation requires simultaneous actions among the three dimensions. For example, let us consider the case of one large financial institution in Malaysia.

Scenario 1

After conducting a security risk assessment over the logical element, IT-related, one of the IT applications identified, namely, the Finance Information System, it was found that the level of logical risk in one customer database system was demonstrated to be high. During the operation of the Finance Information System, the system had deficiencies, software bugs and user errors which always appeared during the operational business process, this annoyed the users of the system. These actions were considered to be unintended actions or not deliberate actions. The CIO, who leads the IT in the corporation was aware of and understood these problems, where vulnerabilities existed in some applications, he believed this would compromise the security of the system. When the system was down due to bugs, users were unable to process their work which caused delays, damages to business reputation and money loss. Later, security risk analysis was conducted by the risk management committee, quantifying the probability and assessing the likely severity of the consequences. Having analysed the logical, IT- related risk, the strategic way to deal with unavailability of the IT system was by switching the current IT system to an alternative system immediately in the case of the bugs and line errors. The management decided to mirror the IT system and its databases over one of the Bank's Servers in order to sustain business continuity without incurring major financial and non-financial losses. Putting this security control into effect does not guarantee security problems can be resolved holistically, because security is not just about technologies but is also involved with people and their reactions towards the technologies. The corporation seemed to ignore the informal dimension of IS/IT security implementation as software testing and risk management training related to security risk handling were not provided in the system development phase, just because the organisation wanted to minimise the budget but not the business risk; this created unbalanced IS/IT security in that corporation. It is claimed that the software testing and risk management training can be considered as a deterrent control for the corporation.

Figure 3.6 provides a conceptual framework for Malaysian publicly listed corporations to achieve the three dimensions simultaneously. The relationships between the three dimensions are shown by the intersections of the three circles in Figure 3.6. Each dimension has internal controls to enable management to oversee the implementation of its elements whether the objective is achieved or not; if not, this will be reported (Entrust, 2003-2004) promptly to the risk management committee.

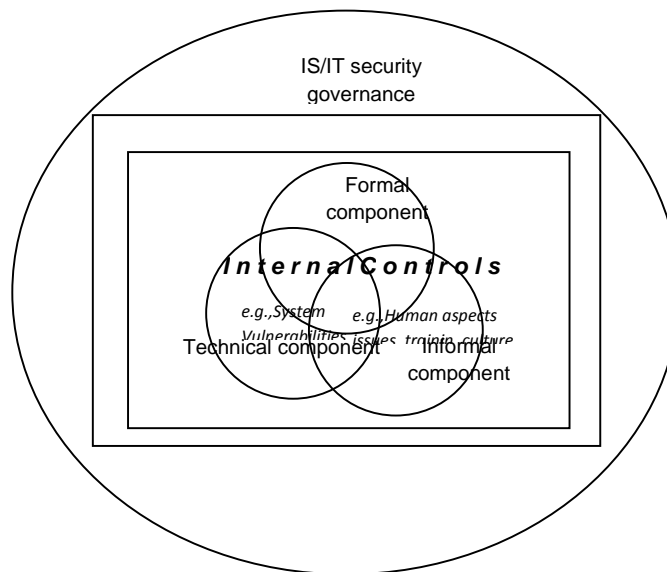


Figure 3.6 A model of IS/IT security governance

Figure 3.6 presents another view of the relationships shown in Figure 3.5 in order to emphasise the inter-relationships among the three components; these are indicated by the overlapping areas.

In the following chapter (4), the elements of the three components as shown in Figure 3.5 are considered in detail as are their inter-relationships. Some attention is also given to the identification of these inter-relationships in practice and to possible ways to minimise any damaging effects.

Chapter 4 A Model of IS/IT Security Governance: The Role of the Boards and Senior Management within Formal, Technical and Informal components

4.1 Introduction

In this chapter the model of IS/IT Security Governance is developed further based on the Conceptual Framework developed in Chapter 3. There are three components of this model: Formal, Technical and Informal. Formal relates to the IT security vision, IS/IT security management strategies, IS/IT security policies and IS/IT security standards to be implemented. The Technical component refers to the identification/determination of IS/IT areas and the establishment of security procedures over the IS/IT areas and business data which are aligned to the strategic vision, management strategies, policies and standards (if any), such as the software and hardware and the security procedures put in place. The Informal component relates to culture, beliefs and norms held by people including employee values and organisational values in the business process. Each of these components contributes to the development of the IS/IT security governance model. To achieve the IS/IT Security Governance Model, the alignments between the three components and the relationships are crucial for achieving IS/IT security governance, these include: Type 1- Formal/Informal (RT1); Type 2- Formal/Technical (RT2); and Type 3-Technical/Informal (RT3). In this model, the alignment and balanced interaction refers to when a single component has been implemented or about to be established, it requires a parallel interaction among the other two components in order to identify the deficiencies or missing requirements and characteristics of the other two components.

Basically, this model is suitable for both mature organisations and immature organisations. For a new corporation which has no policy in place to establish this model the corporation can initiate the risk analysis task by identifying the deficiencies from any type of these alignments, RT1, RT2 or RT3.

The model only covers a sub-set of IS/IT security governance issues, the implementation of risk management and the application of internal controls within the three components.

Throughout this model, the unit of analysis is the relationship between two entities in their supervisory roles. The first entity is called the giver (interchangeably referred to as supervisor) of the responsibility and the second entity is the holder of the responsibility. The Board, senior management and all management levels play an important role in providing the effective supervision by the giver in directing and monitoring actions over the holder throughout the three components and the interaction

among the three components. At the end of this chapter the IS/IT Security Governance Model will be compared with existing security models.

4.2 The Three Components of IS/IT Security Governance

4.2.1 Formal component

The Formal component is the formal processes that set the strategic direction of the organisation. They are approved for implementation by the Board and senior management. Figure 4.1 identifies three layers of the Formal component. IS/IT Security Vision, IS/IT Security Management Strategy and IS/IT Security Policy. When developing the IS/IT Security Policy, the organisation may define its own standards or follow external and industrial standards for implementing IS/IT security procedures to ensure that the IS/IT security policy achieves its goal.

IS/IT Security Vision is concerned with ‘what’ to achieve in IS/IT security while IS/IT Security Management Strategy looks at ‘how’ to achieve the stated vision relating to IS/IT security (Lineman, 2007). The organisation sets the IS/IT Security Vision and IS/IT Security Management Strategy through written policies. The purpose of developing policy is to achieve the strategies and IS/IT Security Vision. Writing the IS/IT security policy may require input from external standards such as national and international standards. Input from external standards will provide the guidelines and requirements for implementing a certain process or activity. However, the organisation can establish its own standards in order to achieve the policies. Standards are more flexible than policy. Standards can be integrated into any domain but policy has a boundary where it needs to be aligned with the IS/IT security vision of the company (Hone et al, 2002).

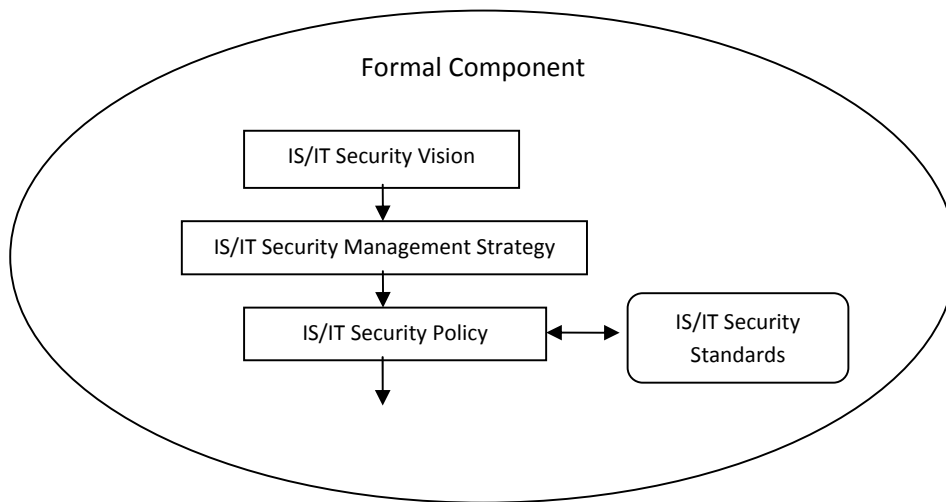


Figure 4.1. Formal Component of IS/IT Security Governance

The three layers seen in Figure 4.1 are inter-related and these Formal components set the framework for IS/IT security practices. To illustrate, the Board and senior management normally set the company vision, rules and regulations through policies (Solms, 2004). The presence of IS/IT security policy indicates the level of involvement of the Board and senior management in IS/IT security governance.

a) IS/IT security vision

The first layer of the Formal component as presented in Figure 4.1, IS/IT security Vision, is concerned with ‘what’ to secure in safeguarding the IS/IT areas of business. For example, the IS/IT are used in business operations for reporting, accounting, resource planning for manufacturing, marketing and human resources.

To establish the vision, the organisation needs to identify what IT areas, business processes and business data need to be secured. The IS/IT Security Vision is concerned with ‘what’ critical resources, such as accounting information systems and product design information system, based on the resource and risk analysis relating to IS/IT. Once the organisation has identified the potential risk areas, the sources of information are likely the lower levels, would help management to profile and compile a list of potential risks for the risk assessment stage. There are two examples of risks and risk owner from two different departments.

1. Department: Accounting Department, the risks were identified from the Accounting Information Systems and the risk owners identified were Accounting Staff as holder of the responsibility and Accountant as supervisor of the responsibility. The examples of risk were system failures and errors due to system vulnerabilities in coding lines of programming.
2. Department: Marketing Department, the risks were identified from the Product Design Information Systems and the risk owners were Sales Staff as holder of responsibility and Marketing Manager as supervisor of the responsibility. The identified risks from this department were confidential product design and parameters being accessible to unauthorised personnel, line sales and marketing staff.

Then later, the organisation needs to assess the level of IT risk so that the management or the giver (supervisor) of the responsibility may advise the level of risk tolerance, which needs to be established before risk mitigation can be considered, along with the establishment of appropriate internal controls. Of necessity, the IS/IT security Vision is a broad statement, for example, the IS/IT Security Vision is: To integrate IS/IT security within use of corporate IS/IT assets in relation to access to a particular IT system including its databases, business data, processes and networks.

b) IS/IT security management strategy

Once the IS/IT security vision has been identified, the next step is to formulate the organisation's IS/IT Security Management Strategy according to the aims of the IS/IT security vision statement. The strategy defines the direction for 'how' a corporation chooses to achieve its IS/IT security vision, analysing the resources, background and corporation's capabilities. As the research objective and domain of this study are concerned with the security of IS/IT resources and the organisation's business data, the formulation of IS/IT Security Management Strategy considers the criteria normally used in the strategic analysis for strategic information systems (Robson, 1997). These criteria include the nature of the environment, values and objectives and resources (Robson, 1997).

The nature of the environment considers a broad factor which may impact on the organisation such as, "demographic factors, legal, political or social pressures within which the organisation operates" (Robson, 1997, p 31). For example, in the context of Malaysian Corporations, all publicly listed corporations must comply with the Malaysian Code on Corporate Governance (2000), Listing Requirements by Bursa Malaysia, Financial Reporting Act and the Malaysian Act on E-Commerce (2006). As highlighted by Haniffa et al (2006), demographic factors such as major shareholdings

owned by non-executive directors and multiple directorships in different corporations may influence the organisation's decision in IS/IT security management strategies and development of IS/IT security policies.

Values and objectives refer to organisational culture as analysing the organisational culture may help management to determine whether the strategies are feasible and acceptable among employees. Robson noted that a strong culture is interpreted as "when the visible and underlying levels are consistent with each other and shared by all" and a weak culture is understood as "when the cultural levels are inconsistent with each other" (Robson, 1997, p. 43). Organisational culture is distinct and unique to one corporation. For example, the management should understand and know best about its customs and beliefs. The language spoken by employees has a significant influence on the organisation. For example, corporate management must be aware that in Malaysia there are three main ethnic groups-Malay, Chinese and Indian, in Sarawak (East) more than 40 sub-ethnic groups, Sabah (East) has more than 30 sub-ethnic groups), multicultural languages (e.g., Malay is a most common language in Malaysia, the Iban language and Kadazan language are the largest native languages spoken in East Malaysia, the English language is widely used in industries and is a compulsory subject at primary and secondary schools) and communication styles (e.g., e-mail, intranet used for putting up notices and policies, on-line leave application).

Resources analysis is also needed in order to determine the organisation's strategic capability based on the strengths and weaknesses of the organisation before the selected strategies are implemented. There are some tools available to analyse the resources for IS/IT security governance such as Porter's Value Chain Model and SWOT Analysis. Each of the tools has its own goal. The objective of using Porter's Value Chain is to identify primary activities and secondary activities, while the SWOT Analysis can be used to assess strengths, weaknesses, opportunities and threats that face organisations.

While the IS/IT Security Vision seeks to identify the broad and general view of IS/IT resources, the IS/IT Security Management Strategy addresses in specific detail which resources are primary or secondary to the business. For example, the organisation may use Porter's Value Chain model to identify the primary activities and secondary activities Primary activities have "a direct relationship with the organisation's customers", while secondary activities "facilitate the smooth functioning and have no direct relationship in adding values of organisation's customers" (Robson, 1997, p 48-49). The primary activities involve in-bound *logistics*, *operations*, *out-bound logistics*, *sales and marketing* and

services, while the secondary activities comprise *administration and infrastructure, human resource management, product/technology development* and *procurement* (Robson, 1997, p 48). By classifying these activities, the Boards and management including all management levels may be able to assess, prioritise and select the most effective and efficient IS/IT security management strategies over the activities that are aligned with business goals and the nature of the business, where security is not merely just a solution but a continuous process.

Apart from the Porter's Value Chain Analysis, the SWOT analysis is useful for the development of IS/IT security management strategies, for two reasons, first identifying the strengths and weaknesses relating to IT resources within internal factors and second, discovering opportunities and threats relating to IT resources within the external environment. For example, after determining the critical areas of IT resources in achieving IS/IT security vision, it is possible to assess the strengths and weaknesses of IT resources. Knowledge of the strengths of IT resources would be used for exploiting opportunities and knowledge of the weaknesses of IT resources would be used to counteract the threats and to repair the weaknesses.

These constraints need to be taken into consideration because each strategy has to be evaluated to measure its strengths and weaknesses before the strategies are documented and accepted within the corporation.

The following are possible examples of strategies to put in place the IS/IT Security Vision.

Strategies

1. Create a security plan for mitigation actions for identified incidents and a back-up management plan to address any IS/IT security deficiencies relating to databases within the IS/IT implementation.
2. Identify suitable internal control mechanisms for assessing the adequacy and robustness (that is, success or failure) of risk management over the use of the database system, IS/IT assets and business data.
3. Set up a framework for evaluating, monitoring and auditing the continued effectiveness of IS/IT security policies and its processes or activities after implementation.

4. Set up a programme of training and education to raise staff awareness about security in the use of data-base systems and measure their compliance with the specified procedures.

The above examples of strategies need to be approved by the Board after determining which are the most beneficial and best aligned with the IS/IT Security Vision. Once approved, policy will be developed according to the IS/IT Security Vision and approved strategies.

c) IS/IT Security Policy

The third layer following the Management Strategy is IS/IT Security Policy. Policy is developed for the approved strategies. Policies are higher level statements than procedures and should remain consistent over time (Lineman, 2007). Policies relating to IS/IT security are statements designed to maintain secure IS/IT assets and business data in terms of confidentiality, integrity and availability.

IS/IT security policy is a direction-giving document that indicates the commitment and involvement of senior management in IS/IT security (Hone et al, 2002b). Therefore, the policy document is a platform for communicating the Board's strategies and vision among the senior management and the lower levels. The policy also provides a framework for relevant organisational structures such as authorised users and defined roles, business IS/IT systems and data-base systems, e-mail systems and other types of business information systems. This information is derived from the intended strategies and IS/IT Security Vision Statement.

d) IS/IT Security Standards

IS/IT security standards place emphasis on the existence of processes and are not designed to be prescriptive policies (Hone et al, 2002). Standards can be employed to explain why processes need to be followed, consistent with the security policy in the organisation and wider industry.

In this study, a standard is an independent or stand-alone element. The IS/IT security standard may not impact on the formulation of IS/IT security management strategy but it may provide inputs for an organisational IS/IT security policy, if matched with security business requirements. A standard also can be used for the development of IS/IT security procedures, processes and activities. The use of IS/IT security standards in this model depends on the direction of the IS/IT security vision of the organisation. Standards ensure that certain procedures, processes or activities exist to achieve the goals set out within the policy requirements.

The Technical component is examined in the next section.

4.2.2 Technical component

The technical component concerns the implementation of IS/IT security procedures over IS/IT areas for achieving the organisation's strategic vision, strategies, policies and standards. There are two layers in the Technical component: first is the Technological Areas; and second is the IS/IT Security Procedures.

a) Technological Areas

The Technological Areas focus on the IS/IT areas that need to be secured based on the potential risks identified, as shown in Figure 4-2. The IT risk identification process provides important input to determine which IS/IT areas need to be secured and aligned with the IS/IT security vision.

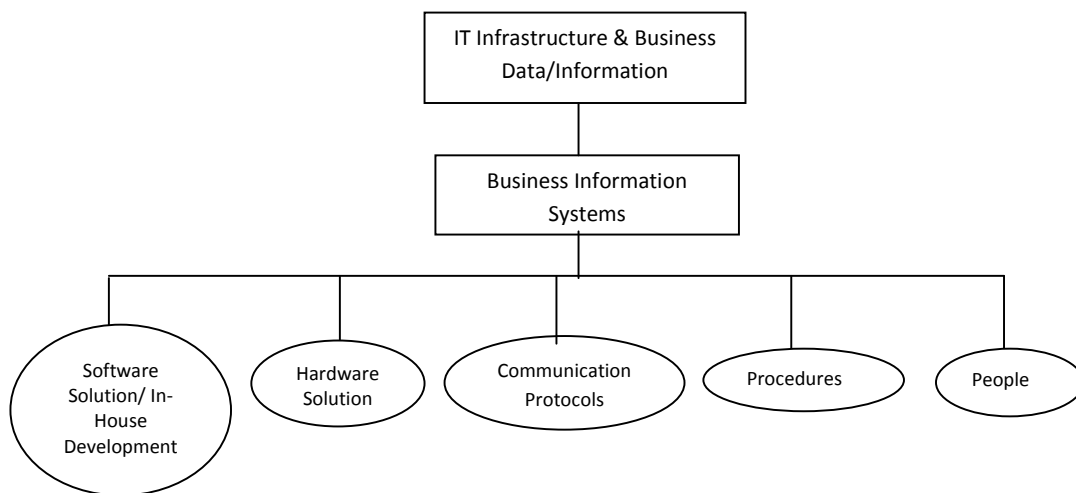


Figure 4.2. Technological Areas of Technical component

There are two layers of the technological areas. The first layer deals with the foundational components; it includes IT infrastructure and business data and information. The second layer encompasses Business Information Systems which derive the business value from the foundational components.

i) IT Infrastructure and Business Data and Information

IT infrastructure is the

physical facilities, IT components, IT services, and IT personnel that support the entire organisation including software, hardware and communication technologies that provide the foundation for all of an organisation's systems"

for enabling and achieving business goals (Rainer et al., 2011 p 11). In this model, business data and information refer to all sensitive and confidential data that are "exposed to elements such as the technology, stakeholders and business processes" (Posthumus et al. 2004 p 639). Conceptually, both IT infrastructure and business data are inter-related because IS/IT security procedures will not work without the presence of business data or having IT infrastructure in place. Figure 4.3 presents the elements of the Technological Areas.

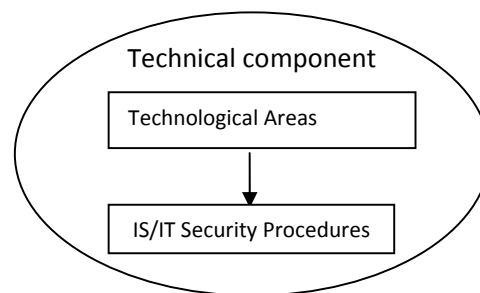


Figure 4.3. Technical component of IS/IT Security Governance

IT infrastructure has become the backbone for achieving business operations, as it is a tool that enables decision making, production, marketing, manufacturing, finance and human resource management (Rainer et al. 2011). Business data comprise all the confidential information of the corporation including financial, accounting, business strategy and customer data.

To preserve the confidentiality, integrity and availability of the business data and information, a range of IT security controls and counter-measures can be used to mitigate concerns about risk in the use of IT infrastructure. The more strategic IS/IT security control was introduced by Straub et al (1998), as shown in Chapter 2- Literature Review, where four lines of security controls/counter-measures including deterrence, preventive, detective and remedy were applied in Straub's model in order to cope with IS/IT risks. In this conceptual framework, the first two lines, deterrent and preventive controls, will be primarily applied within the development of the IS/IT security governance conceptual framework, because both lines imply a combination of passive (deterrent) and active (preventive) approaches. For example, the deterrent control includes a passive approach such as education, training, awareness programmes, rules or guidelines of the organisation for IS/IT security, and the preventive control includes an active approach such as automatic IS/IT security systems,

password access controls, finger prints authorisation, voice and face recognitions tools/technologies for authorisation purposes.

The confidentiality, integrity and availability of the business information may be preserved using more than one security counter-measure or combination of many. In order to address the risk, the management can employ as many security counter-measures as needed, all aligned with business goals. For example, the IT Manager who discharges his obligations in securing the access to particular IS/IT systems may use a combination of the deterrent (i.e., policy) and the prevention (i.e., password access controls and finger prints device) to protect sensitive business information from being accessed by unauthorised and irresponsible people in the real-time situation.

ii)Business Information Systems—Deriving value from IS/IT components

Business information systems are technological solutions based on the business requirements (Rainer et al, 2011). They are aligned with the company goals and objectives. Five components of business information systems were identified for this framework. These are software, hardware, network, procedures and people as quoted below in the dot-points (Rainer et al. 2011).

- Software relates to databases or computer-based applications systems that “enables the hardware to process data”
- Hardware are machines and devices relating to IT such as the processor, monitor and printer where “these devices accept, process and display data and information”
- A network “is a connecting system either wireline or wireless that permits different computers to share resources”
- Procedures are “the set of instructions about how to combine the software, hardware and network components in order to process information and generate the desired output”
- People are “those individuals who use the hardware and software, interface with it, or use its output”

The five components of business information systems are important to organisations because they provide solutions to support the business operations. This relationship was illustrated in Figure 4.2. Two main functions of business information systems are identified for this framework. The first

function of business information systems supports integration of physical parts such as departments and functional areas of organisations (i.e., Accounting Information Systems, Human Resource Information Systems). The second function supports the entire organisation (i.e., Enterprise Resource Planning, Transaction Processing System) (Rainer et al. 2011). However, the specific details of each function are determined according to the business goals of the organisation.

While IT infrastructure provides “the basis for information systems in the organisation”, business information systems “collect, process, store, analyse and disseminate information for specific purposes” (Rainer, et al. 2011, p 38-39).

In this model, the Formal component plays an important role in identifying risks associated with the use of business information systems. The identified risks will determine the IS/IT security management strategy and IS/IT security policies. Once the Formal component is determined, the next stage is to establish the procedures implementing the policies.

b) IS/IT Security Procedures

IS/IT security procedures which consist of security controls and security counter-measures are “the detailed steps that employees follow” (Lineman, D, 2007), to implement the IS/IT security policies. After identifying which Technology Area is to be secured, IS/IT security procedures will be documented and implemented within the organisation.

Figure 4-3 shows that IS/IT security procedures are dependent on specific Technology Area processes. The Technology Area is governed by the Formal component provided by the IS/IT security vision, IS/IT security management strategy and IS/IT security policy. For example, each organisation from any industry has its own data security or information security requirements over the use of IT resources including software, hardware and business information. To determine the right technological areas and IS/IT security requirements, the previous sub-section, namely, IS/IT security management strategy, discussed and provided guidance such as the use of resource analysis to determine the intensity of use (much/medium/least) of IS/IT in achieving business vision and goals. Once the Technology Area has been determined, IS/IT security procedures will be established accordingly.

The IS/IT security procedures outline the security activities that need to be established over the identified technological areas. Both layers, the IS/IT security procedures and Technological Areas are the realisation of the IS/IT security policies established in the Formal Component.

In the Technical component, the IS/IT security procedures are dependent upon the Technological Areas. The establishment of IS/IT security procedures depends on the direction provided in the Technological Areas in terms of ‘what’ to secure (the Vision), ‘how’ to secure (Management Strategy) and ‘what’ to implement (Policies Documents) (Posthumus, et al. 2004), as set out in the Vision Statements for the organisation. Therefore, it can be seen that in this framework the Formal component plays a significant role in the development of the technical component.

4.2.3 Informal component

The third component of IS/IT security governance, namely, the Informal component, is dealing with the people and human aspect issues within the implementation of IS/IT security. As introduced briefly in Chapter 2, Dhillon et al (2000) pointed out that contemporary processes of protecting IS/IT in organisations involve not only maintaining the confidentiality, integrity and availability of IS/IT but also engaging human aspects including the responsibility of employees, integrity of people, trust and ethicality (Dhillon et al, 2000). In addition to that, the definition of human aspects terms are presented; integrity is a “part of the requirement of membership of an organisation” (Dhillon, 2000, pp. 127-128). Trust is a “self- control and responsibility and less emphasis on external supervision” (Dhillon, 2000, p 127-128). Ethicality involves compliance with the company code of ethics and “the ethical content of informal norms and behaviour” (Dhillon et al, 2000, p 128).

Responsibility is knowledge of roles and separation of duties, the employees are expected to exhibit “their own practices on a basis of clear understanding of their responsibilities” and being accountable for what has gone on in the past and development of events in the future (Dhillon et al, 2000, p 127). The definition of the Informal component of this conceptual framework covers the structure of responsibility, integrity, trust and ethicality.

As clearly stated in Chapter 2, the Informal component of this conceptual framework is also related to the security culture, norms of employees, employee beliefs and personal values (Mishra et al, 2007). As noted by Mishra et al (2006), a lack of security culture results in problems of maintaining integrity of the whole organisation and indirectly threatens the protection of technical systems. In addition, the security culture in an organisation has been emphasized in the literature. For example, the greater involvement of the Board and senior management improves the security culture of an organisation (Knapp et al, 2006). The explanation of Knapp et al’s research methods and findings are presented in Chapter 2.

Moreover, Mishra et al (2007) has stressed the important role of human factors in solving IS/IT security problems and has suggested establishing normative controls. Normative controls are a by—product of a dominant security culture which is the totality of behaviour in an organisation that contributes to the protection of all kinds (Mishra et al, 2007). Cultural norms are behaviours and practices that already exist within the corporation perhaps from the environment at the physical location of the organisation.

Figure 4.4 shows that the Informal component of this conceptual framework involves culture, norms and beliefs. In this framework, the culture, norms and beliefs of an organisation are influenced by two elements: employee values and organisational values.

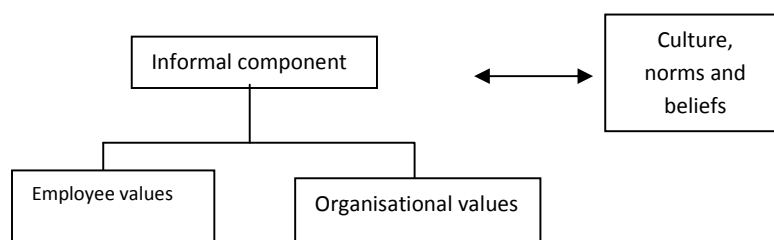


Figure 4.4. Informal component of IS/IT security governance conceptual framework

The research issues of behavioural aspects by Mishra et al., such as values, attitudes and norms are important for the development of personal and organisational values. The behavioural aspect of information systems security governance relates to conformity with the policies and procedures of the organisation and management of people (Mishra et al, 2007).

Furthermore, the model of IS/IT security governance in this study has drawn upon Dhillon's (2007) model where it is claimed that employee values are considered to be related to people's integrity, trust and ethicality while organisational values are concerned with structures of responsibility. Dhillon et al (2007) found that two determinants, structures of responsibility and the integrity of people were the most important factors for behavioural security.

The two specific elements of the Informal component are now discussed.

a) Employee values

Employee values relate to the personal and ethical values of individuals within the organisation (Gaunt, 2000; Wood,2002; Stanton,2004). Attitude of staff, commitment, user behaviour, high levels of trust and integrity are examples of the personal values of employees. The ethicality of employees

involves compliance with the corporation's code of ethics and the external standards of work practices (Dhillon et al, 2007). Employee values held in an organisation may be appropriate or not appropriate for effective IS/IT security implementation, depending on these values and beliefs. For example, the organisation sets policy for the use of security software to protect IS/IT assets and business data from viruses, worms, malicious attacks and other possible forms of attack. One of the procedures stated in the policy is to conduct virus scans periodically over the computer desktop drives and folders. Those who do not follow and comply with the procedures from the policies are considered as lacking in integrity and trustworthiness. Employees with low integrity and trustworthiness will bring risk to the company's IS/IT implementation, as failure to perform the virus scan procedure will expose the systems to threats and vulnerabilities.

Putting policy in place was the example of deterrent controls, where it can be used to control the human actions from committing deliberate or non-intended actions in a passive approach. The example of deterrent control was discussed in an earlier section; the use of four security controls and counter-measures for coping with the IS/IT security risks from the informal aspect is now discussed: deterrent control, preventive, detective and remedy. If the deterrent control is not effective in controlling human actions, the preventive control line will take place. The organisation needs to have strong access controls such as passwords, finger prints, or face recognition in order to control actively and protect the IT system from modifications and data manipulation. Automatic IS/IT security systems such as an Intrusion Detection System, are software applications that monitor the system activities and network for monitoring malicious activities or policy violations and produces reports to a management station (in this case, the IT Department). The Intrusion Detection System may attempt to stop (actively), alert and notify (passively) any intrusion attempts on any suspicious and abnormal activities of employees in the organisation on a real-time basis.

b) Organisational values

The Informal component of the IS/IT security governance framework is also concerned with the organisational values which may influence the business processes. Organisational values are expectations of the Board on the ways in which employees should work and interact with each other in achieving IS/IT security governance and other duties. This includes the establishment of structures of responsibility and authority for the success of IS/IT security, involving the identification of agents (e.g., individual, group, department), identifying their roles and associated actions (Backhouse, et al., 1996). Furthermore, Dhillon et al. (2007) added that structures of responsibility also involve the establishment

of supervisory roles, the separation of duties and establishment of start and finish times of the authority (e.g., when she/he retires, contract ends). The structures of responsibility, if practically and consistently implemented, will become part of the cultural norms in a corporation (Solms et al, 2004). As Solms et al note that the structure of responsibility is derived from the policies and if the employees show conformity with the policies, the security culture will be automatically formed and cultivated. In the previous section on employee values, the policy was used for deterring human actions but in this section the policy is used for structuring the responsibility of security roles.

In summary, ineffective and inefficient controlling of IT risks from the Informal component will lead to corporate failure. Employee values and organisational values are part of the Informal dimension and the effective implementation of the Informal dimension still requires interaction between Informal, Formal and Technical dimensions.

In order to align these relationships management must provide managerial reports on employee values and organisational values from lower levels. If the problems at lower levels cannot be resolved, the supervisor of the responsibility should assess and report the problems to upper levels for decisions and actions. This is because not only does the supervisor have the responsibility but the holder of the responsibility is also responsible to discharge his/her obligations in IS/IT security, such as reporting.

4.3 A model of component Interaction

Most organisations today pay little attention to the inter-relationship between the Formal component, Technical component and Informal component (Koskosas et al, 2004, Backhouse et al, 1996, Solms et al, 2004, Mishra et al, 2007). The Board and senior management of organisations tend to focus more on narrow aspects such as IS/IT management rather than on a comprehensive view (Siponen et al, 2007). Deficiencies in any of these three components may result in unbalanced IS/IT security implementation. The objective of this study is to integrate the three components simultaneously throughout the IS/IT security implementation. The model of IS/IT security governance is a comprehensive conceptual framework because it emphasises the two-way relationship between each of the components, which, in this research context, means a concurrent implementation including the Formal component such as policy, the Technical component such as software or hardware and the Informal component such as culture of the employees of the organisation. The main interactions of the three components—Formal, Technical and Informal are shown in Figure 4.5. This is because IS/IT security governance and its implementation are influenced by the Formal, Technical and Informal

components. The nature of these relationship(s) highlights that interactions among the components are complex.

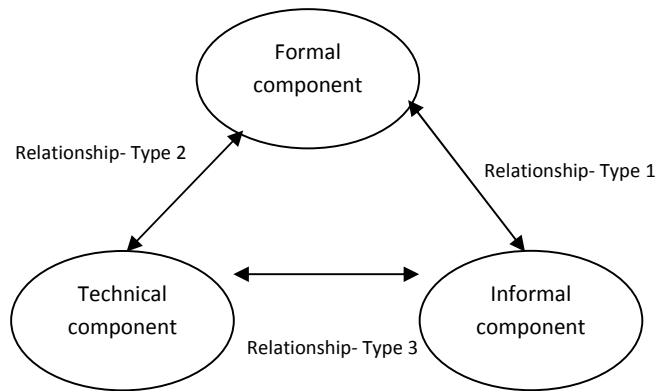


Figure 4.5. Relationships between Formal, Technical and Informal components

Three primary “influence” relationships were identified as shown in Figure 4.5. First is a two-way relationship, Type 1, between the Informal and Formal components, the second is a two-way relationship, Type 2, between the Formal and Technical components while the third is a two-way relationship, Type 3, between the Technical and Informal components. Each relationship is two-directional implying that the related components affect the formation and details of each other.

4.3.1 Relationship-Type 1 (RT1)

To simplify discussion from this point Relationship Type 1 (RT1), the relationship between the Formal and Informal components, will be referred to as RT1. It is expected that the implementation of IS/IT security requires balance between the Informal component and the Formal component. The Formal component needs to be aligned with the Informal component. For example, the implementation of an IT security policy has implications for organisational culture. This notion can be seen in the work of Solms (2004) who argued that the objective of security policy is to dictate the security behaviour of a corporation’s employees through a proper education process (Solms, 2004). However, educating employees to influence security behaviours is a challenging task in an organisation because it requires consistent, time -consuming and effective processes such as providing courses, training and refreshing security awareness to ensure that a security culture is cultivated.

The implementation of IS/IT security requires the alignment of the Informal component with the Formal component. The Informal component, like personal values, local and organisational culture, needs to be aligned with the Formal component. An example of local culture is geographic location

where the cultural environment of one location differs from another location. In Malaysia, corporations are influenced by regulations such as the Malaysian Code of Corporate Governance but in other countries the requirements may be different.

In RT1, the Informal component is worked in parallel with the Formal component, for example, policy is developed with reference to the corporation's culture, norms and beliefs. In this type of relationship, the Informal component is associated with the Formal component by identifying the culture, norms and beliefs of an organisation before the Formal component is developed. By making reference to the culture and norms of corporations, policies become more effective because the corporation has incorporated individual beliefs and organisational values within the policy. For example, the writing style of formal documents should reflect the culture of an organisation to ensure that the documents are accepted and understood by all the employees from different backgrounds (Linemann, 2007).

Another example of how the Informal component is associated with the Formal component is establishment of supervision and employee's roles (Informal component) within the security policy (Formal component). Management will be aware of the strengths, weaknesses, attitudes and capabilities of employees after receiving the security reports and security incidents results from the lower levels. Management will use this knowledge in the selection of individuals to be involved in an IS/IT security role. In other words, the Informal component assists management to make decisions on which team or individual would be most suitable for implementing a security role based on the personal values of the employees and the culture.

Figure 4.6 shows how the Formal component is connected with the Informal component.

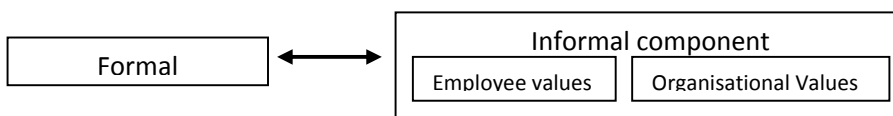


Figure 4.6. Formal component has a relation to Informal component

Education, training and awareness programmes are examples of the Formal component (Brian, 2001). Human resource needs such as education, training and security awareness programmes are important for the development of employee values and also organisational values. In this conceptual model the Board and senior management need to have effective risk strategies by providing the Formal component such as continuous education, training and policy awareness programmes in order to

improve employee values and organisational values because IS/IT security risk issues are mainly caused by human actions (Dhillon et al, 2007). IS/IT security risk management components may help the Board and senior management to detect if any potential IS/IT threats were caused by human actions. Human actions relate to structures of responsibility (organisational values), supervision roles (organisational values), people with high integrity (employee values), trust among people (employee values) and ethicality (employee value).

4.3.2 Relationship-Type 2 (RT2)

The second relationship, Type 2 (RT2) considers the relationship between the Formal and Technical components. The need for alignment between the Formal component and the Technical component is emphasised in this relationship. The Formal component sets the strategic direction for the technologies and the technological implementation based on the corporation's vision and policies. To have an effective Formal component, the organisation also needs to have an effective implementation of the Technical component so that the goal of IS/IT security can be achieved. A review of implementation of the Technical component may reveal discrepancies or identify improvements needed such that a review of the Formal component may be appropriate leading to changes to the Technical component. For example, to protect the data-base system and its critical data successfully, the policy may need to incorporate additional security software so that the alignment between the Formal component and the Technical component can be achieved.

However, after implementation, the outcomes of the Formal component and the Technical component may need to be realigned. For example, if the security level as set out in the policy was found to be too low, the policy or its implementation strategies will need to be reviewed and improved. Then, the corresponding Technical component will need to be altered to raise the level of security in order to achieve effective IS/IT security.

The Technical component will inform the Formal component of the acceptance of the corporation's vision and policies among employees. Let us consider the following scenario. The IS/IT security reports of a corporation show that the number of Spams has increased gradually over the past few years. The management found that Spam filter software has not reduced the number of Spams. Hence, to improve the deficiencies of the Technical component it may be necessary to review policies and IS/IT security management strategies to determine if any up-dates are needed. In this case, the

management may have to reshuffle the IS/IT strategies by implementing Virtual Private Networks to heighten the security over the corporation's network.

4.3.3 Relationship Type 3 (RT3)

Finally, the third relationship, Type 3 (RT3) refers to the relationship between the Informal and Technical components. The alignment of components is needed in this type of relationship to achieve IS/IT security. Misalignment of components may increase business losses in the organisation because up to 70% of the security incidents by number are due to non-deliberate actions, e.g., ignorance of responsibility (McIlwraith, 2006). This study identified that the major reason for these incidents was the lack of supervisory roles and unclear structures of responsibility in security roles in the organisation.

The implementation of the Technical component is likely to be associated with the Informal component through the values of the workers and of the organisational values. This may be quite subtle and be reflected in the understandings of what implementation actually means. For example, an understanding of what security means and the sharing of permissions to access certain security levels are examples of how the Informal component needs to be aligned with the Technical component. The values of workers are important in the Technical component because security issues are mainly social problems (Dhillon et al, 2000), where security procedures cannot be successfully implemented without high employee values and high organisational values. For example, individuals who have inadequate employee values and lack of supervision by their higher management may be able to change the security of a company's database settings and its system privileges for achieving their own benefits or other intentional acts. Lack of organisational values also has a link to the state of employee values, such that unclear structures of responsibility and supervisory roles may lead to bad corporate governance practices (e.g., employees repeat making errors due to no controls and effective monitoring by supervisor, the upper management level).

Conceptually, the Informal component and the Technical component are partners and need to be balanced with each other. An effective Informal aspect such as norms and beliefs, including employee values and organisational values, may improve positive employee perceptions of job responsibilities in certain IS/IT system procedures. The management should draw upon the culture, norms and beliefs of the organisation before embarking the Technical component on real practices. The employee values and organisational values play significant roles in achieving IS/IT security procedures (Dhillon, 2000).

However, conversely, the Technical component also needs to be aligned with the Informal component. In this case, the implementation of IS/IT procedures may reveal discrepancies and unexpected behaviour from the employees such as stealing and altering other employees' data. If any deficiency happened in this relationship, the organisation also needs to revise or have effective management strategies to determine the capabilities of the organisation (e.g., strengths, weaknesses, threats, opportunities) in order to achieve IS/IT security. In the Technical component, the management will review the technological reports such as the network log, database access log, malicious activities, log information about said activities and report activities. If the upper level management or supervisor of the responsibility finds any suspicious activities in the employees' actions, the supervisor has the responsibility to give advice, reprimands or soft reminders to ensure that they comply with the rules, policies and technical procedures of IS/IT security. From the management perspective, once the potential IS/IT security issues have been identified from the Informal component, assessment and mitigation need to be addressed effectively and efficiently in the technical component. For example, the management needs to consider the mitigation in the technical perspective, where IT security controls seemed not effective enough, the real time/automatic security system controls including the Intrusion Prevention System (extension of Intrusion Detection System) is required to be actively in place to stop deliberate or unintended acts that are detected coming into IT systems and internal networks. There are a few technical processes identified about how Intrusion Prevention Systems prevent and block intrusions that are detected by the actions;

1. *Sending an alarm.*
2. *Dropping the malicious packets.*
3. *Resetting the connection.*
4. *Blocking the traffic from the offending IP address.*

(Boyles, 2010, p. 258)

4.4 Risk Management and Internal Controls: Relationship with the three components and interaction model

The three types of relationships among the components, namely, RT1, RT2 and RT3, have been explained in detail. In this section, discussion takes place on how risk management and internal controls are inter-related as well as how they integrate with the three components and their interactions.

This study aims to develop a governance framework for the effective and efficient implementation of IS/IT security. Effective and efficient IS/IT security requires that risk management for the three components with appropriate internal controls are in place.

4.4.1 Relationship between Risk Management and Internal Control

Internal controls are a part of the risk management process. Figure 4.7 depicts the relationship between risk management and internal controls.

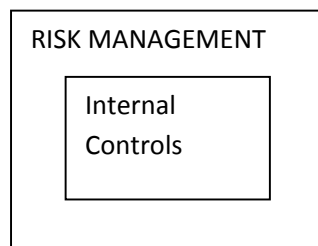


Figure 4.7. Relationship between risk management and internal controls

Risk management and internal controls are inter-related processes. The example of this relationship is illustrated in Table 4.1a and Table 4.1b explain how internal controls are part of the risk management process. They consist of two major parts: the first part presents the relationship between risk management and internal controls; and the second part generally provides the monitoring and review activities against the first part. Some parameters used in the first part were based on variables used by Cooper et al (2004), a *standard worksheet* of risk identification and assessment.

In this model, the study considers three main stages of risk management activities: risk identification; risk analysis and assessment; and risk mitigation (Standards Australia and New Zealand, 2004). Throughout the risk management process within the model, the monitoring and review activity takes place (Standards Australia and New Zealand, 2004). The standard defines

- risk identification as “what is at risk”, for example, identify which IS/IT areas and business data that are at risk in the business
- risk analysis and assessment provide a view and relative importance of the identified risks, as aligned to the IS/IT security vision
- risk mitigation concerns the action plan and contingency planning in response to identified risks, e.g., IS/IT security systems controls

- monitoring and review, e.g., the supervisor of the responsibility should ensure the resources are effectively conducted by employees, through detecting, recovering and fixing the deficiencies

(Standards Australia and New Zealand, 2004, pp 3-4)

In Table 4.1a, after the potential risks have been identified from the procedural processes or activities, the next process is to analyse and assess the risks to show their relative importance. In the risk analysis and assessment stage, the organisation can categorise the risk either high risk impact or low risk impact based on organisational requirements (Cooper, 2004). The management of the organisation has the power to set the risk privilege accordingly as given to the nature of business, business goals and security requirements of the organisation. The first two stages of risk identification and risk analysis and assessment are to identify, analyse and assess what potential IS/IT risks exist in the IS/IT infrastructure and business data.

	Risk Management & Internal Controls	
	(1)Risk Identification	(2)Risk Analysis & Assessment
Policy/Procedure/Process	Identified Potential Risk	Risk Assessment Likelihood of Risk Impact
Policy: Password Controls Procedure: Changing of password. The policy requires an employee to change at least a minimum of 5 times and maximum of 12 times	Frequency of password changes may not be adequate. No password changes being done by employees	High
Policy: Access Authorisation for database data Procedure: Security Access Levels	Access to data elements may be available to unauthorised users	High

Table 4.1 a) Examples of relationship between Risk Management and Internal Controls

The third stage, in Table 4.1b, risk mitigation, addresses how to minimise the IS/IT risks by providing internal security controls in place. The Board and senior management need to ensure that the monitoring and review process happens across all the stages.

In general view, this model identifies that security internal controls are part of the risk mitigation. Security internal controls as part of management internal controls strategy can be applied within the risk mitigation stage, by ensuring that organisations implement security controls software and hardware or related IS/IT.

	Risk Management & Internal Controls		Monitoring and Review
	(3)Risk Mitigation		
Policy/Procedure/Process	Current Internal Security Controls	Recommended Security Internal Controls	Monitoring Technique
Policy: Password Controls Procedure: Changing of password. The policy requires an employee to change at least a minimum of 5 times and maximum of 12 times	None	The organisation should review Password Controls and its Password Log Reports.	Ongoing Check-Senior Manager will ensure the employees have performed regularly the change of password procedure
Policy: Access Authorisation for database data Procedure: Security Access Levels	Yes. The data dictionary for security access privileges is documented in the procedure	The organisation should also review Password Log Reports, Network Log or Firewall Logs to detect any significant or suspicious events	Ongoing Check: Senior manager will ensure the monitoring and review of the related log reports to ensure only authorised users have access to certain data elements

Table 4.1 b) Examples of relationship between Risk Management and Internal Controls

The risk management process and the monitoring and review of the model are discussed next. There are three stages of risk management, the first stage is Risk Identification, the second stage is Risk Analysis and Assessment and the third stage is Risk Mitigation. The discussion is followed by the important role of monitoring and review within the risk management process.

4.4.2 Stages of Risk Management and Monitoring

a) Stage 1: Risk Identification

Understanding the objectives of the organisation is a key to the risk identification (Standards Australia and Standards New Zealand, 2004). As Table 4.1 shows, the risk is identified from the implementation of Policy and its procedures within the organisation. This model has identified the potential risk from the implementation of policy because policy is a Formal documentation to be used for achieving the objectives of the organisation (Doherty, et al., 2006).

b) Stage 2: Risk Analysis and Assessment

The measurement of the procedural processes and activities is an example of the Risk Analysis and Assessment. First, once a specific activity has been identified as a potential risk, then the risk assessment will be undertaken to assess the likelihood of risk impact associated with the risks identified. Potential impact can be measured using two categories, High Risk Impact or Low Risk Impact (Cooper et al., 2004), as seen in the Risk Assessment column in Table 4.1, high risk impact or low risk impact may cause monetary losses or loss of reputation if not mitigated effectively. The risk assessment result of either low or high potential impact is dependent on how much alignment occurs between the IS strategic goals and IS/IT security (National Cyber Security Summit Task Force, 2004). Misalignment between IS/IT strategy and IS/IT security may lead to misleading risk assessments and incorrect risk mitigation processes.

The model of this study will examine whether the identified risk has had internal controls applied to it. Secondly, if no internal controls have been applied for the current activity, the Board and senior management will require the development and implementation of internal controls as part of the mitigation to control that risk. In this model, if organisations do not have security internal controls in place, they may develop effective and efficient security internal controls. If security internal controls are already implemented within the current process, then the model may identify deficiencies and enhance the mitigation strategy by identifying security internal controls.

c) Stage 3: Risk Mitigation

Risk Mitigation will be undertaken based on deficiencies found in the risk identification and risk analysis and assessment. Assessment (as identified earlier in Stage 2, Risk Analysis and Risk

Assessment) provides an important input to the Risk Mitigation process, namely, security internal controls and monitoring techniques.

Within the risk management process, Risk Mitigation provides a strategy and solutions for minimising associated risks. Security internal controls are part of Risk Mitigation activities in this framework. Security internal controls as part of the mitigation process are used as a tool to reflect whether the activities including IS/IT security policy, procedures or processes have been performed in an effective and efficient way.

d) Monitoring and Review

The monitoring activity over the risk management process is crucial to ensure IS/IT resources are used effectively. The outcomes of the risk management processes need to be reviewed so that the management knows what is lacking or any improvement needed for certain areas

Examples of the potential IT risks of each of the three components are presented below.

- Formal component: IT incidents such as malicious attacks pose a risk to the corporation if there is a lack of policy relating to IS/IT security. Where no IS/IT security policy is in place, organisations appear not to be managing corporate IS/IT risks.
- Technical component: System deficiencies, bugs, code errors, viruses and spams are examples of IT risks to corporations from the Technical perspective. This type of risk if not mitigated may expose corporations to threats and system vulnerabilities.
- Informal component: Human error, lack of knowledge, lack of training, dishonesty and lack of trust and integrity are examples of IT risks arising from the Informal perspective. If informal risks are not addressed, this may impact on the quality of the Technical implementation.

The model shows that the implementation of IS/IT security governance is entirely weighed by these three components. The absence of one component may lead to misalignment of IS/IT security governance implementation by the organisation.

4.4.3 Risk Management and Internal Controls

4.4.3.1 Risk Management and Internal Controls: Formal component

Risk management and the application of internal controls are important to the Formal component like IS/IT security policies. Risk management is needed within IS/IT security policies development and implementation because it identifies, assesses and mitigates the potential IT risks from any deficiencies, threats and vulnerabilities.

This conceptual model identifies that the application of risk management and internal controls influence good practices of the Formal component like IS/IT security standards. In terms of risk management, every guideline provided by IS/IT security standards, if implemented effectively, may control the risks associated with IS/IT use. Internal controls can be used to ensure that standard practices are consistent with policy goals. For example, after the risk identification stage, the organisation may provide a checklist of appropriate standards for implementing the processes or activities.

Policy relating to IS/IT security may provide a measurement tool so that the expected benefits of the approved strategy including procedure goals can be assessed. This measurement is an example of the application of internal controls. An effective internal controls application over risk is required in this framework to gauge the success of risk management in securing IS/IT systems and assets.

4.4.3.2 Risk Management and Internal Controls: Technical component

In this model, the implementation of risk management and internal controls over the Technical component is crucial. It is important to note that the Technical component has links with the Formal and Informal components.

The Technical component comprises two elements, namely, the technological areas stage and the procedures stage. The technological areas stage concerns the IS/IT required to be secured and to be aligned with the IS/IT security vision, while the IS/IT security procedures stage provides the steps to establish security solutions or counter-measures. Risk management and internal controls have a significant role to ensure that risks from the Technical component are managed and the IS/IT resources are used effectively and efficiently.

Through this model, the organisation has a proper way to identify and manage the Technical risks within the technological areas stage. Since the technological areas stage is aligned with the IS/IT

security vision, any potential IS/IT risks identified in the Technical component are becoming risks to the business. The CIO who is responsible to advise on the risks reported from the lower levels like the IT manager, needs to monitor and react effectively and efficiently over the daily, weekly or monthly security reports regarding the IT system vulnerabilities and threats. The IT Manager is responsible to manage and maintain the security of resources, by identifying and assessing the risks and promptly reacting at this level if deemed necessary but, if not workable, the matter needs to be discussed at a higher level, the CIO level.

In the technical dimension, the IT Manager should be able to fix the IT systems and databases presenting any vulnerabilities and threats through input from the Programmers Staff and IT Technical Staff. For example, the IT Technical Staff such as Database Administrator (IT Technical Staff) who is normally involved with the administration of databases applications, found the e-mail spams have threatened and jeopardised the business data, where, by opening the e-mail spams may expose the IT systems to viruses and lead to the loss of business information. In this situation, the Database Administrator (IT Technical Staff) is responsible to provide the IT security solutions such as Intrusion Detection and Prevention System (IDPS), primarily focused on identifying possible incidents, logging information and reporting attempts (Scarfon et al., 2007). The following are four types of IDPS technologies that are significant for this model: 1) Network-based; 2) Wireless; 3) Network Behaviour Analysis; and 4) Host-based.

- *Network-based, which monitors network traffic for particular network segments or devices and analyses the network and application control to identify suspicious activity.*
- *Wireless, which monitors wireless network traffic and analyses it to identify suspicious activity involving the wireless networking protocols themselves.*
- *Network Behaviour Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial service (DdoS) attacks, certain forms of malware and policy violations.*
- *Host-based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.*

(Scarfon, et al, 2007, p ES-1)

The above security technologies-IDPD, can be used as preventive controls in stopping, detecting and halting the potential threats and preventing unintended activities from coming into the corporation's private network or, if deemed necessary, this matter should be discussed, communicated

and reported directly to the IT Manager for further decisions and strengthen the IT security internal controls.

Internal controls which are part of risk management help organisations to ensure that the technological areas including its policies and IS/IT security procedures are effectively and efficiently implemented. The management of an organisation is responsible to establish and improve internal controls within the technological areas and the IS/IT security procedures. However, to achieve the internal controls depends on the involvement of the Board, senior management, the lower levels including junior managers and operational staff. For example, after risk assessment was conducted by the IT Manager, it was found that the increased number of e-mail spams was due to external threats from outsiders; incoming e-mails had penetrated the corporate e-mail system and intranet. The security controls installed were not protective enough. Therefore, two types of internal controls systems would be needed to control the risk. The first type is the automatic application of Intrusion Prevention Detection installed and operated within the database applications and network, to block reactively the suspicious activities. The second type is the passive internal controls system for monitoring the activities over the use of IS/IT. In the passive internal controls system, for example, the system will give alerts and signals of potential security breaches through the information logs.

The first type of internal control is now discussed further. The CIO may receive feedback from the IT Manager, where the IT Manager may advise the CIO to heighten the system by installing a real-time IT security controls system within the application, such as automatic anti-spamming software enables to prevent the spammer's tactics getting through into the corporation's private network. The anti-spamming software may stop the up-coming e-mail spams coming into employees' e-mail. If the suspicious activities are detected, the anti-spamming software will notify the IT Technical Staff through alert notices or on the screen alarms for active reaction purposes.

Apart from the automatic responses, the second type of internal controls is the passive approach where the Technical Staff receive alerts from the computer system (e.g., potential breach) and also receive input such as the state of a system and its stored information, whether the information stored in the Read Access Memory (RAM), in the files system and log files, appear as expected. Later the Technical Staff would fix the problems and discharge his/her obligations based on the flow charts of troubleshooting IS/IT systems. Some obligations may not allow the Technical Staff to create and write the scripts or executes some tables and properties. For internal controls purpose, the IT Manager is required to discover if there are any suspicious or breaching activities (e.g, unauthorised viewing or

manipulating the tables) by his/her IT Technical Staff and subordinates. Let us say that if the IT Technical is unable to resolve some technical problems based on the flow charts of troubleshooting (obligations), then the IT Manager may require his/her staff to attend education and training sessions (RT1:Technical/Formal), giving chances for improvement and improving knowledge (RT3:Technical/Informal). But, if the IT Technical Staff is still not improved, the IT Manager should make some decisions, whether to reshuffle/send the staff to a department that deals in non-critical business activities which carries a low risk, rather than delegating him/her in the critical business activities (high risk), or any other appropriate solutions. The IT Manager plays a significant role in identifying and assessing the risk and also in advising the potential mitigations for minimising and preventing the risk.

At departmental level, the CIO has the power to make decisions and approve certain IT budgets. If the budget requires more, the CIO needs to approach and report to the Risk Management Committee and CEO of the organisation with reference to risk mitigations strategies.

That is why the IS/IT risks need to be brought up at the Corporate Risk Management Committee so that the Board and senior management are consistently active, review and mitigate the Technical risks which may affect the business. Later, this study identifies that risk management processes can be operationalised throughout all the IS/IT security procedures stage. This can help organisations to achieve minimum risks relating to IS/IT.

4.4.3.3 Risk Management and Internal Controls: Informal component

The Informal component which involves employee values and organisational values is always neglected within IS/IT security implementations (Mishra, et al, 2004). It is believed that the security problems are derived from all three components including the Informal component. All significant areas including the IS/IT security risks from the Informal component should be addressed at the corporate governance level (Information Security Governance, 2004), including the CIO from senior management and the IT Manager from the lower management level. Corporate governance is not only the responsibility of the Board and senior management but also of all levels of employees.

For example, the Board monitored the managerial reports of IS/IT risks in the corporation and found that the risk associated with e-mail spams may cause system disruptions and files corruptions; business delays may cause business losses. After further investigation, the Board realised that the policies (e.g., education, training, awareness programme) and procedures (e.g., anti-spams software)

were already in place but the spams e-mails are still of concern and the Board wants to know why this still continues to happen. It was shown that all employees had attended the awareness programme and training on how to achieve the procedures of anti-spams software but only little improvement was achieved, which still dissatisfied management.

To find out why the anti-spams issue was still problematic, a drill-down study was conducted, where the IT Manager with his subordinates had to perform two tasks: first to view the internet logs, detecting who had opened the e-mail spams; and second, to study who already had been to anti-spams training and awareness programmes conducted by the corporation. Surprisingly, mostly, the trained and skilled employees were the people who opened the e-mail spams and their intended actions damaged to business data, business delays and, ultimately, financial losses and reputation damage. It is believed that the major cause of this was due to lack of the organisational value being embraced by the employees, they did not feel responsible for the security tasks assigned to them due to many factors. First, the understanding of the responsibility given was poor and of low quality; second, they were not sure to whom they were responsible, in terms of supervisory roles; third, they saw the security responsibility as technical problems. Organisational values have a connection with employee values. Employee values may affect the organisational values. When employee values are low, they also influence organisational values, where employees have a low integrity and are not trustworthy, it would also degrade the organisational values in accomplishing the responsibility of security tasks.

To consider the risk level, a few strategies can be considered, based on the risk assessment. For example, after finding out who were not behaving responsibly and had not complied with the policy and procedures on e-mail spams, the IT Manager may reinforce and conduct assessment over the elements of training, education, awareness, soft skills and values and participations. But, if these elements are still not workable and not implemented by employees, the IT Manager may get some advice from the CIO. The CIO may send reminder notices to employees or reprimands, to warn that their actions had caused high risks to the business. If the problem still cannot be resolved at CIO level, then the issue needs to be brought up at the CEO and Board level for ultimate action. The cost-benefit analysis conducted at the CEO and the Board level may show that the worst case would be that the employee/s be sacked due to risk factor.

Therefore, to accomplish the mitigation process of risk management, internal controls play an important role in the Informal component to ensure that employee values and organisational values are appropriate. For example, the risk assessment conducted at lower level has shown that the employee

was not fully responsible for the security tasks due to lack of understanding of the security roles and unclear supervisory roles. As part of the risk mitigation process, internal controls need to be established to react to the risk according to the risk level. For instance, the internal controls would be establishing the functional requirements for each security task, consisting of job scopes and the obligations (e.g., write, delete, create), job lists, who are responsible, the supervisor in charge of the task and information requirements for the task. Besides that, the internal control for this mitigation would also consider whether the security responsibilities have been communicated and understood between the giver (supervisor) of the task and the holder of the task. If these internal controls were not achieved as intended, at lower levels, this is a major issue of the IT Manager as leader and supervisor. The CIO should be able to advise the level of risk and prompt reactions towards this case, for example, transfer the employee to another unit or department within the organisation.

4.4.4 Risk Identification and Internal Control Application Process for the interaction of the three components model

This section will explain how IS/IT security risk is identified and the application of internal controls for the model interaction. Figure 4.8 illustrates the relationship between risk management and internal controls for the interaction of the three components.

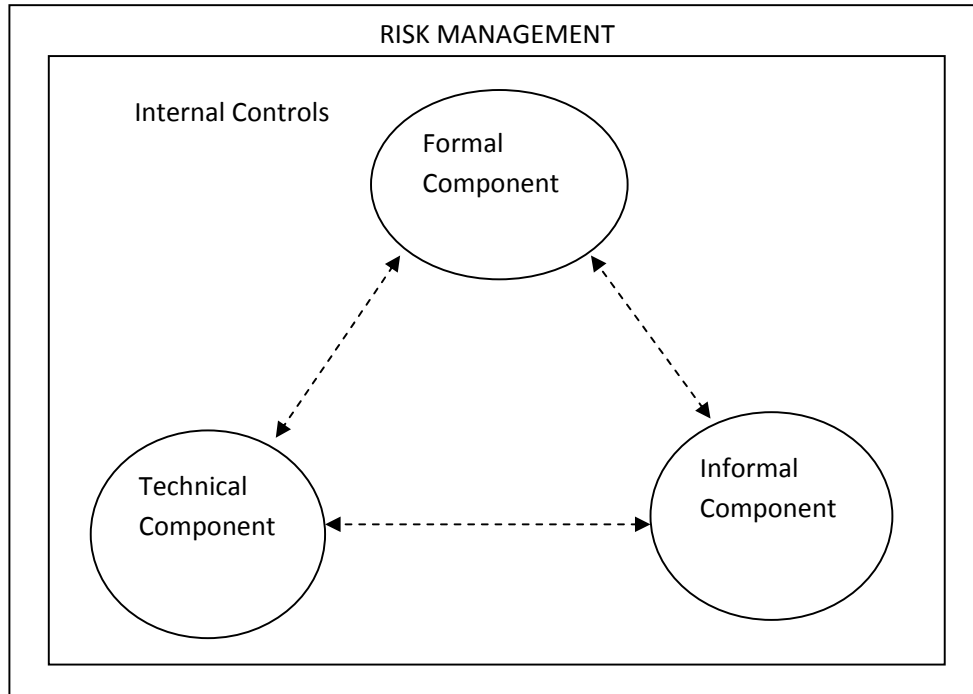


Figure 4.8 Relationship between risk management and internal controls for the relationships among the three components

It is first necessary to identify the critical issue areas which may compromise confidentiality, integrity and availability of IS/IT assets and data. The critical areas are identified for each of the three types of relationships namely: RT1-Formal/Informal, RT2-Formal/Technical and RT3- Informal/Technical. In achieving IS/IT security governance, critical areas will depend on the IS/IT security vision and security requirements in an organisation. The management are responsible to identify and prioritise the critical areas needs based on the business goals of the organisation which can be seen in Table 4.2.

Table 4.2 is based on Table 4.1 with the addition of the identification of supervisory roles/structure of responsibility. In the conceptual model, once a critical issue area has been identified, the next process is to determine the potential risks from the relationships (e.g., RT1, RT2 or RT3) associated with the issue areas. These issue areas and risks are illustrated through examples in Table 4.2. For example, the second issue area identified from RT1 relates to the password policy, integrity of the employee and unauthorised access to the Accounting Information Systems, as in Column 2. Risks associated with it are recognised in Column 3. An identified risk of RT1-Formal/Informal from this issue area was “Accounting Staff share passwords and unauthorised people can view and manipulate some Accounting data or files, which may cause data modification by unauthorised parties including writing, changing, deleting and creating”.

Clearly, this action was due to lack of supervision roles in discovering employees’ activities, lack of check and balance, employees did not understand, or were not clear about or neglected their obligations in the access to certain IT systems.

As the structure of responsibility is significant in IS/IT security governance tasks, the next process is to establish the supervisory roles, in Column 4, the giver of responsibility and the holder of responsibility, based on the obligations and policy undertakings. After identifying the security issue area (e.g., Accounting Information System) and entities (e.g., supervisor and the holder of responsibility), the next step is to grant the entities ‘status’ based on the hierarchy of types of access control like “Top Secret/Secret/Classified/Unclassified” in the Bell La Padula Model (Bell and Padula, 1976). The Bell La Padula Model is used in this conceptual framework because it keeps confidential and important data secret, where a computer user of one Accounting Information System with a Secret access (a low level clearance) should not be able to read files marked as Top Secret (a high clearance), but someone with Top Secret should be able to read all files within the hierarchy. Using the theory by Bell and Padula for the conceptual framework, the management may establish roles, obligations (access

rights) and provide start and finish of access to an Accounting Information System, based on employee privileges and designations.

Risk identification is part of the risk management activities. The risk identification stage helps an organisation to identify any potential scenarios that may happen if not addressed effectively and efficiently. In this case, each relationship has a diverse range of risks depending on the issue area.

After risk identification, the conceptual model examines whether organisations have applied internal controls to that particular risk or not (Cooper et al, 2004). This can be seen in Column 5. The internal controls are important mechanisms to ensure that the risk related to certain areas is controlled and minimised. If no internal controls are applied, the organisation needs to establish internal controls for that particular risk as seen in the “suggested internal controls in place” column. In Table 4.2, the suggested internal controls for the second issue discussed in Column 5 were:

“first, the Accountant should monitor the activities of his/her Accounting Staff, by discovering any suspicious events over the password log reports, network log reports, bio-metric authentication reports; and second, the Accountant is required to ensure his/her Accounting Staff attend security training or policy awareness programme on security password indicating active participation in the IS/IT security procedures”.

However, if relevant internal controls have been already implemented, the organisation may enhance and improve the existing internal controls in place.

Additional potential areas, the identified risks and associated internal controls are shown below in Table 4.2.

No	(1) Relationship Type(RT)	(2) Issue Areas	(3) Identified Risk	(4) Giver of Responsibility and Holder of Responsibility	(5) Suggested Internal Controls in place.
1	RT1: Formal/ Informal	E.g., Language style of IS/IT Security Policies documents	Documents are not understood because too simple, technical, wordy or complicated	(Between CIO and Operation Manager, IT Manager, Area Sales Supervisor, IT Manager, Purchasing Supervisor)	The CIO who wrote the policies should verify the document is intelligible enough. The CIO should get feedback from all the experts/counterparts including Operation Manager, IT Manager, Area Sales Supervisor, IT Manager, Purchasing Supervisor). The CIO should conduct education and training programme about the document to identify any language issues and the contents of policies.
2	RT1: Formal/ Informal	E.g., Security Password Policies	Accounting Staff share passwords to view some Accounting data or files.	(Between Accountant and Accounting Staff)	The Accountant should monitor the activities of his/her Accounting Staff, by discovering any suspicious events over the password log reports or network log reports. The Accountant is required to ensure his/her Accounting Staff to attend security training or policy awareness programme on security password indicating active participation in the IS/IT security procedures
3	RT3: Informal/ Technical	E.g., Information System Development	E.g., Employee able to change database codings. Some critical sales formulas in the Sales Information System sales may be changed and modified, this led to inaccurate of data	(Between Area Sales Supervisor and Sales Staff, Programming Staff)	The Area Sales Supervision is required to delegate the tasks, to more than one Sales Staff for discovering if any suspicious activities done by the Programming Staff or his/her own Sales Staff. The Area Sales Supervisor is required to monitor the Password Log Reports, Network Log or Firewall Log to detect any significant/suspicious events from the Programming Staff and Sales Staff
4	RT2: Formal/ Technical	Databases, Network, Internet Policies or other IS/IT security policies	Misalignment between security requirements and business goals, may cause losses	(Between IT Manager and IT Technical Staff)	The IT Manager is required to monitor the installation and implementation of the security hardware and software over the resources were correct and achieved the intended goals, by checking-up and auditing related areas as done by the Technical Staff.

Table 4.2: Risk Identification and Internal Controls for the component Interaction

In IS/IT security governance, the active involvement of the Board and senior management can be seen through the directing and monitoring actions done by the supervisor of the responsibility. In the next section how the directing and monitoring actions influence the three components is discussed.

4.4.5 Directing and Monitoring Actions over risks from Formal, Technical and Informal components and the model interactions

This section will discuss the important role of the senior management to make sure IS/IT security governance is profoundly achieved within the organisation, through the two major responsibilities of corporate governance, namely, the ‘directing’ action and the ‘monitoring’ action. The directing and monitoring actions in this model refer to the involvement of the Board and senior management towards the implementation of IS/IT security as a whole. The goal of this model is to stress the involvement role of higher level management and lower levels management within the implementation of the Formal, Technical and Informal components of IS/IT security and interactions. The higher level may be a supervisor responsible for ensuring that the responsibility and obligations of IS/IT security are discharged by the lower levels, namely, the holder of responsibility.

4.4.5.1 The directing and monitoring actions

‘Directing’ and ‘monitoring’ actions are two important activities of IS/IT security governance (King Report,2002; Solms,2006; ITGI,2006; Posthumus,2005; Kizirian,2004; Knapp,2006; BS17799,2002; Entrust,2003-2004; Ezingard,2005; Ghose,2006). The directing action in this model refers to the role and responsibility of the Board, senior management and all management levels to achieve the intended goals. The monitoring action is a reflective process in terms of measuring success or failure of the intended goals and the activities conducted at the directive stage (Solms, 2006). There are many ways that can be used for monitoring the directives such as, in general:

- managerial and operational reports
- security incidents statistics reports
- periodic meetings with departments and related roles on security issues
- evaluate the risk management and internal controls reports

In the conceptual model, to prevent failure of IS/IT use, the directing action needs to be monitored and evaluated to mitigate the risks.

4.4.5.2 The directing and monitoring actions: The Three Components and the interactions

The directing and monitoring actions are mapped out across the Formal, Technical and Informal components to achieve an effective implementation of IS/IT security governance (Solms et al, 2006). The success of risk management and internal controls application over the three components as shown in Figure 4.9, section 4.5 is influenced by the effectiveness of the directing and monitoring actions.

The directing and monitoring actions are the heart of the corporate governance practices. The Board and senior management are accountable for the success or failure of the business, where it is still subject to supervisory commitments and structure responsibilities performed at the ground level. The outcomes depend upon the effectiveness of the directing and monitoring actions, as conducted between the two major important entities: first, the giver of the responsibility, normally the higher level of supervisor; and the second, the holder of responsibility, normally the subordinates of the supervisor. More importantly, the relationship between the two entities is subject to obligations, where obligations concern *what has to be done* in order to achieve the objective of responsibility. Not only the Board and senior management but all employees members within all management levels share similar responsibility towards the IS/IT security job. The giver of the task is responsible to delegate and assign the security tasks to the holder, then, in return, the lower levels should react and be responsible to perform the security tasks effectively. This process will continuously happen throughout the layers between the giver of the responsibility and the holder of the responsibility based on the hierarchy system and the obligations in order to direct (manage) and monitor the resources effectively and efficiently.

The model of IS/IT security governance in this research provides an added value to all layers of employees including the strategic, tactical and operational levels and reemphasises the active involvement of the Board and senior management in directing and monitoring the IS/IT resources and business data. The model provides strategic locations to achieve the business goals and at the same time protect the IS/IT resources and business data; where the Board and senior management need to ensure that the alignment between the three components of IS/IT to achieve the best security outcomes. To accomplish IS/IT security governance, a right mix of these three components is crucially important. For example, it requires an appropriate set of tools and skilful employees to ensure that the goals of the IS/IT Security Governance Model are achieved. The Board and senior management needs to ensure this alignment occurs because they are the one who approve and endorsed the policy and resources, make decisions on management strategy, foster security culture and show commitment to IS/IT security to their employees. Without their active involvement in ensuring that the responsibility delegated and the

obligations discharged between the giver of responsibility and the holder of the responsibility are met, the IS/IT security governance is not likely to be successful.

4.4.5.2.1 The directing and monitoring actions: The Formal component and the interactions

In the Formal component, the Board and senior management have responsibility to provide direction in terms of the corporate vision, strategies, policies and standards relating to IS/IT security to all employees, to ensure that the IS/IT security risks are controllable. These activities must also conform to the prevailing laws and regulations applicable to the organisation. The outcomes of directives of the Formal component implementation also need to be measured as part of the monitoring actions. This section will discuss the role of Boards and senior management including all management levels within the Formal component and its interaction, specifically, the relationship between the giver of the responsibility and the holder of responsibility within the Formal and its interaction.

In the Formal component, the formulation of the security policy is normally based on the business goals and security requirements in the corporation. The Board and senior management are normally the group who endorses the security policy and approves the resources and access privileges to achieve the policy requirements.

As far as the model of IS/IT security governance is concerned, the expression of the Formal component needs to be informed by the state and ground realities of the Technical and Informal components. For example, a new corporation plans to establish security policy but is unsure where to start. This model will help the organisation by examining and aligning the formal dimension with two components interactions: Formal/Technical and Formal/Informal.

a) Formal/Technical

To establish the security policy, some deficiencies would be identified from the technical aspects. For example, let us explore the supervisory roles between the IT Manager (as a supervisor of the responsibility) and IT Technical Staff (as a holder of responsibility), and his (IT Manager) counterparts. To comply with the policies, the IT manager needs to provide reports on how he/she handles and fixes the problems at the ground level over the holder of responsibility. The organisation has to accept the risk if there was no action taken by the supervisor or inability to resolve the problems at the ground level. Apart from detecting deficiencies from his department, the IT Manager needs to work rigorously with his counterparts from other departments/units/sections to identify the vulnerabilities and threats over the IT systems. In linking with the Formal dimension component, that

is, the IS/IT security management strategy needs to be in parallel with the ground level and technological reports of the technical component. (Resource analysis such as SWOT analysis and Porter's Value Chain analysis can be conducted to identify the strengths, weaknesses, threats and opportunities of the IT systems and also to classify whether the IT systems were primary activities or secondary activities.) This alignment is significant to determine the correct technological areas for security policy formulation and development. The classification of technological areas for policy was determined according to the IT security vision and IT security management strategy of the Formal dimension.

b) Formal/Informal

The management has a big role in endorsing security policies; but examining the informal requirements is also important. In this model, employee values and organisational values are two indications of the informal dimension, which have a link to the formal dimension. In organisations, the Human Resource Department also has a role in providing enough and appropriate human resources and making the employees aware of their responsibilities, high integrity, trustworthiness, ethicality and other characteristics. The development of skills and characteristics is beyond the scope of the Human Resource Department alone and also of related departments like Finance, Engineering and Manufacturing, Sales and Marketing and IT. Therefore, the development of security policy requires input from the Human Resource Department and related departments to ensure that employees possess the required skills and characteristics. The implementation does not end here, the security responsibilities are continuously discharged by the supervisor and the holder of responsibilities throughout the management levels in order to minimise the risk. Apart from that, the management should have trained and checked the integrity of the employees to achieve IS/IT security policy.

In spite of providing Formal directives, the Board and senior management including the strategic, tactical and operational management levels have the responsibility to monitor the implementation of the Formal directives and the interaction. This model includes an example of how to monitor the effectiveness of the Formal directives and its interaction.

First, each giver of responsibility or the one who holds the supervisor role needs to discover the results of internal controls of the policy implementation (Formal/Informal). For example, the giver of responsibility, such as the Accountant, may monitor by examining the Key Performance Indexes (KPIs) over his/her Accounting Staff, such as the Accountant is required to delegate the security responsibility in protecting financial information stored in the Profit Information Systems databases

from being hacked, modified, deleted or manipulated by Accounting Staff. In order to achieve the KPIs of this type of responsibility, the Accountant needs to discover the list of password logs and network logs reports, examining who had used the Profit Information Systems and who had done the data manipulation, e.g., addition, deletion, changes and queries over the business data (Formal/Technical). Based on the obligations, e.g., the Accounting Staff is tasked to add new data and to display data only, but the Accounting Staff is not allowed to delete or up-date the data because the Accounting Staff held the *Secret* access status, which was a low level clearance according to Bell la Padula (Bell and Padula, 1976). The Accounting Staff is not able to delete, up-date and read some files marked as the *Top Secret* status (a high clearance), whereas the Accountant who holds *Top Secret* status is able to delete, up-date and read all files within the hierarchy.

If any suspicious activities occur or the obligations of the responsibility are not discharged correctly, the Accountant should be able to set the level of risk accordingly, such as react and fix the software deficiencies (Formal/Technical), install Firewall technologies, passwords, bio-metric authentication devices and passwords to increase the security (Formal/Technical), send the Accounting Staff member back to the education programme or reshuffle the staff to supporting business departments rather than placing him in primary business departments (Formal/Informal), Accounting Staff are required to attend policy awareness programme (Formal/Informal) and the Accountant needs to up-date the policies and business rules if necessary (Formal/Informal).

After scrutinising the results of the KPIs (part of internal controls), the Accountant may determine to react and provide strategic actions by assessing whether the requirements of technological resources and human needs have been accomplished concurrently with the policy requirements.

The monitoring by the giver of the responsibility including the Board, senior management and all management levels needs to emphasise balanced implementation between the three components, so that the holder of the responsibility is always aware of the responsibility and obligations of the tasks.

4.4.5.2.2 The directing and monitoring actions: The Technical component and its interaction

To achieve the Technical component of IS/IT security, the Board and senior management including all management levels of employees are responsible for providing directives including resources and procedures on how to achieve the Formal requirements regarding implementation of the Technical component. The Board and senior management may provide and approve the security tools to be employed and the endorsement of the procedures for achieving the security policies. The

management has responsibility for providing adequate security technological resources based on the business and policy needs of the organisation, through a lot of discussions with the CIO and counterparts and junior managers before the resources are endorsed. The implementation of technological resources is not successful without aligning the Technical component with the Formal and Informal components.

a) Technical/Formal:

The CIO, who is responsible to provide and manage IT/IS security resources, needs to work closely with other counterparts such as Chief Operating Officer, Chief Marketing Officer and Administrative Officer, ensuring that the security counter-measures and security controls are aligned with the IS/IT security vision, IS/IT security management strategies, business IS/IT resources (Technical/Formal) and policy requirements (Technical/Formal) in each department/section of the organisation. At the ground level, the CIO and counterpart levels may assess whether the resource analysis results (e.g., SWOT Analysis) conducted at the IS/IT security management strategies (component of Formal dimension) were followed and the planned security counter-measures are in accordance with the IS/IT security policies. To establish the security counter-measures, the tasks are complex. The IT Manager and his subordinates have a bigger responsibility to identify the security problems, vulnerabilities and threats at the very ground level. In parallel, the IT Manager needs to work rigorously together with his counterparts such as the Accountant, Purchasing Supervisor, Operation Supervisor and Area Sales Supervisor, to identify the deficiencies and security problems throughout the operational level. The management can use the security reports for policy up-dates and development, risk mitigations purposes and future internal controls checklists.

b) Technical/Informal

In achieving the technological security implementation, the management also needs to consider the informal dimension, that is, the structure of responsibility and the supervisory roles involved in the IS/IT security. As already explained in the Technical dimension section of this chapter, technical components are the realisation of the Formal dimension, where the determination of IS/IT areas and security counter-measures are derived from the IS/IT security vision, IS/IT security management strategies and IS/IT security policies. To see how this alignment works, see the example in the next paragraphs.

Having considered the IT systems, databases and networking system (technological areas) in place, the IT Manager and the heads of department are required to prepare the functional requirements

of IT systems comprising *name of IT resources, security responsibilities and tasks, who is the holder of responsibility, who is the supervisor (giver)*, so that the IT Manager and each Head of Department has a clear framework of security responsibilities and subordinates in their charge.

After the technological areas have been determined such as the IT Payroll System (as aligned with policies), the next step is to minimise its risks (such as data lost/stolen). Where in the automatic control approach such as an Intrusion Detection and Prevention System (IDPS), this model is able to prevent and control the security problems using automatic preventions to halt and stop suspicious activities and intrusion attempts. This type of interaction seeks to address how the informal component, like structure of responsibilities, plays part in order to achieve the Technical component. For example, in the traditional IT payroll system, the more detailed supervision by department heads throughout the company is achieved by frequent comparison of personnel records and payrolls by the IT Payroll system which involves sending the relevant sections of the report to each departmental supervisor. If the IT Manager and his subordinates could cooperate in a way like that, the risk would be low. But if the IT Manager and his subordinates could not cooperate, this creates problems and will increase the risks to the organisation. The CIO as upper management needs to communicate, report and discuss this matter to the Board level for ultimate decisions and if the problem cannot be solved, the Board would have to accept a higher degree of risk than it had anticipated.

So, what the model would suggest is to provide extra control, preventive control, namely, IT security internal controls, in the IT Payroll system, a kind of automatic and real-time security system which incorporates the Network Intrusion Detection Systems and Host-based Intrusion Detection System, to maintain the integrity of payroll data, rather than using humans to do the comparison of personnel records with the IT system. The automatic security system would be able to stop the IT Payroll system if the personnel data such as the amount of gross salary has changed (e.g., due to increment, human error or deliberate actions or failure to adhere to mandatory/discretionary access controls). As already discussed in the previous sections relating to Intrusion Prevention Systems (extension to Intrusion Detection System) the attempts at intrusion can be stopped by resetting the connections, sending an alarm, dropping the malicious packets, blocking the traffic from the offending IP address. In this case, the user of the system is required to inform the upper level, the supervisor, then the supervisor will validate and check, if due to increment, the IT Payroll system can resume but, if due to deliberate actions, the supervisor needs to investigate and fix the problem at his/her level. Or, if still

not resolved, the next process would be to report to upper level for decisions or management has to accept the risks.

Despite the directives, the Board and senior management need to measure the effectiveness of the implementation, through the monitoring action.

In the monitoring action, the management is responsible and accountable to ensure that the resources are used effectively and achieved according to policies. After the directing action takes place between the supervisor of responsibility and the holder of responsibility, monitoring would provide a clear structure of roles and using internal controls as a check and balance.

The management may use internal controls to monitor the security progress report of the procedures implementation between the two entities, the giver of responsibility and the holder of responsibility over the use of technological resources, either success or failure. For example, to achieve the network policy, the Area Sales Supervisor is required to monitor the usage of Sales Information Systems by his Sales Staff. The Area Sales Supervisor may delegate some obligations to his Sales Staff; Sales Staff can *display*, or *print*, or *write*, or *change*, or *delete*, or *create*, depending on the business rules of the organisation. This model is rather focused on deterring and preventing, by identifying this responsibility, the Area Sales Supervisor able to monitor by discovering who (Sale Staff) had performed *display process*, *print process*, *write process*, *change process* and *delete process*. The Area Sales Supervisor can use the network log report as a monitoring tool for detecting suspicious or abnormal activities done by his subordinates, the Sales Staff.

The management needs to review actively the internal controls results with other senior managers and junior managers to maintain the goal of IS/IT security. The monitoring review is important in IS/IT security governance because the management has a role in providing and enhancing technological resources for supporting business operations.

To ensure that the alignment of the Technical component with the other two components is achieved, the management needs to oversee that the technological resources have been implemented and fulfil the needs of policies. The implementation of the technological resources also needs to be aligned with the employee values such as skills and characteristics to achieve the maximum outcomes of the IS/IT security policies. As far as the model is concerned, to make the technological resources operational, the internal controls could provide the report on whether the following two types of interaction have presented the stated indications.

i) Technical/Formal

- sufficient skills and effective training provided
- availability of resources (human) to support the tasks
- capability of resources (human) to perform the tasks
- resources analysis conducted to identify the strengths, weaknesses, threats and opportunities of the technological resources (SWOT analysis) and to classify whether the technological resources were primary activity or secondary activity in the business (Porter's Value Chain Analysis), for risk management purposes

ii) Technical/Informal

- Establishment of supervisory roles in directing and monitoring the security over the technological resources
- Establishment of functional requirements (structure of responsibility) of the security job tasks, e.g., holder of responsibility, giver of responsibility, responsibility name
- Employees possess characteristics, such as have a high integrity, trustworthy, obedience to ethical requirements set forth by corporation

The monitoring part can be established by reviewing the internal controls results for each of the alignments and who were responsible for the security job. In this framework, the two entities are important, the giver of responsibility and the holder of responsibility. For example, reviewing the internal controls results of the Technical and Formal components relationship, the management may review the security reports periodically on the security tools used for maintaining IS/IT security, whether it is effective or not. If the internal controls are not effective during the monitoring process, the lower management level needs to advise the upper management level about alternative security tools for addressing the issue of IS/IT security.

4.4.5.2.3 The directing and monitoring actions: The Informal component and its interaction

The Informal component relating to culture, norms and beliefs influences the way employees practise and react to IS/IT security in organisations. The success of the Informal component of IS/IT security depends on the involvement of the Board, senior management and all management levels specifically in the directing and monitoring responsibilities. The following scenario briefly presents how the involvement of the Boards and senior management in the Informal component impacts on IS/IT security.

For example, in Company ABX, the management has IS/IT security policies relating to security controls/counter-measures and procedures such as the use of encryption software in place for implementation by all employees. There are a few areas of encryption: over the folders, disks, databases and communications. However, the perception of employees relating to the use of encryption software as part of policies to protect sensitive information could be positive or negative, with the following consequences.

- Positive perception: e.g., Follow the policy and security procedures relating to encryption software, this suggests business has a low risk, security is in the state of stable.
- Negative perception: e.g., Security procedures of implementing encryption software for protecting confidential data were ignored, this suggests if no actions is taken at the giver/holder of the responsibility, the upper management level needs to accept the risk.

Using this model the negative perception of employees of the security control procedures is now discussed, in addressing and achieving a balanced alignment between the two interactions of the Informal/Technical and Informal/Formal.

a) Informal/Technical

The model seeks to identify the deficiencies and suggests ways how to address them, from the components' interaction. For example, the issue of encryption may slow down the performance of the processor (Central Processing Unit-CPU) and delay the process requirements of the networking system (eventually affecting the wireless network) (Rodrigues, 2006). The problem impedes users committing to the encryption activities.

The other important problem identified from the encryption software is if the password is lost, the recovering process is not that easy, it involves cracking activities. These deficiencies may constrain the user implementing the use of encryption software, such as some users still think the process is difficult and complicated if the password is lost where files cannot be decrypted (business data loss).

To prevent this from happening (problem: where security procedure was ignored), the management has to conduct risk identification and assessment activities over the security task given to its employees. For instance, let us explore the lower operational level, the relationship between the Area Sales Supervisor (as a giver of responsibility) and the Sales Staff (as a holder of responsibility). The supervisor has instructed the Sales Staff to use encryption software for sending highly confidential information, e.g., credit card numbers, through the networking system, the potential risk of this action

would be data loss, due to inability to decrypt, in the case of forgotten password. The Area Sales Supervisor needs to overcome this problem and strategise the mitigation action, such as do back-up over the data or files before the encryption process begins. It is claimed that achieving IT security governance is difficult because the process is very complex.

b) Informal/Formal

The reluctance of employees to implement the security procedures of encryption software may be due to insufficient skills, no manuals provided or the language of the manuals is too technical and training may be not provided by the organisation. The encryption process entails technical procedures and requires knowledge of how to perform it. Lacking formal components may affect the smooth implementation of technical procedures. Let us consider again the supervisory relationship between the Area Sales Supervisor and Sales Staff. The Sales Staff should be able to perform the security procedures, be capable to respond and report instantly to the Area Sales Supervisor if some deficiencies occur in the process such as inadequate skills to perform the task or manuals not understood. After receiving this report, the Area Sales Supervisor is required to investigate and fix the problems at his level until resolved, if not, the matters need to be brought up to upper management level for decisions and actions, before accepting the higher level of risk. Due to no enforcement and unclear guidance in supervisory roles over the activities such as do not know who are the supervisors of the responsibility and what obligations in delegating the responsibility, or the policy was not read and understood by employees because they believed no one cares (monitoring not happening).

These negative perceptions reflect the organisational values of the informal dimension. Organisational values relate to the structure of responsibilities which are mainly derived from policies. The Board and senior management need to ensure that they understand the people of the organisation and then they will be able to strategise the structure of responsibilities and establish clear supervisory roles and obligations within the IT systems. The formulation of IS/IT security policies involves senior management level and department levels such as the IT Department and the Human Resource Department. As far as the IT Department is concerned, the specific security responsibilities and some obligations are coming from IT views, especially the CIO, IT Manager, IT Technical Staff and Programming Staff because they are the technical experts in their fields. The IT Department prepares and produces the formal statements relating to IS/IT security roles and responsibilities, including training and educating the staff relating to supervisory roles, the giver of the responsibility and the holder of the responsibility. The collaboration between the IT Department and Human Resources Department is significant in achieving the structure of responsibility. The collaboration involves

discussions and communication in terms of the capacities provided by Human Resources such as skills, training and awareness programmes to strengthen employee values. Human Resources may provide some obligations and information relating to the rights, privileges and designations of an individual which can be used to strategise policies and determine the IT systems/database privileges.

The perception by employees of IS/IT security is influenced by the existing culture and norms of the organisation. A positive perception may arise because of the active involvement of the Boards, senior management and all management levels in the Informal component including effective actions such as a clear structure of responsibility and clear supervisory roles to report, full commitment, active participation, leadership and consistent monitoring over the policy implementation. With strong commitment from all management levels in supervisory roles in the hierarchy and discharging the obligations, a negative attitude of employees towards IS/IT security may be changed.

It is clear that the involvement of management plays an important role within the Informal component. Full commitment by management is needed in IS/IT security such as a constant checks and balances in the hierarchy system, giving examples of security behaviour to all employees such as deter and prevent are important in IT security and having frequent meetings with the Chief Information Officer and other junior managers to discuss the IS/IT security issues within the business operation.

The culture, norms and beliefs in one organisation including the organisational values and employee values held represent the reputation of that organisation. However, the Board and senior management still have responsibility to provide direction over all management levels in shaping the IS/IT security behaviour based on the policies, resources and tools to achieve the organisational values of the organisation. The tone of the Board and senior management through leadership impacts on IS/IT security.

The supervisor of the responsibility and the holder of the responsibility need to show full commitment in practising IS/IT security such as: implement the security tools effectively, always back up business and sensitive data and always monitor those who have responsibility to access sensitive data. Apart from that, the Boards and senior management could also encourage ethical values, integrity and honesty through presentations, company newsletters, e-mail communications and meetings to raise awareness.

Even though culture is difficult to quantify some examples of how the monitoring action may be used include to examine the commitment and involvement of senior management and other

management levels in IS/IT security practices including through the commitment shown in security awareness programmes, the information disclosure of IS/IT security in annual reports and transparent statistics of security incidents.

However, to achieve optimum IS/IT security, balanced implementation between the Informal component and the Formal and Technical components is needed. This is because the culture of each organisation needs to be tailored to the needs, IT vision and background, policies and tools procedures. For example, different employees have different backgrounds in terms of disciplines, skills, commitment and experiences. Whereas different views of personnel like experts/disciplines would affect how they perceive and implement the procedures. Professional people such as Medical Practitioners, Accountants, Engineers and Architects implement their tasks according to their expertises and standards; the way they interpret and implement the security responsibility may be different and unique. The establishment of structures of responsibility and clear supervisory roles in place may reduce and minimise the human actions caused by unintended acts such as not delegated the task or not discharged obligations on access controls. This may be due to lack of organisational values. Indirectly, this factor may contribute to the supervisory roles and structure of responsibilities in IT security.

The security tools should be appropriate to the business requirements to achieve policies. Even though some IS/IT security systems are available in the market, the IT Managers still need to convince the upper management levels, considering the budgets, cost-benefit analysis, availability of human resources, supervisory roles and structures of responsibility and the urgency of risk mitigation according to business needs.

The language to be used in the policy and procedures should be understandable and easy to follow by different types of employees. Considering the cultural differences and different views of personnel is part of the informal dimension that needs to be involved in the policies relating to IS/IT security.

4.5 The directing and monitoring actions over three components and interaction through use of risk management and internal controls

All management levels have responsibility to monitor the internal controls results for each of the alignments. An internal control, as part of the management mechanism, can be used to measure the effectiveness of the alignment. For example, to monitor the internal control results for the Informal and Formal components alignment, the supervisor of the responsibilities should review the security training

reports including IS/IT security awareness programmes attended by the employees of the organisation to indicate that the Formal requirements are balanced with the Informal needs. If this alignment does not occur the supervisor of the responsibilities is ultimately accountable for the failure of IS/IT security due to his inactive role.

Obviously, the Board and senior management are accountable for all IS/IT risks from all three components. The management at all levels has accountability to monitor the progress towards achievement of the Formal component, the Technical component and the Informal component through risk management and use of internal controls. The management can use internal controls results as a part of the monitoring activities to ensure that risks related to the Formal, Technical and Informal components are controlled according to the organisation's objectives.

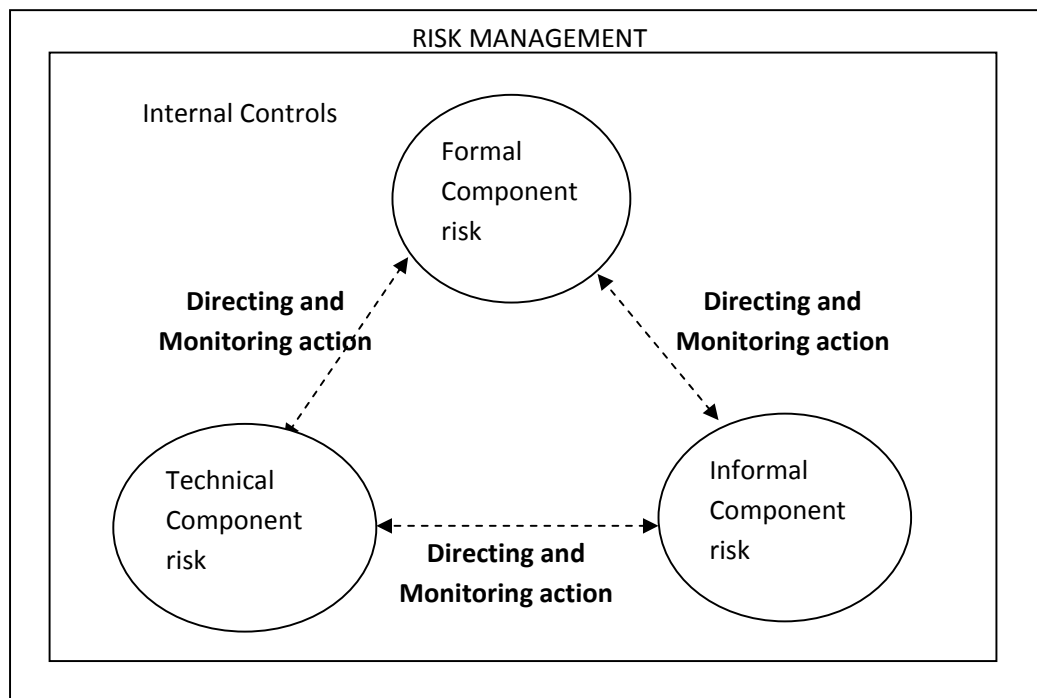


Figure 4.9 The directing and monitoring actions over the three components and interaction through use of risk management and internal controls.

In conclusion, the active role of the Boards and senior management in directing and monitoring actions consistently may link to better risk management and the application of effective and efficient internal controls.

4.6 Objectives, Conceptual Framework (Chapter 3) and IS/IT security governance model

The model of IS/IT security governance in this chapter is a detailed extension of the one in Chapter 3. The objective of the Conceptual Framework in Chapter 3 is to provide an extensive(general) model of how management deals with issues relating to supervision roles and responsibilities at all management levels, incorporating risk management and internal controls within the three components. The objective of this chapter is to break down the component details and their interactions by giving examples of specific security problems/deficiencies of some components and component interactions within supervision roles and responsibilities.

Linking back to Chapter 3, Figure 4.10 (taken from Chapter 3) shows that the conceptual framework developed in the early stage of research has been used for reference and the development of the IS/IT security governance model in this chapter. The Figure has two types of elements, internal and external, but this study is limited to internal elements as can be seen in Figure 4.10. In this chapter, the discussion of the model covers the information relating to elements of each component, component interaction, relationship between risk management, internal controls and the three components and interaction and directing and monitoring actions over risk from the three components and interactions.

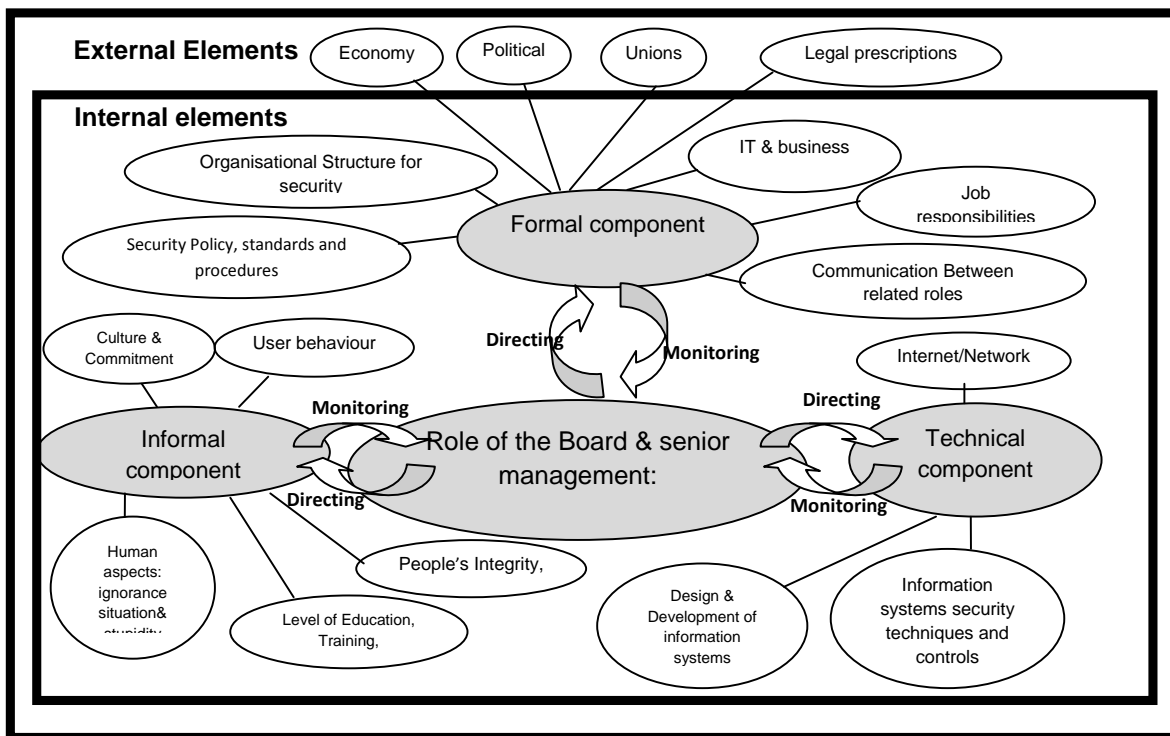


Figure 4.10. Conceptual framework of IS/IT security governance

4.7 Comparison between the IS/IT Security Governance Model and other existing security models

To date, a number of security models and theories have been developed to improve IS/IT security within organisations. This section compares the IS/IT Security Governance Model with another researcher's model and the security models found in the literature, analysing their strengths and weaknesses. The weaknesses identified in the previous security models are addressed in the IS/IT Security Governance Model.

Mishra et al. (2007) stressed the importance of the three elements which were the Formal, Technical and Informal aspects in IS/IT security. A theoretical framework by Mishra has proposed that the management of people such as security culture, individual values and beliefs in organisation is crucial to ensure that the policies and technical procedures relating to IS/IT security are followed. The anomie theory was applied in the Mishra's theoretical framework which came from the sociology discipline to investigate the IS/IT security behaviour within groups. The anomie theory is useful in IS/IT security because it involves cultural and environmental pressure for achieving organisational rules and norms. However, Mishra's theoretical framework only addressed the management of the informal aspects but did not align it with the Technical and Formal aspects. The relationship interactions of the three components were not presented in Mishra's paper. Therefore, in this study it is proposed that the implementation of the three components and the interaction of these components is needed within the IS/IT Security Governance Model in order to overcome the limitations of Mishra's model.

Other researchers, Straub et al. (1998), have applied the General Deterrence Theory (GTD) from criminology within the risk planning model in order to reduce security incidents in organisations. GTD includes four lines of sequential actions—Deterrence, Prevention, Detection and Remedy. In their IS security risk planning model Straub et al (1998) using GTD, counter-measures work according to lines of controls. If potential offenders ignore the Deterrence control, the next line control takes place which is Prevention control. Remedy control is effected when there is non-compliance with the first-three lines and the examples of Remedy controls are warnings, reprimands, termination of employment and legal action. Clearly, the directing elements of IS/IT security were presented in the Straub's model. However, the model by Straub et al (1998) has limitations where the monitoring element by the Board and senior management was less emphasised. If the security internal controls of the lines are not effectively monitored by the supervisor of the responsibility, the organisation may be likely to re-invent

the wheel from time to time. The investment in resources may not be returned or the Return on Investment (ROI) may not be adequate.

To address these weaknesses, the IS/IT Security Governance Model suggests that effective internal controls and monitoring of the policies and procedures will help organisations to achieve the goals of the directives. The monitoring process will help the supervisor of the responsibility to detect risks and address immediate actions by improving directives for achieving IS/IT security. For example, through the monitoring action of IS/IT security governance, the implementation of the lines of control in Straub's model can be evaluated. After evaluation, the management can improve directive actions such as endorsing new policies, changing management strategies and approving security budgets for establishing security controls. The role of the Board and senior management is crucially important in the IS/IT Security Governance Model because they are responsible and have the power to respond to all types of business risk.

The next model to be identified is ISO 17799. IS/IT security standards like ISO 17799 have been used internationally to improve IT security management practices within organisations. The standard is comprehensive and is seen as the best reference framework for IT security management where it covers multi-facets which range from technical, human and legal to business survivability. External standards like ISO 17799 can be used as a reference for internal policy development and as a tool for achieving internal policy. However, ISO 17799 has some limitations in the way that IS/IT security controls are being practised; it focuses on the existence of processes rather than on how effectively the processes are being implemented (Siponen, 2006). For example, the topic of the standard, the goal and the prescription of the ISO 17799 standard are presented below.

BS ISO/IEC17799: 2000, p. 11

6.2 User Training

To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

The standard is merely ensuring that employees follow its contents but does not provide strategies on how to achieve it. Having the standard in place does not guarantee that the goal of IS/IT security is achieved. To overcome this problem, the IS/IT Security Governance Model proposes the application of internal controls over the intended goals. The internal controls help management to determine whether certain elements have achieved their objectives. The IS/IT Security Governance

Model highlights the important role of the supervisor of the responsibility and holder of the responsibility in ensuring that the internal controls are applied to achieve certain goals of the standard.

4.8 Summary

The three components of the IS/IT Security Governance Model, namely, Formal, Technical and Informal have been discussed in detail. The Formal component comprises three layers which are the IS/IT Security Vision, the IS/IT Security Management Strategy and the IS/IT security policy including the IS/IT security standards. The two layers of the Technical component identified are the Technological Areas and the IS/IT Security Procedures. In the Technological Areas, there are two inner layers, namely, IT infrastructure and Business Data and Information and Business Information Systems. The Informal component refers to the culture, norms and beliefs of the organisation and the model classified two elements of the Informal component, employee values and organisational values.

The importance of the interaction model of the three components has been raised in this model, RT1, RT2 and RT3, the ways risk management and internal controls can be applied across these three components and their interactions have been pinpointed. Examples of relationships between risk management and internal controls are provided. Apart from that, there are also examples of how risk management and internal controls can be applied within the component interaction. Also discussed was the involvement of the Board and senior management by providing directives and monitoring actions across the three components and their interactions.

Finally, the strengths and weaknesses of the existing models have been considered and the limitations of previous models have been addressed in the current IS/IT Security Governance Model.

Chapter 5: Research Design and Methodology

5.0 Introduction

The research design and methodology adopted in this study are discussed in this chapter including the development of the triangulation approach to the research design to be employed.

The aim is to collect primary qualitative and quantitative data. In terms of the qualitative method, interviews with the Boards of directors and senior management of publicly listed companies in Malaysia within multiple studies were planned. The researcher aimed to analyse the interview data using two techniques: software analysis and manual analysis. In terms of quantitative method, a mail survey to collect primary data on IT/IS security governance from the viewpoint of Boards of directors and senior management of publicly listed companies in Malaysia was to be developed. To analyse the mail survey data, it was planned to use statistical analysis techniques including mean, frequency and descriptive information.

In terms of secondary data, content analysis was to be used to acquire quantitative and qualitative data from websites. The researcher planned to conduct content analysis and to examine 210 annual reports of Malaysian publicly listed companies. Manual analysis will be used in analysing the results of searches.

5.1 Research Design

A research design is always based on research questions. In this chapter, the research design outlines procedures for every research activity conducted in this study (Cooper et al., 2003). The information to be considered in the research design of a study includes the research paradigm, research philosophy, research approach and research type. These issues will be further discussed in the following sections.

The research problems in this study are: Lack of involvement of the board and senior management in understanding IS/IT security problems, unbalanced implementation of IS/IT security within the Formal, Technical and Informal components and lack of internal control applications over IS/IT security. These three research questions have driven to the development of two major questions as follows.

Research questions

Question 1

In what way does the involvement of Boards and senior management impact on the implementation of IT/IS security governance?

Question 2

How can directing and monitoring actions in the technical, formal and informal dimensions of IT/IS security governance in corporations be implemented efficiently and effectively?

The process of answering the above research questions is a challenging task due to the sensitive nature of the study to be conducted. For example, the following are some of the main reasons corporations did not participate in IT/IS security research conducted by Kotulic et al., (2004).

- Corporation employees cannot participate in every request they receive
- Corporation policy does not allow employees to participate in any surveys
- Corporation policy does not allow sharing of information about its computer security policies with outside entities
- As the time of a management team is valuable and they receive benefits from corporations, the corporation does not allow them to participate in the research project
- Corporation security policies prevent complete answers to some requested questions
- The questionnaires contain some questions that require answers that would reveal proprietary information

(Source: adapted from Kotulic et al., 2004, p.604)

Therefore, to minimise their effects and when considering the reasons listed above for limited data gathering in a related research area, it was decided that this study needs to acquire more than one data type, quantitative and qualitative. The explanation of how these two data types may help to answer the research questions in this study is discussed in the next section.

5.2 Research Paradigm

A triangulation approach will be adopted in the data collection to answer research questions 1 and 2. As can be seen in Figure 5.1, the adoption of more than one method is useful in the context of this study. Triangulation was adopted for two reasons: first, the nature of study to be conducted; and second, the collection of more than one data type. Because IT/IS security governance is sensitive in

nature, triangulation offers some ways to overcome failure or low participation as it involves different sources of data (Kotulic et al., 2004). Therefore, triangulation is utilised to maximize the collection of data that may be sensitive.

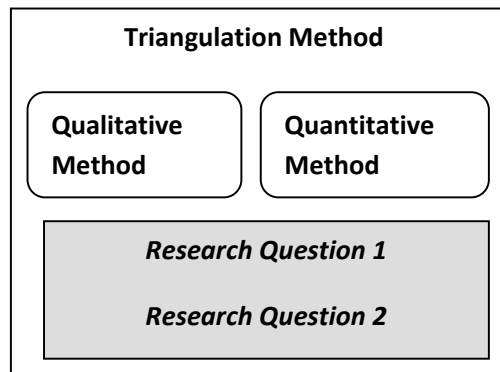


Figure 5.1. A triangulation method designs approach adopted in this study (Ticehurst et al., 2000)

The goal of triangulation was to collect interview data (qualitative), mail survey data (quantitative) and website data (quantitative) in order to gain a broader understanding of the research issues being investigated. While the interview method was aimed to acquire qualitative data relating to how Boards and senior management thought about IT/IS security processes within their work-place, a website analysis and a mail survey were planned to generate the quantitative data in regard to security awareness and attitudes towards IS/IT security governance. Triangulation offers the potential to increase the validity of an IT/IS security governance study as this approach offers both subjective and objective perspectives from participants (Creswell et al. 2007).

In this study, both data types were collected to answer both research questions which can be seen in Figure 5.2. Through the qualitative method, the researcher is part of the research process where the researcher tries to get inside the minds of the directors, senior management and other employees who provide explanations of their situations or behaviours from their own points of view (Veal, 2005). In the context of IT/IS security governance, the researcher will be able to examine the processes at all levels of activity in the corporation, from top to bottom and from bottom to top (Solms et al. 2006). To collect qualitative data, it was planned to conduct multiple interviews using twelve cases. The positive aspect of a multiple case design is that the generalisability of a study can be improved by using more than one case (Tharenou et al., 2007). A case is an in-depth analysis which enables comprehensive inquiry and is conducted in the field. As noted by an IT/IS security researcher, “time is far better spent focusing on a few, select firms with whom the researcher has developed an excellent rapport and trust” (Kotulic et al., 2004, p 605). Using a qualitative method of data collection like interviews as described

in Figure 5.2 would be expected to increase the trust level and rapport between a researcher and participants. As the area to be investigated is sensitive, a face-to-face interaction may improve the trust level and rapport between interviewer and interviewee(s) and, as a result, richer information on IT/IS security could be gained.

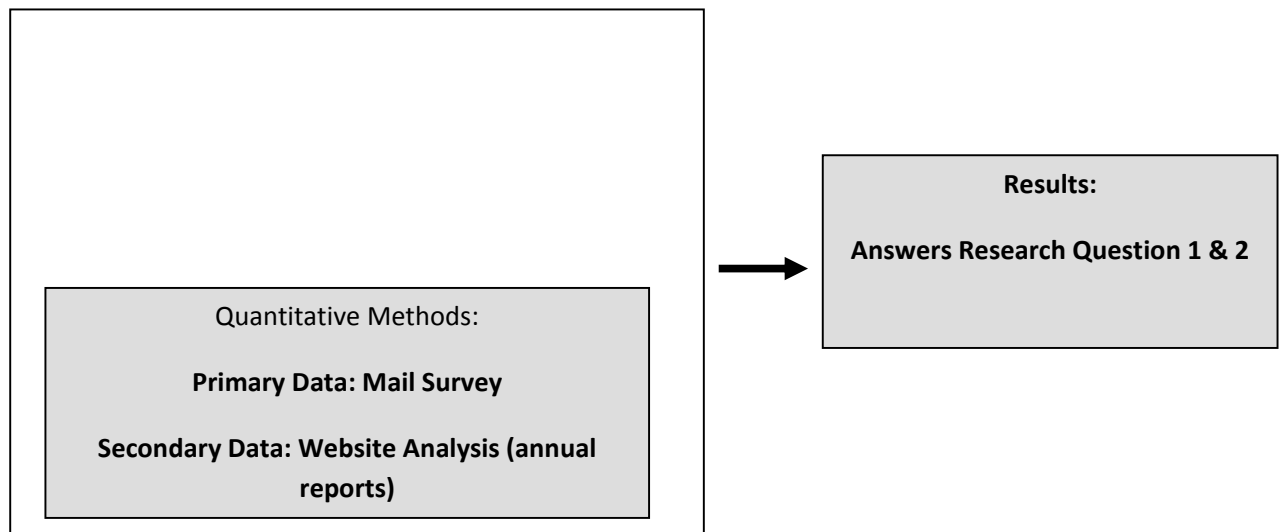


Figure 5.2. Triangulation Method Designs approach taken in this study

It was planned to collect interview data primarily from the senior managers, junior managers and Board members of Malaysian publicly listed corporations. Using the qualitative method, the researcher aimed to gather two types of secondary data: website data and organisations' documents. The website data like annual reports of Malaysian companies and the organisations' documents like policies relating to IS/IT or IS/IT security were aimed to be gathered in order to strengthen the qualitative results and answer the research questions

The contents of annual reports of Malaysian publicly listed corporations are owned by Bursa Malaysia. The general terms and conditions and disclaimer of Bursa Malaysia have been read and understood, the contents of the website can be viewed and printed for research purposes (Berhad, B.M, 2011).

The quantitative method complements the qualitative method. In the quantitative method, the researcher will gather two forms of data: primary and secondary data. As for primary data, an anonymous mail survey will be conducted in order to maintain the anonymity of respondents due to the sensitive nature of this study. A mail survey will be undertaken as it enables anonymity of respondents when returned by mail and it is inexpensive to conduct (Ticehurst and Veal, 2000). As it is proposed to select the sample for the study from the population of Malaysian publicly listed companies,

respondents may prefer the anonymity when sensitive and confidential matters like IT/IS security are involved.

The researcher planned to gather the secondary data, website data, from annual review reports and to use website analysis to investigate how much information on IS/IT security awareness in IT/IS Security was disclosed on company websites to enrich the research data. Moreover, information sought from websites is free and accessible. The website analysis is significant in this study because the website contains all pdf annual reports from all industry sectors of Malaysian publicly listed companies.

5.3 Sample for study

5.3.1 Group Target Design

The main board companies of Malaysian publicly listed companies were chosen as the population for data collection. The main board was chosen because it represents the largest board of *Bursa Malaysia* or Malaysian publicly listed companies with 624 in total as at December 2008.

The population was divided into groups in ranks of market capitalisation as at 31 December 2008. In this study, market capitalisation is regarded as "the total value of a listed company's shares based on current market price" (Berhad, B.M, 2008).

The population was to be classified into three groups because the higher ranked companies were thought to be likely to promote a better corporate governance disclosure in their annual reports than lower ranked companies. It was planned that there will be three groups of the population for this study: Group A. Group B and Group C. Group A is the Top Group with rank 1 to 100, Group B is a Middle group where the rank is between 101 to 524, and the Group C is the Bottom Group, ranging from 525 to 624.

Population and the ranks	Sample of Group Design	Category
1 to 100 in rank	Group A	Top Group
101 to 524 in rank	Group B	Middle Group
525 to 624 in rank	Group C	Bottom Group

Table 5.1 The group design of study using 2008's market capitalisation

5.3.2 Sample analysis

In the triangulation approach, utilising Interviews, Mail Survey and Website Analysis, the sample size and approach may vary for each method. The sample size used for each method will be explained in detail in the relevant section.

5.4 Research Methods

5.4.1 Interviews

The semi-structured interview was the second method employed in this study in order to obtain rich data from Malaysian publicly listed companies. The semi-structured interview is suitable for the topic area because it allows the interviewer to tailor the questions into the study's context. This method provides better access to an interviewee's views, experiences and opinions in a flexible setting without any constraining formats when the interview takes place (Lindlof and Taylor, 2002). Important skills are required for conducting interviews such as establishing rapport with the interviewee, flexibility and performing active listening (Silverman, 2009). These characteristics allow positive interaction between an interviewer and respondent without losing sight of meaning in the interview process.

The researcher has had some background in academic teaching and had some experience in conducting tutorial classes, it is claimed that the researcher possesses interview skills; the tutorial skills concerned with questioning and probing towards students' thoughts and understanding about the topics would help to achieve the objective of the interview. Apart from that, the researcher aimed to improve the skills of interview through questions and answers sessions with experienced researchers and utilise the open nature of the internet by watching the video presentations and lectures that related to interview skills.

5.4.1.1 The development of the interview instrument

Although there was no guidance from previous research, numerous questions were developed and tested with colleagues and supervisors. It is believed that the remaining questions satisfy the tests of relevance, validity and acceptability to interviewees.

The development of interview questions was predominantly governed by research questions 1 and 2, while also being influenced by the conceptual framework of IT/IS Security Governance in Chapter 3.

The researcher planned to develop three sets of interview questions, a different set for each of the Board of directors, senior management and junior managers. In this study, the Chief Executive

Officer or Managing Director is assumed to represent the Board and senior management level in the company. A CEO plays dual roles in two groups, the management and the Board. The Chief Information Officer and Chief Financial Officer are assumed to represent the senior management level while the IT/IS/Information Security Managers correspond to the Junior Management level in the company.

The interview questions were planned to be broken down into three dimensions; formal questions, technical questions and informal questions. Each respondent needed to reflect on all dimensions. Table 5.2 shows the number of questions relating to the dimensions and the position levels.

In order to ensure as broad a representation as possible it was necessary to contact people from each level of authority and from each of the three components. As indicated in the paragraph following Table 5.2, it was expected that these factors would affect the ranges of knowledge and experience of the managers.

As noted earlier, the web analysis had indicated that disclosure of information relating to IT/IS security governance was to some extent a function of size. Therefore, companies were selected to reflect different levels of size.

Because three interviews of unknown length were planned for each company, resource constraints were the dominant factor in selecting the number of companies.

In the questions design shown in Table 5.2, it was planned that the interview questions for each position would be developed to convey similar meanings even though numbers of questions vary according to position levels. The interview questions will be modified according to the position levels in the company. For example, the question about 'policy' is suitable for a CEO, the question about 'policy and procedures' is suitable for a CIO/CFO while the question about 'procedures of implementation' is suitable for a junior manager.

	No of Interview Questions			Total
	Formal Dimension	Technical Dimension	Informal Dimension	
<u>Board of Director/senior management</u> CEO	7	3	5	15
<u>senior management</u> CIO/CFO	5	5	3	13
<u>Junior Management</u> IT/IS/Information Security Managers	5	1	2	8

Table 5.2: No of planned interview questions by Dimensions and Designation/Position Levels

The planned sample for interviews is presented in Table 5.3. It was intended that each group participate in the interview process. As presented in the earlier sections, the samples for each group were planned as follows: 100 for Group A; 424 for Group B; and 100 for Group C. In Table 5.3, the sample of Group B is doubled as compared with Group A and Group C because the population of Group B was much higher.

	Group A	Group B	Group C	
No of Companies	3	6	3	
Total Listed Companies				12

Table 5.3 No of Planned of Listed Companies According to Group

Table 5.4 shows the planned number for each group according to designation and planned sample (Table 5.3). The CEO plays two roles in an organisation: one is overseeing the day-to-day business operation; and, as a member of the Board of directors, he/she has overall responsibility and accountability for controlling corporation resources and maintaining business reputation. The researcher expected to interview twelve Malaysian corporations, comprising twelve CEOs representing

senior management and Board of directors, twelve CIO or CFO and twelve junior managers who represent management of corporations.

	Top	Medium	Bottom	
CEO	3	6	3	
CIO/CFO	3	6	3	
Junior Manager	3	6	3	
Total of Interviews	9	18	9	36

Table 5.4 No of planned interviews to conduct according to group

Interview Procedures-Access to Corporations

After receiving Ethics approval from the University of Tasmania a formal letter with Information Sheet (Appendix 5A) was sent to all intended potential interview participants, 36, electronically. The researcher also intended to select the cases across industry sectors to examine if the nature of business and industry type impact on IS/IT security governance. E-mails and phone calls were planned to be used as a medium of communication between researcher and participants to arrange appointments. Getting access to Malaysian corporations is a challenging task because of the need to interview key people in the organisations like CEOs and key management members.

One of the motivations of this study was to contribute to the knowledge of IS/IT security governance within corporate governance practices, specifically in Malaysian corporations. Their participation is significant in this study to answer the research questions and to address research problems, apart from supporting the conceptual framework and the model of IS/IT security governance. The effective administration of the interviews may improve participation. To achieve this, a follow-up call was planned to ensure that they had already received the invitation letter and information sheet, to increase the trust and establish rapport with the corporate personnel. The consent form will be sent to corporations if the participants are agreeable.

The appointments were scheduled to be made with participants about one or two months before the interviews were to be conducted.

To ensure the objective of the interviews is achieved, the researcher planned to identify requirements and prepare the interview materials for the interview sessions such as audio/cassette recorder and its transcription needs, list of questions and a list of corporation addresses.

5.4.2 Questionnaire

It was planned that a mail survey be conducted to acquire quantitative data from the study's participants. During the preparation of the questionnaire, many drafts were expected to be produced, seeking the relevant information required on the IT/IS security governance topics. Poor questions need to be removed to avoid jargon, ambiguity, leading questions, multi-purpose questions and to simplify their wording (Ticehurst and Veal 2000).

The questionnaire will be divided into two parts (Appendix 5B). The first part seeks demographic information of respondents and the background of the corporation while the second part aims to explore people's opinions and agreement or disagreement on IT/IS security governance topics within their corporations. In the demographics section, respondents were asked to answer a combination of two types of question; two open-ended questions and several closed questions. In the second part of the questionnaire, respondents were predominantly asked their opinions using closed questions with a *likert-scale*. A *likert-scale* was used in this study to indicate the respondent's agreement or disagreement with a statement. Factors relating to the involvement of the Board of Directors and senior management in IT/IS security governance in corporations were anchored on a five-point numerical scale from 1=strongly disagree to 5=strongly agree. The written questionnaire consisting of 28 questions within two sections can be seen in Appendix 5A.

Other aspects of questionnaire design including the nature of the introductory remarks, ordering of questions and layout of questionnaire were to be carefully considered during the development of the instrument. The opening remarks in the questionnaire were important as the researcher needed to assure the respondents about the University's strict rules of confidentiality, ethical obligations and the terminology used for this study.

A small pilot survey was undertaken with the University's academic staff. After conducting the pilot test, some validity aspects needed to be addressed including interpretations of question wording by respondents, questionnaire wording, order of questions, repetitive questions and also instructions about how to return the mail survey to the researcher. The input received in the pilot study improved the questionnaire.

The development of the questionnaire is described as follows. The questions were primarily based on the research questions, literature review and the conceptual framework of this study. The links between questions, research questions and the conceptual framework are presented in Table 5.5. Basically, as mentioned earlier, the questionnaire will be divided into two parts: first are demographic

questions; and second are questions relating to IS/IT security governance. It was planned that the number of questions to be asked was 28, six (6) demographics questions and twenty-two (22) IS/IT security governance questions.

The study has two refined research questions. Research question 1, seeking what evidence exists in corporations, examines the three dimensions of IS/IT security governance, namely, formal, technical and informal, in order to discover the level of involvement of the Board and management in IS/IT security. Research question 2 examines the processes of directing and monitoring actions over three dimensions of IS/IT security governance, as found in research question 1 and also examines the simultaneous relationship between the three dimensions by considering the internal controls and risk management of the factors of IS/IT security.

It can be seen in Appendix 5C that the questions were also based on the conceptual framework. The conceptual framework has seven major sections: 1) Introduction, 2) IS/IT risks and IT governance, 3) IT risk governance and internal controls, 4) Formal, technical and informal dimensions of IT risk governance, 5) Internal controls for IT risk governance across the formal, technical and informal dimensions, 6) Developing a model of IS/IT security governance and 7) IT Risk Governance and Internal Controls Management Practices in Malaysian Corporations. Each of the questions, including one demographic question (role), has a link with the research questions and the conceptual framework.

5.4.3 Website Analysis

Due to IT/IS security being a highly sensitive area, secondary sources available on company websites including annual reports were utilised to help answer the research questions. Content analysis was planned as for the website to gather quantitative data such as the number of passages found relating to IT/IS security on the websites (Tashakkori and Teddlie 2003). The passages related to security of IT/IS will be used for evidence to achieve the research objectives of the study.

The researcher aimed to examine website data using the Foxit Reader program to reduce search time. This application was planned to be used exclusively for searching texts and highlighting sentences that corresponded to the topics sought manually. It is proposed that the frequency of the passages found be recorded using tables.

The sample to be used for analysis of website annual reports will be in accordance with the three main groups, Group A, Group B and Group C. 210 Listed Companies' (of 624 in population)

annual reports available from the Malaysian publicly listed companies' websites will be used. The 210 companies were divided into three groups as shown in Table 5.5. The number in Group B was doubled because this group had the majority population.

Sample Group	Number of Sample of Annual Reports
Group A	50
Group B	110
Group C	50
Total	210

Table 5.5 Number of sample for website data according to group

Before conducting the analysis of the 210 annual reports, a pilot study was planned to be conducted to review annual reports of 20 companies using content analysis. It was proposed that the twenty (20) companies be randomly drawn from the population of Malaysian corporations and remain part of the sample of this study. The main criteria of pilot selection will be based on whether they have shown good principles and best practices in Corporate Governance. The study aimed to use the results of the best company ranking by the Corporate Governance Survey 2008. The study was conducted by the Minority Shareholder Watchdog Group in collaboration with its partner, the Nottingham University Business School. The key item areas of the Corporate Governance Survey reflected the principles and best practices of the Malaysian Code on Corporate Governance, Listing Requirements and International Best Practices. It is expected that the twenty companies have exhibited corporate governance principles and best practices. The preliminary findings of the twenty were planned to be used for designing the topics/ keywords for content analysis over the sample. The aim of the pilot study was to identify the similar keywords and terms relevant to IT/IS security governance before embarking on the real search.

5.5 Before Analysis

This section will explain how the earlier developed conceptual framework of IT/IS security governance (Chapter 3) and research questions are to be operationalised within the triangulation approach -qualitative and quantitative.

Figure 5.3 shows the relationship between research questions, the developed conceptual framework in Chapter 4 and the data type to be used in the data analysis. There are two sections in

Figure 5.3, A and B. Section A in the figure was presented to model the approach to answering research question 1 and 2 which aimed to examine the involvement of the Board of directors and senior management in IT/IS security governance within the three dimensions, formal, technical and informal.

Section B was framed to model the approach for addressing research question 1 and 2 which aimed to examine how IT/IS security governance is directed and monitored in the formal, technical and informal dimensions.

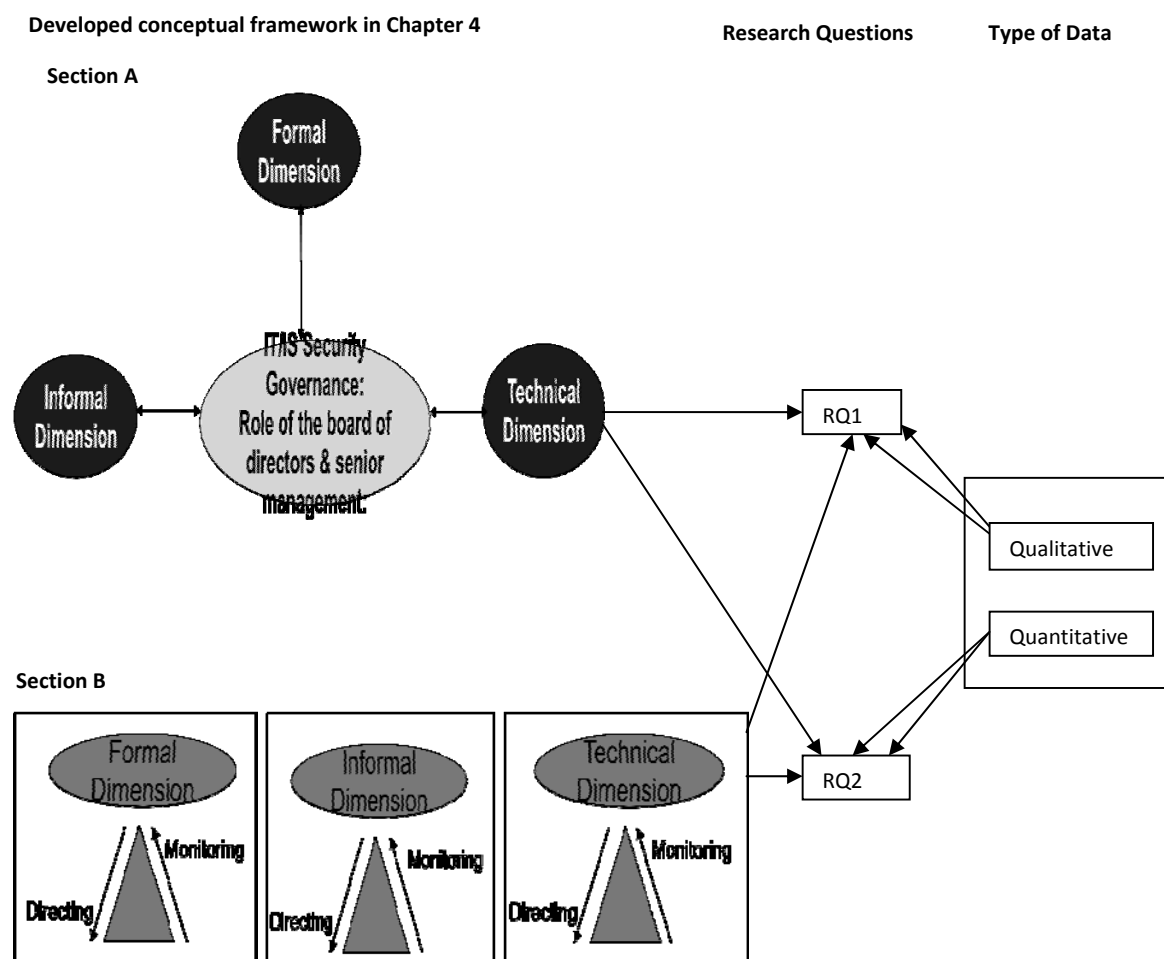


Figure 5.3 The relationship between research questions, the developed conceptual framework and data type

5.6 Data Analysis

5.6.1 Data Analysis Process

Qualitative data will be primarily taken from interviews, edited field notes and e-mail responses not mentioned earlier. While quantitative data will be based on website analysis of annual reports and mail-survey responses.

5.6.1.1 Data Analysis Procedures for Qualitative Data

To guide the analysis of qualitative data in the phase, the Three-Phase Analysis Model by Miles and Huberman (1994) as shown in Figure 5.4, consisting of data reduction, data display, drawing and verifying conclusion was planned to be used. Before the interview data were analysed, the researcher aimed to transcribe the conversations between the interviewer and interviewees from the recorded audio files. For validation purposes, the transcribed interview data will need to be proofread by the interviewees of this study in case of mistyped and wrong words and meanings during the transcription process.

It was intended that there will be two stages of qualitative analysis, the first stage is to conduct software analysis and the second stage is to undertake manual table analysis. The main goal of using manual table analysis was to ensure that the results of the first technique were valid (answerable according to research questions and conceptual framework) and reliable (results repeated in the second technique) and also to complement the first software analysis technique if some of the results/data were missed during the automatic analysis process.

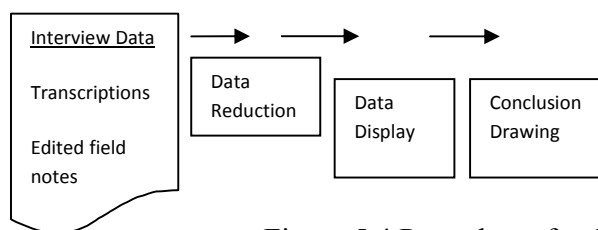


Figure 5.4 Procedures for Qualitative Data

The researcher planned to follow Miles and Huberman (1994) for analysing the qualitative data over the two types of analysis techniques.

Software analysis

The qualitative data such as transcriptions, edited field notes and e-mail responses will be exported into Leximancer Version 3.07 analysis software (Leximancer Manual, 2009) to reduce and display the data; analysing the data in such a way helps to draw and verify conclusions. A series of processes was planned to be undertaken in the Leximancer analyses. These include improving transcripts within the software setting requirements and formats, removing unrelated concepts and grouping interview data into files according to dimensions and cases. It was planned that the parameters of this study be set into database software settings based on the topic of the interview questions, research questions and conceptual framework, where this stage is critical in order to reduce and display the required data for analysis.

Leximancer analyses are entirely text grounded, the next aim of analysis will be to use qualitative analysis (interpretative technique) for interpreting the displayed data such as concept maps of Leximancer and extracting evidence (e.g., words, sentences) of real world views by participants.

Manual content analysis

Manual content analysis, a traditional technique, was planned to be used in analysing the interview data. The columns and rows of a table will be used to organise the data.

There will be two major steps involved in this process: first, set up the analysis framework; and second, report results and findings. It was planned in the analysis framework table that all the interview transcripts will be reduced, organised and displayed using themes (themes developed in Chapter 3) against issues gained from the interviews. Later, the research questions will be used for arranging the results of analysed data before drawing the conclusions.

5.6.1.2 Data Analysis Procedures for Quantitative Data

Website Analysis

It was planned that there will be three analytical stages involved in the website analysis. The first stage will be searching the sentences relating to the “security” term across the annual reports sections widely. The reason for using a single word of “security” is to capture sentences that discuss logical-IT related and also non-IT related. It is believed that each corporation has its own culture, some refer to security as physical in nature and some refer to it as logical-IT related in nature. The researcher does not want to miss the rich meanings over the term ‘security’ used in the reports.

Over the security results found in the first stage, the second stage will be more focused on examining whether companies have already discussed logical or IT related. The filtering process in this stage is to remove data relating to non-IT. The results of the searches on IT-related will be placed according to dimensions, formal, technical and informal. The qualitative method will be utilised to identify several similar words used, as some terms might be interchangeably used by various corporations. For example, corporation Y uses ‘information security’ referring to IS/IT security but in corporation Z the term used was different but holds similar meaning, such as ‘IT security’. That is why ‘security’ was to be searched in the first place to avoid any missing statements related to IS/IT security.

Then, the final stage will be extracting the sentences related to logical IT-related into the study’s framework. The results of the final stage will be significant in this study to answer the research questions and support or reject the conceptual framework of IS/IT security governance.

Mail Survey

It was planned in the case of analysing quantitative data that a statistical package software be adopted. A range of procedures and available functions are provided by the software for answering the research questions and to test the model of IS/IT security governance. As most of the data to be collected had adopted a 5 point *likert- scale*, the researcher aimed to produce descriptive statistics to examine the average (means) of respondents’ agreement towards the IS/IT security governance practices in their corporations.

Apart from that, three steps will be undertaken to acquire the mail survey data, which are: [1] ethics approval, [2] distribution of mail survey, [3] administration of the survey responses.

In the first step of procedure, the researcher planned to obtain approval from the Ethics Committee.

To achieve the second step which is distribution of the mail survey, the researcher aimed to use the sample population of this study, namely, Group A, Group B and Group C. It was planned that the corporate mailing addresses be obtained from the Bursa Malaysia’s websites. Post-paid envelopes for returned mail survey will be prepared with a set of instructions on how to return the survey.

The researcher believes that the final stage of administration of mail survey will be critical and planned to make the Universiti Malaysia Sarawak the secretariat centre.

Chapter 6 Website Analysis

6.0 Introduction

The data analysis, results and findings of the website data are presented in this chapter. A sample of 210 sets of annual reports was selected to represent the population of about 624 Main Board, Malaysian Publicly Listed Companies; the annual reports were dated between years 2008 and 2009. The preliminary stage of data analysis was an extensive review, interpretation and selection of the phrase(s) containing items that related to IS/IT Security. The Foxit Reader application was used to examine the item “security” relating to the IS/IT Security Governance Model throughout the sample of 210 company annual reports. The technical about Foxit reader is explained in Appendix 6A. There were two steps involved in analysing the website data: first, the selected texts and phrases relating to the themes identified from the IS/IT Security Governance Model were analysed; and second, the phrases relevant to the Research Questions were sorted.

6.1 Sample Analysis

The rationale for this decision was that preliminary work had indicated that larger companies disclosed more relevant information than others and that smaller companies disclosed nothing.

The total number of companies was 624 companies, see Appendix 5D for records on market capitalisation and profits (in Malaysian Ringgit-MYR). Group A represents the top 50 companies in market capitalisation, with profits ranged between MYR31,637,134 (highest rank) and MYR2,280,000(lowest rank). Group B represents a random selection of 110 middle companies in market capitalisation where the profits recorded were between MYR2,271,437 (highest rank) and MYR26,791(lowest rank). Group C represents the bottom 50 companies in market capitalisation, the profits ranged between MYR25,805 (highest rank) and MYR1,985(lowest rank). (See Table 6.1).

Group	Description	Sample (No of set of annual reports used for analysis)
A	Top 50 in market capitalisation	50
B	Middle 110 in market capitalisation (random)	110
C	Bottom 50 in market capitalisation	50
Total		210

Table 6.1 No of sets of annual reports used for analysis in sample groups

6.2 Demographic Analysis

Of the 210 annual reports, only 16.2 % (34) companies disclosed information relating to the IS/IT Security Governance Model. The analysis further identified that out of the 34 companies, half (n=17) represented the Trading/Services sector, nine the Finance sector, three the Consumer Products sector, two Industrial Products and one each in the Plantation sector, Property sector and Technology sector. Across the industry sectors, there was a balance of disclosure between Group A (n=17) and

Group B (n=16) but only one company from Group C disclosed information relating to the IS/IT Security Governance Model.

A total of 101 items was found which relate to the IS/IT Security Governance Model. Over one-third (36.6%) of items found in the Business Operation Review asserted that some of the current companies had IS/IT Security Procedures in place. Slightly less than one-fifth (17.8%; n=18) of the items were discussed in the Corporate Risk Management section. Not many items were found in the important sections like Statement of Internal Controls (only 8.9%; n=9), Corporate Governance Statement (9.9%; n=10), CEO/Chairman Message (4.9%; n=5), Audit Committee Report (5.9%; n=6). With respect to the group type of sample, almost three-quarters (70.3%; n=71) of the items were found in Group A, 28.7% were found in Group B and only 1 item was found in Group C.

6.2.1 Group A

a) Analysis according to Industry Sectors

From the website analysis of 50 annual reports in Group A, 71 “security” items which related to IS/IT were found within industry sectors as can be seen in Table 6.2. The findings show that about one-third (17) of companies in Group A disclosed information on IS/IT security.

The largest group (60.5%) of “security” items was found in the Trading/Services sector within 10 companies. While the Finance sector represented by five companies contributed about one-third (31%) of the items found. About 8.5% of the items was discovered in “Consumer Products”. None of the searched items was found in other industry sectors.

These results show that the involvement of the boards and senior management in IS/IT security governance implementation may be determined by the industry sector. This can be seen through the dominant results of “security” item shown in “Trading/Services” and “Finance” industry sectors of Group A.

Item of analysis	Industry Sector of Company (n=50)	No of company's annual reports contain item	No of Item Found	Percent of Item Found (Frequency)
“security”	Finance	5	22	31.0%
	Plantation	0	0	0%
	Property	0	0	0%
	Consumer Products	2	6	8.5%
	Industrial Products	0	0	0%
	Construction	0	0	0%
	Trading/Services	10	43	60.5%
	Infrastructure Project Cos	0	0	0%
	Total	17	71	100%

Table 6.2 Analysis on Group A According to Industry Sectors

b) Analysis according to section of Annual Report

“Security” was further analysed according to the sections of the annual report which can be seen in Table 6.3. In Group A the “security” item was hugely discussed in the “Business Operation Review” section. Mostly, this section (Business Operation Review) contained progress reports by senior management at departmental or committee levels. This section contained almost half (43.66%) of the total “security” items and were found from eight company’s annual reports. IS/IT security stood out in the section of “Business Operation Review” in Group A because this may signal that the implementation of IS/IT security has involved all management levels which include the Strategic Level (The board/CEO/Chairman), the Tactical Level (Senior Management) and the Operational Level (Junior Management) within companies.

“Corporate Risk Management” had 12.68% of the items on “security” within 3 companies’ annual reports. Another section related to risk was “Risk Factors” (4.23%) which were found in two companies’ annual reports. This analysis indicates that the risk caused by IS/IT is also seen as a business risk.

This was followed by “Statement of Internal Controls” which constitutes 8.45% and involved 3 companies’ annual reports. These three companies have shown that they have IS/IT security internal controls in place.

Discussions on “security” were discovered in the “Corporate Governance Statement” with 7.04% of the items but only four companies had shown awareness of IS/IT security governance practices.

Four companies discussed IS/IT security in the “Audit Committee Report” which contributed 5.63% of the items.

Interestingly, the findings showed that 2 companies highlighted the importance of IS/IT Security in the “CEO/Chairman Message”. Though the number of CEO/Chairman who discussed IS/IT security in that section was low this would indicate that IS/IT security is perceived to be important by the boards of directors and senior managements of these two companies.

However, the “security” item was also found in other sections like “Compliance Information”, “Box Article”, “Towards Greater Innovation” and “Standard of Business Conduct”.

No of Company's Annual Reports=50				
Item analysis of	Section of annual report	No of company's annual reports contain items	No of Item Found	Percent of Item Found (Frequency)
"Security"	Business Operation Review	8	31	43.66%
	Corporate Risk Management	3	9	12.68%
	Statement of Internal Controls	3	6	8.45%
	Corporate Governance Statement	4	5	7.04%
	Audit Committee Report	4	4	5.63%
	Corporate Social Responsibility	2	3	4.23%
	Risk Factors	2	3	4.23%
	CEO/Chairman Message	2	3	4.23%
	Standards of Business Conduct	2	2	2.82%
	Towards Greater Innovation	1	2	2.82%
	Box Article	2	2	2.82%
	Compliance Information	1	1	1.41%
	Board and Senior Management Profile	0	0	0%
	Product and Services	0	0	0%
Total			71	100%

Table 6.3 Analysis on Group A according to Section of Annual Report

6.2.2 Group B

a) Analysis according to Industry Sectors

The study analysed 110 annual reports from Group B across industry sectors. The analysis of Group B found that 30 "security" items were related to the IS/IT Security Governance Model, 14.5% (16) of companies disclosed information on "security". (See Table 6.4).

Two dominant industry sectors were identified, "Trading/Services" and "Finance". It was noted that "Trading/Services" and "Finance" are dominant sectors neither in Group B nor in Group A. "Trading/Services" contained a majority of the "security" items found on the annual reports with 56.67% from 7 companies. The "Finance" sector constituted almost a quarter (23.33%) of the "security" items which were found in 4 companies' annual reports.

The "security" item was also found in the sectors of "Industrial Products" (from 2 companies' annual reports) and "Technology" (from 1 company's annual report) where each constitutes 6.67%. While both "Plantation" and "Property" industry sectors had about 3.33% percent each (one company each).

The industry sector had an impact on the involvement of the boards and senior management in IS/IT security governance implementation throughout the information disclosure. "Trading/Services" and "Finance" were the leading industry sectors in reporting on IS/IT security which was evident from the majority of the annual reports in this section.

Item of analysis	Industry Sector of Company (n=110)	No of company's annual reports contain item	No of Item Found	Percent of Item Found (Frequency)
“security”	Finance	4	7	23.33%
	Plantation	1	1	3.33%
	Property	1	1	3.33%
	Consumer Products	0	0	0
	Industrial Products	2	2	6.67%
	Construction	0	0	0
	Trading/ Services	7	17	56.67%
	Technology	1	2	6.67%
	Total	16	30	100%

Table 6.4 Analysis on Group B According to Industry Sectors

b) Analysis according to section of Annual Report

The analysis of “security” items according to section of annual report is presented in Table 6.5.

Almost one-third (30.0%) of the items was found in “Corporate Risk Management” which involved only one company’s annual report.

The “Business Operation Review” contained 20.0% of items on “security” and represented 4 companies’ annual reports.

The “Corporate Governance Statement” had 16.67% of the “security” items and represented four companies’ annual reports. The item was also found moderately (6.67%) in each of “Statement of Internal Controls”, “Audit Committee Report”, “CEO/Chairman Message” and “Towards Greater Innovation” and represented 2 companies’ annual reports each. The other section that contained the “security” item was “Board and Senior Management Profile”, it had the smallest (3.33%) number. In this single company annual report, a specific role on “IT Security” was assigned to the senior management team. This might indicate the active involvement of senior management in IS/IT security governance in that company. The number of items found in this group was lower than Group A even though the sample was doubled in this group. This may indicate that the companies with higher market capitalisation were more likely to have higher levels of Corporate Governance in IS/IT security than companies with lower levels.

No of Company's Annual Reports=110				
Item analysis of	Section of annual report	No of company's annual reports contain items	No of Item Found	Percent of Item Found (Frequency)
"Security"	Business Operation Review	4	6	20.0%
	Corporate Risk Management	1	9	30.0%
	Statement of Internal Controls	2	2	6.67%
	Corporate Governance Statement	5	5	16.67%
	Audit Committee Report	2	2	6.67%
	Corporate Social Responsibility	0	0	0%
	Risk Factors	0	0	0%
	CEO/Chairman Message	2	2	6.67%
	Standards of Business Conduct	0	0	0%
	Towards Greater Innovation	2	2	6.67%
	Box Article	0	0	0%
	Compliance Information	0	0	0%
	Board and Senior Management Profile	1	1	3.33%
	Product and Services	0	0	0%
Total			29	100%

Table 6.5 Analysis on Group B according to Section of Annual Report

6.2.3 Group C

a) Analysis according to Industry Sectors

In Group C, 50 annual reports were examined within these sectors:- "Finance", "Property", "Consumer Products", "Construction", "Trading/Services" and "Technology". Only one "security" item was found in the "Consumer Products" sector represented by one company's annual report. No discussion relating to "security" was found in the rest of the group. See Table 6.6.

Item analysis of	Industry Sector of Company (n=50)	No of company's annual reports contain item	No of Item Found	Percent of Item Found (Frequency)
"security"	Finance	0	0	0
	Property	0	0	0
	Consumer Products	1	1	0
	Industrial Products	0	0	0
	Construction	0	0	100%
	Trading/Services	0	0	0
	Technology	0	0	0
	Total	1	1	100%

Table 6.6 Analysis on Group C According to Industry Sectors

b) Analysis according to section of Annual Report

One item on “security” relating to IS/IT was found in the “Statement of Internal Control”. Table 6.7 shows that the annual reports in Group C had very low disclosure of information relating to “security”.

The very low number of items found was clearly seen in both types of analysis in Group C: (Table 6.6) and (Table 5-3b). Undoubtedly, the group also made impact on the involvement of the board and senior management in IS/IT security governance. The findings highlight that the companies with lower profits were more likely to have low disclosure on IS/IT security.

No of Company's Annual Reports=50				
Item of analysis	Section of annual report	No of company's annual reports contain items	No of Item Found	Percent of Item Found (Frequency)
“Security”	Business Operation Review	0	0	0%
	Corporate Risk Management	0	0	0%
	Statement of Internal Controls	1	1	100%
	Corporate Governance Statement	0	0	0%
	Audit Committee Report	0	0	0%
	Corporate Social Responsibility	0	0	0%
	Risk Factors	0	0	0%
	CEO/Chairman Message	0	0	0%
	Standards of Business Conduct	0	0	0%
	Towards Greater Innovation	0	0	0%
	Box Article	0	0	0%
	Compliance Information	0	0	0%
	Board and Senior Management Profile	0	0	0%
	Product and Services	0	0	0%
	Total		1	100%

Table 6.7 Analysis on Group C according to Section of Annual Report

The previous analyses showed that there are two factors which may influence the involvement of boards and senior management: Industry Sector and Group.

6.3 Data Analysis Procedures

After analysing the items according to industry sector and section of annual reports, the next critical stage is to select and analyse the most relevant texts and phrases containing the items that relate to the themes identified in the IS/IT Security Governance Model. Then, the phrases relevant to the Research Questions will be sorted and extracted to discover support for the themes of the IS/IT Security Governance Model.

6.4 Data Analysis and Research Questions

The results and findings of the data analysis were organised according to Research Questions 1 and 2 and themes of the IS/IT Security Governance Model. The analysis technique used was dependent on the Research Questions and Research Objectives. To answer Research Question 1, the across-cases analysis technique was used to find information relating to IS/IT security aspects across cases. The second technique, namely, single-case analysis, was used to answer Research Question 2, to study and validate component interactions within a single case.

6.4.1 Data Analysis and Research Question 1

Research Question 1: *In what way does the involvement of Boards and Senior Management impact on the implementation of IS/IT Security Governance in the Formal, Technical and Informal components?*

6.4.1.1 Formal Component

The content web analysis identified nine areas that related to the formal component.

a) IS/IT Security Vision

The IS/IT Security Vision is the most prioritised element of the Formal Component in the IS/IT security governance model as it indicates the intentions of the board and senior management in achieving and maintaining the confidentiality, integrity and availability of IS/IT assets and business data within companies. The analysis of 210 sets of annual reports revealed that only six companies provided information on the security vision of their IS/IT; four statements were from Group A and two were from Group B. No information was found in the smaller capitalisation group annual reports with regard to the IS/IT Security Vision. Only the larger and medium capitalisation companies provided information in regard to the IS/IT Security Vision.

The IS/IT security governance model suggests that the functionality of IS/IT with regard to confidentiality, integrity and availability could be compromised without effective directives and monitoring by the board and senior management through excellent supervision roles.

Trade-offs between the IT investment and its risk management strategy is greatly needed for achieving the IS/IT Security Vision of IS/IT security governance model. As disclosed by a large capitalisation company,

“The Board of Directors understand the necessity to leverage and optimise IT investments and resources for the best interest of the Group and to safeguard it’s IT resources, intellectual property management and information (P. 82, Company A50)”.

To establish the IS/IT Security Vision, the corporation needs to identify the IT areas, business processes and business data that need to be secured. The board and senior management should be able to identify the most important IS/IT issues that are aligned with business goals. For example, one larger

capitalisation company disclosed the strategic focus for Internet banking, the critical resources that need to be protected and security requirements including security controls and counter-measures.

“Our strategic focus for Internet banking is to make the online channel a key channel for our customers. Improvement was made on key operational areas to ensure accessibility of Internet banking to our customers. Security features were increased such as the implementation of two-factor authentication to offer further protection to our customers. In carrying out these efforts, we are encouraged by the 19 per cent growth in our Internet banking subscriber base as well as the heightened level of transactions over Company A1 Online and our self-service machines during the financial year under review.”(P. 42, Company A1)

From the disclosed information of Company A1, the key operational areas of Internet banking and customer data were recognised as the critical risk areas. When linking these data to the IS/IT security governance model, after the corporation has identified the potential risk areas, the management needs to formulate effective strategies how to achieve IS/IT Security Vision, for instance, create a security plan for mitigating the risks involving security controls and resource planning.

A clear IS/IT security vision in place helps organisations manage the security risks through effective strategies and better IS/IT security governance practices. For example, Company A9 had a clear IS/IT security vision, where the organisation had aligned the security requirements with technological resources and business goals.

“The Company A9 Group continues to undertake initiatives to maintain 100% systems availability and robust system performance for the Group’s computer systems, peripherals and network infrastructure and to enhance security features on all its computer platforms and network infrastructure to ensure secured data protection and uninterrupted transmission. Precautionary measures are regularly reviewed and enhanced to ensure customers’ interests are protected at all times for all online products and services (P. 94, A9)”.

In the IS/IT security governance model, after knowing to what extent IS/IT can support business operations by the internal employees, the board and senior management should be able to define IS/IT Security Vision. The following statement suggests that Company A6, a larger capitalisation company, had an IS/IT Security Vision.

“These initiatives contribute towards a systematic methodology to ensure the confidentiality, integrity, availability and non-repudiation of information and Information Systems against current or any potential threats prevalent in the evolving and changing internet world. This enables the Group to retain its customer trust and maintain high rates of utilisation for the Group’s products and services (p. 127, Company A6)”.

Clearly, the IS/IT Security Vision of Company A6 was concerned with security of the company’s products and services.

b) IS/IT Security Management Strategy

The IS/IT Security Management Strategy is purposely developed in order to achieve the goals of the IS/IT Security Vision. As noted in the IS/IT Security Governance Model, the strategy addresses

how to achieve the vision, for example, by putting the IS/IT security structures in place, setting up IS/IT committees, creating a security plan, setting up a programme of security training and education, setting up and including IS/IT security within the corporate risk management and corporate internal controls agenda, setting up a framework for evaluating, monitoring and auditing the IS/IT security processes.

Each proposed strategy varies according to the nature of the business, culture and environment. The analysis revealed six IS/IT Security Management Strategies. The strategies include IS/IT Security Risk Management, IS/IT Security Internal Controls, Organisational Structure of IS/IT security, Education and Training relating to IS/IT security and IS/IT Security Audit.

i) Risk Management

Only three larger capitalisation companies disclosed IS/IT security risk management information in their statements.

In regard to the IS/IT security governance model, a poor IS/IT Security Governance practice such as an unclear IS/IT Security Vision, misalignment between business goals and security controls requirements, less effective management strategies or policies, could contribute to many possibilities such as business losses and bad reputation. For example, one statement disclosed and discussed security risks and the possible impact.

“The Group’s businesses may be vulnerable to security breaches to key systems, assets and facilities resulting from acts of vandalism, sabotage or terrorism. Potential disruptions to operational systems or destruction of facilities from such security breaches and attacks, could adversely affect the Group’s reputation, its businesses, or financial results (P. 27, Company A11).

The IS/IT security management strategy, which is one of the formal elements of the IS/IT security governance model, suggests that all types of business risks including IS/IT security risks are the responsibility and accountability of the board and senior management. Therefore, a proper structure is vital, corporate committees like the Risk Management Committee are responsible for incorporating and overseeing IS/IT security risks. There are many strategies that can be placed engaging IS/IT security risks. For example, as disclosed by a larger capitalisation company, the Risk Management Team of Company A4 had conducted a security workshop to help employees in identifying and mitigating risks in order to improve and maintain the IS/IT security level.

“Two additional workshops were carried out by the risk management team to enhance awareness of risk management in addition to the regular risk management induction programmes for new staff. There was also a workshop on “Business Information Security” to highlight various risks associated with information security (p. 99, Company A4)”.

As identified in the IS/IT security governance model, in Chapter 4, continuous risk identification, assessment and mitigation over the IS/IT security risks should be carried out by employees as part of fulfilling IS/IT security responsibilities. To provide a comprehensive view of IS/IT risks surrounding the organisation, establishing a framework relating to IS/IT risk was one of the IS/IT security management strategies in the IS/IT security governance model:

“In 2008, an IT Risk Framework was developed and is continually maintained to ensure that risks are correctly identified and the necessary remedial actions are in place (P. 127, Company A6)”.

The risk management over the technological resources and IS/IT security procedure may be covered in the audit plan. For example the following risk areas were covered in the Audit Plan of Company A2.

1. *Quality of assets*
2. *Operational controls*
3. *Financial controls*
4. *Customer satisfaction*
5. *Compliance with laws and regulations*
6. *Lending practices*
7. *Management efficiency*
8. *Information technology*
9. *Data centres and network security*

(P. 48, Company A2)

ii) IS/IT Security internal controls

In the IS/IT Security Governance Model, IS/IT security internal controls are part of IS/IT Security Risk Management. Internal control is a mechanism to ensure intended goals are achieved within the risk management process. The analysis revealed that only two companies disclosed IS/IT security internal controls information. For example, the following statement discloses how the IS/IT security internal controls may be integrated into the risk management process.

“There are documented procedures in place that cover management accounting, financial reporting, procurement, information systems security, compliance and other risk management issues. The objective of the policies and procedures is to ensure that internal control principles or mechanisms are embedded in operations. This enables the Group to respond quickly to evolving risks and immediately report on any significant control failure (P. 82, Company A50)” .

iii) Organisational structure of IS/IT security

The analysis then proceeded to examine if there are any existing specific job roles relating to IS/IT security. Only 3 companies presented specific information of IS/IT security roles.

The existing established organisational structure with reference to the IS/IT security role was evidenced in two reports. The first was from Group A in the “Finance” industry sector;

“Operational Control and Information Technology Security” (P. 117, Company A6)

and second was from Group B in the “Trading/Services” industry sector;

“Management Team: (IT Security)” (P. 41, Company B101).

The existence of an organisational structure for IS/IT security unit/group within the two companies suggests that the boards and senior managements had clear IS/IT Security Visions in securing its IS/IT infrastructure and business data.

The analysis revealed that in one company the development of an IS/IT security role took place after the re-organisation of the IT department. This can be seen in the re-organisation process of the IT Department of one medium capitalisation company in five areas including ‘security’ which were stated as follows:

“Re-organisation of IT Department, IT department was re-organised taking the following attributes into consideration Focus, Specialisation, Functional Fit, Business-Aligned, Security and Career Centric (p. 42, Company B2)”

The board and senior management of Company B2 had shown that the protection of its IT infrastructure and business data is prioritised at governance level through the organisational structure of IS/IT security. The IS/IT security governance model suggests that the existing/potential organisational structure for IS/IT security would enhance the integration of expertise from different disciplines or departments in achieving effective operation of IS/IT and maintaining security over IS/IT.

iv) Education and Training relating to IS/IT security

Nine companies disclosed information on training attended by the board and senior management.

Six top capitalisation and three medium capitalisation companies disclosed information relating to training with regard to IS/IT security. For example,

“Importance of IT Security was attended by the board of directors (P. 70, CA8)”

“the boards and members of the Audit Committee in Company A21 attended training in “Importance of IT Security (p. 26 & 31, Company A21)”

and

“Directors’ Training: Importance of IT Security (P. 20, Company B18)”.

Apart from seeking disclosures on IS/IT security training attended by the Board and Senior Managers, information was sought about whether the corporation prepared, organised and held their own IS/IT security training for their internal employees. Only three companies disclosed information in this respect.

A workshop is identified as part of the education and training elements relating to IS/IT security. One larger company disclosed details on IS/IT security workshops conducted by the Risk Management Team for raising awareness on how to manage the risks. The statement relating to the workshop has already been presented in an earlier sub-section, Risk Management. The statement relating to workshop is represented as follows.

“Two additional workshops were carried out by the risk management team to enhance awareness of risk management in addition to the regular risk management induction programmes for new staff. There was also a workshop on “Business Information Security” to highlight various risks associated with information security (p. 99, Company A4)”.

Another company showed that a proactive strategy like an IS/IT security forum was seen to be important in the corporation's risk management programme. The forum is an interactive method to acquire information from employees about IS/IT security issues in the organisation.

"The Group maintains a strong knowledge of and continues to refine its mitigation strategies against Information Technology threats by participating in specific forums on Information Security and industry dialogues such as the Internet Banking Task Force. These initiatives contribute towards a systematic methodology to ensure the confidentiality, integrity, availability and non-repudiation of information and Information Systems against current or any potential threats prevalent in the evolving and changing internet world (p. 127, Company A6)".

The other example of training that was disclosed by a corporation is presented below:

"Throughout the year, the Company had conducted various training and development courses for the benefit of its staff for their career development and to provide better customer service and provide quality customer service. Among the trainings and courses held were Quality Management System and Information Security Management System training (p. 7, Company B11)".

In the IS/IT security governance model in Chapter 4 providing continuous education and training relating to IS/IT security is a critical strategy for the development of employee values and organisational values. Few companies disclosed details of training relating to IS/IT security.

v) Audit

The audit differs with internal controls to some extent. The audit uses the detection approach, while internal controls are a mechanism based on the prevention approach. The audit acts as a check and balance to evaluate the effectiveness of processes after implementation.

The auditing process is identified as part of the IS/IT Security Management Strategy in the IS/IT Security Governance Model. In this context, the Audit strategy helps management to evaluate the effectiveness of IS/IT security processes in many areas including IS/IT Security policies and IS/IT Security procedures implementation. In the context of IS/IT security governance, the IS/IT Security procedures are concerned with the application of security controls and security solutions. The management may use the audit results, such as deficiencies in IS/IT security procedures implementation, to determine the risks that are relevant to IS/IT assets and business data as set forth in the IS/IT Security Vision.

The annual reports were examined to discover whether companies included IS/IT security in the audit process. Only 5 companies disclosed details of audit scope in relation to IS/IT security. The determined areas for auditing within companies were varied.

As disclosed by two companies, the audit included the IS/IT Security procedures.

- *"The internal auditors also participate in risk management and IT projects to provide assurance of good governance and application of security controls (p. 20, Company B2)"*
- *"The scope of internal audit covers reviews of adequacy of the risk management processes, operational controls, financial controls, compliance with laws and regulations as well as management directives,*

lending practices and information technology, including the various application systems in production, data centres, and network security (p. 162 Company A2T)”

Apart from the IS/IT security procedures implementation, compliance on IS/IT security processes was part of audit areas covered.

- *“General IT Controls Review at Company A14, the audit scope includes review of overall IT management, delivery and support of service providers, access control management and compliance to Security Policy (p. 80, Company A14)”*
- *“A process audit was conducted by a consultant to determine the compliance and maturity level of Information Security in Company B4 (p. 62, Company B4)”.*

c) IS/IT Security Policy

IS/IT Security Policy is a higher level statement designed to maintain secure IS/IT assets and business data. While the IS/IT Security Management Strategy addresses how to achieve the IS/IT Security Vision, the policy document is developed as a platform for linking the IS/IT security management strategy with the board’s IS/IT Security Vision.

Information was sought about the disclosure of information on IS/IT Security Policies. Nine companies provided information; five from the top capitalisation companies and another four from the middle capitalisation companies. The following are examples of disclosed statements of IS/IT Security Policies.

Top capitalisation companies

“Company A13 has in place an IT Governance policy based on current Information Technology (IT) issues identified internally and raised by the Internal and External Auditors. It consists of six core policies, namely, IT Security Policy, IT Network Policy, IT Application Control Policy, IT Desktops, PDA, Email, Internet and Intranet Policy, Purchasing, Licensing and Usage of Corporate Software Policy and Business Continuity Facility Policy. (p. 116, Company A13)”.

Medium capitalisation:

“The Corporate Information Security Policy (CISP), which was developed and communicated to all staff, covers the management of information, data security and provides guidelines on the acceptable use of Company B4 IT resources. The CISP also provides basic guidance on operational controls related to information security at Company B4 Group of Companies. (p. 62, Company B4)”.

“The Group also formulated and implemented the ICT Policy and Guidelines to ensure proper protection of ICT resources, data integrity and security. The ICT Policy and guidelines were approved by the Board and enforced in April 2008 (p. 63, Company B3)”

“IT Policies and Procedures. There is also an IT Policy which incorporates the Corporate Policy on the usage of Personal Computer Software and Corporate Policy on the usage of E-mail and Internet. This is in addition to the IT Asset Hardware & Software Policy and the Security Implementation for the Antivirus Level Protection. These policies are established to achieve and maintain confidentiality,

integrity, availability, authenticity and reliability of information and information processing.(p. 70-71, Company B101)”.

There were various security areas covered in the IS/IT security policies as disclosed in the companies’ reports. The ultimate goal of IS/IT security policy was to achieve and maintain confidentiality, integrity and availability of the IS/IT assets and business data, regardless of company size.

Interestingly, the IS/IT security definition has been extended to authenticity and reliability of IS/IT assets and business data, as identified by a larger capitalisation company.

“IT policies and procedures are in place to achieve and maintain confidentiality, integrity, availability, authenticity and reliability of information or information processing facilities ...There are documented procedures in place that cover management accounting, financial reporting, procurement, information systems security, compliance and other risk management issues (p. 82, Company A50)”.

Organisational aspects such as policies were important elements of the IS/IT Security Governance Model to ensure that IS/IT assets and business data are secured from the intended actions of disgruntled employees, the intended actions of irresponsible employees and the unintended actions of naïve employees.

IS/IT security policy is a *direction-giving document* and is primarily derived from the board’s vision in conjunction with IS/IT. In the new informatics era, corporations take opportunities to adopt new business models such as E-business for remaining competitive in the globalised market. Employing new business has an effect on the IS/IT security policy. If the IS/IT security policy is already in place, it needs to be reviewed or up-dated accordingly to suit the IS/IT security vision and business goals. There were two sets of statements showing the important role of the IS/IT security vision in the IS/IT security policy development.

Group A

The following example presented the case of a top capitalisation company in the Finance industry sector:

“To support new business and service delivery capabilities, emphasis is also given to needed improvements in the overall IT infrastructure. The objective is to provide a more robust infrastructure to support the business and to better meet compliance requirements. We will also continue to invest in security management to enhance security integrity and to keep abreast with changes in the environment and to comply with security guidelines and policies” (p. 90, Company A2)

Group B

The other example of the IS/IT security policy and IS/IT security vision relationship is shown by the following company with a background in the “Trading/Services” industry sector:

“Company A13’s corporate security will now consolidate both physical and logical security under one programme within the corporate agenda, allowing for constant and proactive response to

new business concerns. In 2008, a comprehensive Corporate Security Policy was prepared to review and improve Company A13's security management.(p. 97, Company A13)"

The disclosure of IS/IT security policy in the company's annual report suggests that high amounts of IS/IT were used to support the business operations. The established policy demonstrates that the organisation has a structure, defined tasks and responsibilities in IS/IT security.

d) IS/IT Security Standards

IS/IT Security Standards are independent documents which may exist in any domain or business process. Normally, they only provide guidelines on what elements need to be implemented but do not cater for specific processes. In the IS/IT Security Governance Model, there are two types of IS/IT security standards, internal and external.

Seven companies disclosed information about IS/IT security standards. Most of the companies that disclosed the information had employed external security standards for security management practices.

- *"the data centres were certified with the International Standard of ISO27001, ensuring that the team maintains best practice in information security management system.(p. 39, Company A7)"*,
- *"Service delivery improvement works included: NSS Certification– A technology certification in compliance with security standards (p. 12, Company B101)"*

The external standard ISO27001 was the most popular International Standard used by disclosing companies.

6.4.1.2 Technical Component

The technical component of the IS/IT Security Governance Model identifies two layers; Technological Areas and IS/IT Security Procedures.

The Technological Areas are concerned with 'what' IS/IT areas need to be secured and aligned with the IS/IT Security Vision. The Technological Areas in the IS/IT Security Governance Model are divided into two layers; IT Infrastructure and Business Data and Information and Business Information Systems.

The IS/IT Security Procedures outline the IS/IT security controls processes or activities that need to be established and aligned with IS/IT Security Policy. The establishment processes of IS/IT Security Procedures are determined by the Technological Area.

Only 14 companies disclosed information on the Technological Areas and IS/IT Security Procedures.

a) Technological Resources Areas

i) IT Infrastructure and Business Data and Information

IT infrastructure is the physical facilities, IT components and IT personnel that provide the foundation for all of the organisation's systems for enabling and achieving business goals. Business data and information refer to all sensitive and confidential information that is exposed to the technologies, stakeholders or business processes. IT infrastructure and business data are closely related to each other because without IT infrastructure or business data in place the IS/IT security policy and IS/IT security procedures will not work.

Nowadays, legacy systems are still important in some corporations, their retention may be due to many factors such as high dependency on them, integration costs or the readiness of employees. However, the evolution of IS/IT in organisations today provides opportunities to invest in and up-grade IS/IT infrastructure for delivering business benefits such as:

“Company A6 invested RM45 million in upgrading its existing mission-critical ICT infrastructure and replacing legacy operating systems. The IBM z890 mainframe platform was replaced with the latest IBM z10 Enterprise Class mainframe computers with an increased total processing capacity and memory size of 1,908 million instructions per second (“MIPS”) and 64 Gigabytes respectively. The new mainframes also have inbuilt enhanced non-disruptive system maintenance features that allow maintenance work to be carried out without bringing down the system. Overall, the service level for core banking systems in terms of availability and response time has improved significantly (p. 170, Company A6)”.

In the case of Company A6, the adoption of new IT infrastructure offers expectations of benefits such as improving performance in terms of availability and response time. The up-grading of IT infrastructure would enable the corporation to achieve the security vision with regard to availability.

Protecting business data is critically important because it comprises confidential information like financial, accounting, internal processes, business strategies and customer data that are exposed to the IS/IT infrastructure. Security of business data and information could be compromised if there is no clear IS/IT security vision over the technological areas. In the disclosed information provided by the reports, security of business data was included within the IS/IT security policy to show how important it is.

- *“The Corporate Information Security Policy (CISP), which was developed and communicated to all staff, covers the management of information, data security and provides guidelines on the acceptable use of Company B4 IT resources. The CISP also provides basic guidance on operational controls related to information security at Company B4 Group of Companies (p. 62, Company B4)”.*
- *“IT policies and procedures are in place to achieve and maintain confidentiality, integrity, availability, authenticity and reliability of information or information processing facilities (p. 83, Company A50)”.*

The significance of business data and information can be influenced by the amount of IS/IT used for business operations. For example, Financial institutions, Services or Manufacturing based

companies require higher levels of security in terms of confidentiality, integrity and availability throughout their IT business operating systems depending on the IS/IT Security Vision. The following shows the importance of security counter-measures strategies to protect business data from being accessed by unauthorised or irresponsible people, as disclosed by a large capitalisation company in the financial sector.

“IT Security. In 2008, the Group continued to improve its Information Architecture with efforts in prevention, detection and response against internal threats, such as misuse of privileges, leakage of confidential data and external threats, such as third-party phishing websites and continued threats from aggressive malware (p. 127, Company A6, Finance)”.

ii) Business Information Systems

Business Information Systems are technological solutions based on business requirements. They support the integration of physical parts between departments and functional areas of the organisation to achieve certain business requirements. One report gives an example of Business Information Systems:

“To further enhance efficiency, effectiveness and security of communications throughout the Group, we have installed and commissioned Internet Protocol Virtual Private Network (IP-VPN) infrastructure during 2008 (p. 32-33, Company B32, Plantation)”.

Apart from supporting integration between departments, it also supports the entire organisation.

“The foundation project phase of Corporate Geographical Information Systems (GIS) is set to commence in FY08/09 and would span over the next four years. The ICT Division has been entrusted by CA12 Management to drive and coordinate the GIS corporate-wide initiative. This includes managing internal A12 fibre optic network, property management, security and logistics. A Service Oriented Architecture (SOA) solution will be included in the implementation scope to optimise the functionality of the Corporate GIS project and sharing of information between various A12 applications (p. 95, Company A12)”.

b) IS/IT Security Procedures

The IS/IT Security Procedures consist of security controls or solutions to ensure that the IT infrastructure, business data and information including business information systems are well protected. In an organisation, the IS/IT Security Procedures are implemented based on the acceptance of the risk level, Severe, Medium or Low, according to the technological areas identified. For instance, security counter-measures were put in place to safeguard the IS/IT infrastructure, as disclosed in a larger capitalisation company.

“ the special-purpose Cryptographic Coprocessor and Zip Specialty Processor of the new mainframes provide high speed data encryption/decryption to facilitate tape encryption and end-to-end network protection using standard industry security protocols such as IP Security and Secure Socket Layer. The implementation of tape encryption will eliminate the risk of unauthorised disclosure of data should any backup media be lost or stolen in transit (p. 170, Company A9)”.

The adoption of new business models such as E-Commerce applications has required organisations to increase the network security level due to the nature of the Internet which can be accessible by all. Since E-Commerce can reach suppliers, manufacturers, customers or business partners widely, providing effective security counter-measures has become essential to mitigate any possible risks. The following is an established IS/IT Security Procedure used for safeguarding a new business model, as disclosed by a large capitalisation company.

“In response to constantly evolving cyber security threats, a unified security management suite was commissioned to provide firewalling, intrusion prevention, security monitoring, analysis, and threat mitigation capabilities. The collaborative nature of the security suite facilitates identification of threats in a centralised manner, and provides self-defending network security capabilities to counter new security threats (p. 170, CA9)”.

The following disclosures show how other companies secure their IT infrastructure through the IS/IT security procedures.

- *The Division has implemented security upgrades in critical areas to ensure that data integrity within its ICT systems is not compromised (p. 92, Company A12, Trading/Services)”*,
- *“The Group has been upgrading its resorts’ network infra-structure to improve the speed and security of its services (p. 23, Company A33, Trading/Services)”*

6.4.1.3 Summary

The formal component comprised nine areas which were ‘IS/IT security vision’, ‘IS/IT security management strategy’, ‘risk management’, ‘IS/IT security internal controls’, ‘organisational structure of IS/IT’, ‘education and training relating to IS/IT security’, ‘audit’, ‘IS/IT security policy’ and ‘IS/IT security standards’.

In the IS/IT security vision, only six companies (of 210) disclosed information on the security vision of IS/IT. The majority who disclosed were from Group A. The three smaller issues highlighted in the IS/IT security vision were first, trade off between the IT management and risk management strategy, second, the alignment was needed to achieve business needs, security requirements and business goal. Third, the identification of critical business activities may lead to the critical risk management.

While in the IS/IT security management strategy, the goal of IS/IT security management strategy was to establish ways to achieve the IS/IT security vision. In the web analysis results five strategies were reported, which included ‘risk management’, ‘IS/IT security internal controls’, ‘organisational structure of IS/IT’, ‘education and training relating to IS/IT security’ and ‘audit’.

Risk Management

There were three companies from Group A which presented data relating to IS/IT security risk management. Four points of issue were highlighted; first, the importance of risk management to prevent potential business losses and bad reputation, second, the educational and awareness programme

needs to be conducted continuously within the risk management programme, third, development of an IT risk framework, and the fourth, the technological resources and security procedures considered in the risk management plan and covered by Audit.

IS/IT security internal controls

IS/IT security internal control was part of IS/IT security management strategy in the model of IS/IT security governance. Only two companies disclosed information relating to IS/IT security internal controls on the website. The issue brought out was how internal controls were applied in the risk management process.

Organisational structure of IS/IT security

The organisational structure referred to any specific security role relating to IS/IT security. There were three companies who released this information on the web. Surprisingly, two companies that revealed the specific role in IS/IT were from Group B. All the specific roles were handled on a group basis rather than on an individual basis.

Education and Training relating to IS/IT security

The educational aspect was also part of IS/IT security management strategy within the formal component. Nine companies revealed information on education and training aspects relating to IS/IT security, where the majority came from Group A. Two issues concerned with training were related to; first, the board of directors and senior management had attended the training relating to IS/IT security; and second, the development of IS/IT security training programme within organisation.

Audit

In the IS/IT security governance model, the audit process was an example of IS/IT security management strategy. In the website analysis, the goal of analysis was to examine if audit was conducted within the IS/IT processes. The analysis revealed that five companies had included IT within their audit process. The areas of IT covered by audit were IT projects, various application systems in production, data centres and network security, overall IT management, compliance to security policy and maturity level of information security.

IS/IT security policy

The IS/IT security policy is a communication tool, which connects the IS/IT security vision with IS/IT security management strategy. There were nine companies who made their IS/IT security policy public, with a balanced representation from each group, Group A and Group B. Several policies relating to IS/IT areas and IS/IT security controls had been disclosed on the website analysis. These include IT network policy, IT application control, IT desktop, PDA, e-mail, internet, intranet, purchasing, licensing and usage of corporate software, hardware, business continuity facility, management of information, data security and operational controls related to information security. The goal of IS/IT security policy was to maintain confidentiality, integrity and availability and these security elements can be extended to authenticity and reliability.

IS/IT security standards

The independent document, namely, IS/IT security standard, had two types, internal and external. The internal standard was written by the company and the external standard was developed and written by external bodies (local or international bodies). As reported in the website analysis, there were seven companies which showed what type of standards they used. All information reported came from the external standard and there was no information disclosed on internal standards. The external standards highlighted were International Standard of ISO127001 and NSS Certification— a technology certification in compliance with security standards. The most popular standard used was ISO127001.

Technical component

In the IS/IT security governance model, there were two layers of the technical component, first, technological areas and second, IS/IT security procedures. The technological areas comprised two inner layers, IT Infrastructure and Business Data/Information and Business Information Systems. And the IS/IT security procedures were concerned with security counter-measures/controls, where IS/IT security procedures were determined by technological areas. Interestingly, 14 companies made the information relating to technological Areas and IS/IT Security Procedures public on the website. Four issues underlined from the website analysis were first, the adoption of new infrastructure, second, the upgrading of IT infrastructure, third, the improvement of information architecture and fourth, the adoption of new business models.

Business Information Systems

Business information systems were technological solutions based on business requirements. The purpose of business information systems was to integrate parts between departments and functional areas to achieve certain business requirements. Two examples were brought up from the website analysis; Internet Protocol Virtual Private Network and Corporate Geographical Information Systems (GIS).

IS/IT Security Procedures

IS/IT security procedures supported the IT infrastructure, business data and business information systems. The adoption of security procedures was based on the acceptance of the risk level. The highlighted examples of IS/IT security procedures were two; first, security countermeasures— Cryptographic Coprocessor and Zip Specialty Processor, encryption/decryption, firewalling, intrusion prevention; and second, security controls—security monitoring, analysis, and threat mitigation capabilities.

The web disclosures did not yield much evidence of the impact of the involvement and the role of individuals. They do show that some companies appear to be deeply involved in IS/IT security matters. However, failure to disclose information on the website does not mean that companies and, hence, boards and senior managers are not involved in IS/IT security.

6.4.2 Data Analysis and Research Question 2

Research Question 2: *How can directing and monitoring actions in the technical, formal and informal components of IT/IS security governance in corporations be implemented efficiently and effectively?*

To answer Research Question 2, a single-case analysis of the interactions of components was conducted to determine if any data support the components interaction.

6.4.2.1 Component Interaction

In the IS/IT Security Governance Model, the inter-relationships among the three components of Formal, Technical and Informal are important to achieve good practice of IS/IT Security. Understanding the reciprocal requirements among the components enables the board and senior management to consider the factors involved in the implementation of the IS/IT Security Governance Model. The factors include the organisational culture, business vision and goals, management strategy, technological fit and employee values and beliefs.

6.4.2.1.1 The relationship between Formal and Informal components, Relationship Type 1

The following presents information disclosed on how the Formal component has an impact on the Informal component, as identified by one larger capitalisation company. The educational aspect is one of the formal elements in the IS/IT security governance model. The educational aspect may increase the organisational values and employee values. The example of this relationship (Formal/Informal) can be illustrated in the case of Company A6 (p. 127). The statements of Company A6 (p.127) have been presented in an earlier section, 'Education and Training relating to IS/IT security', but they were limited to the role of education and training within the formal component. However, the statements by Company A6 (p.127) are now represented, the main goal is to analyse the interaction between formal and informal components.

"The Group maintains a strong knowledge of and continues to refine its mitigation strategies against Information Technology threats by participating in specific forums on Information Security and industry dialogues such as the Internet Banking Task Force. These initiatives contribute towards a systematic methodology to ensure the confidentiality, integrity, availability and non-repudiation of information and Information Systems against current or any potential threats prevalent in the evolving and changing internet world. This enables the Group to retain its customer trust and maintain high rates of utilisation for the Group's products and services". (P. 127, Company A6)".

In the case of Company A6, the Formal components like Information Security Forums and Dialogues were crucial for the development of the Informal component. The mitigation strategies provided in the Formal component had influenced the way employees should work and interact with each other in achieving IS/IT security governance. For example, the *systematic methodology* was identified as the organisational values of the Informal component on how the employees should practise to maintain confidentiality, integrity, availability and non-repudiation of IS/IT assets and business data in their organisation. Indirectly, the good IS/IT Security Governance practices could

increase the confidence level of potential investors and maintain the trust of customers towards the organisation's services and products.

Interestingly, the IS/IT Security Management Strategies of the Formal component such as training and forums are important for the development of Organisational Values of the Informal component. The enforcement of formal educational aspects may reinforce informal values; all employees including the board, senior management including supervisors of the responsibility and holders of responsibility may begin to be responsible and accountable to their responsibilities, roles and separation of duties in IS/IT security.

The following is an example of the Formal/Informal relationship.

“The Directors have attended such trainings and forums in areas that would enable them to effectively discharge their duties to the Group and/or that are relevant to the Group's business activities (P. 70, CA8)”.

6.4.2.1.2 The relationship between Formal and Technical components, Relationship Type 2

The Formal component is important to the Technical component because it provides strategic directions, strategies and policy for the implementation of technological resources and IS/IT security procedures. The IS/IT Security Policy is developed to ensure employees maintain the security over IS/IT assets and business data such as:

“The Group also formulated and implemented the ICT Policy and Guidelines to ensure proper protection of ICT resources, data integrity and security (p. 63, CB3)”.

The objective of the IS/IT Security Policy is mainly to state basic guidelines on the acceptable use of IS/IT systems and the way of handling business data.

“The Corporate Information Security Policy (CISP), which was developed and communicated to all staff, covers the management of information, data security and provides guidelines on the acceptable use of Company B4 IT resources. The CISP also provides basic guidance on operational controls related to information security at Company B4 Group of Companies (p. 62, Company B4)”.

The Formal component such as the IS/IT Security Policy does not only provide technological guidelines to an organisation's employees but also demonstrates the credibility and high reputation of the organisation in securing the business data such as business strategies, accounting and financial information and customer data. The good IS/IT Security Governance practices may attract more investors and increase share market value. As disclosed by a large capitalisation company,

“In 2008, a comprehensive Corporate Security Policy was prepared to review and improve CA13's security management. The policy is based on international standards and reflects industry best practices. It applies to all CA13's assets, including means of handling, storing and processing information, and gives CA13 an edge over its competitors in terms of financial exposure and reputation for reliable and secure business practices (p. 97, CA13)”.

6.4.2.1.3 The relationship between Technical and Informal components, Relationship Type 3

IS/IT Security issues are not only technological issues but also social problems. Both components, the Technical and Informal need to be aligned. To achieve IS/IT Security, the implementation of the Technical component is associated with the Informal values held by workers such as organisational values and employee values. The organisational values relate to the responsibility of employees in achieving business processes, while the employee values concern the personal and ethical values held. Lacking any of these informal values, the implementation of the Technical component such as IS/IT Security Procedures may reveal discrepancies and unexpected behaviour. The following disclosure provides an example of the Technical/Informal relationship.

“the special - purpose Cryptographic Coprocessor and zIIP Specialty Processor of the new mainframes provide high speed data encryption/decryption to facilitate tape encryption and end-to-end network protection using standard industry security protocols such as IP Security and Secure Socket Layer. The implementation of tape encryption will eliminate the risk of unauthorised disclosure of data should any backup media be lost or stolen in transit (p. 170, CA9)”.

The next example shows how the Technical component such as IS/IT Security Procedures is important to the Informal component in preventing threats and vulnerabilities.

“Two- factor authentication was also introduced to safeguard e-Banking customers against unauthorized access. The enhanced security system incorporates a Public Key Infrastructure based hardware token which must be used in tandem with a Personal Identification Number to thwart key logging and phishing frauds (p. 170, CA9)”.

An effective Technical component like IS/IT Security Procedures may have had an impact in controlling and minimising the security threats by employees. Effective Technical component refers to the capability and ability in controlling and monitoring the activities of employees using particular IS/IT systems if any suspicious activities are detected the Technical component will inform the Informal component. The following statements illustrate how security counter-measures/controls such as web-surfing monitoring, e-mail transmissions, logs were used to control/minimise human actions.

“In 2008, the Group continued to improve its Information Architecture with efforts in prevention, detection and response against internal threats, such as misuse of privileges, leakage of confidential data and external threats, such as third-party phishing websites and continued threats from aggressive malware. New and improved systems have been installed to closely monitor the usage of Information Technology (IT) resources for staff. The monitoring occurs at the desktop level, such as web-surfing monitoring and email transmissions, and also at server and network level, where additional logs are centrally collated and monitored for suspicious activity (p. 127, CA6)”.

6.4.2.2 Summary

The interactions of three components, formal, technical and informal are significant in the IS/IT security governance model. The component interaction had three types, first, the Formal/Informal relationship (RT1), second, the Formal/Technical relationship (RT2) and third, Technical/Informal relationship (RT3). From the website analysis, the component interaction happened due to the reciprocal requirements among the components.

The relationship between Formal and Informal components, Relationship Type 1

From the website data, the educational aspect was an example of formal components. In the IS/IT security governance model, the educational aspect was recognised as an example of IS/IT security management strategy within the formal component. The formal component had interaction with the informal component through the educational aspect. The educational aspect, if effectively implemented, may improve the organisational values and employee values.

The relationship between Formal and Technical components, Relationship Type 2

The website analysis had provided an example of the formal component which was IS/IT security policy. IS/IT security policy had interactions with the technical component in two ways, technological resources and security procedures. The technological resources focused on the IT vision and the security procedures were concerned with security counter-measures/solutions. The existence of the formal component including policy may encourage the employees to implement the security procedures efficiently and effectively.

The relationship between Technical and Informal components, Relationship Type 3

It was found that the technical component had an impact on the informal component. From the website analysis, the automatic security counter-measures/controls had been used to control and minimise the actions of humans. Some of the automatic security controls to which attention was drawn were tape encryption and two-factor authentication. The website analysis also revealed that the non-automatic security counter-measures/controls affected the informal component. The non-automatic security counter-measures/controls highlighted were web-surfing monitoring, e-mail transmissions and logs.

Chapter 7 Data Analysis: Leximancer Software Analysis

7.0 Introduction

As stated in Chapter 5: Research Design and Methodology, the interview data were analysed using software analysis, namely, Leximancer Version 3.07.

The results of data analysis are presented in *concept map* form. In this study, the *concept map* was employed and three forms of output were utilised, first, the output presented in table form (e.g., *frequency*, *percentage*), second the output presented in the visualisation form (e.g., *thematic circles*, *ray*, *nodes*) and third the output presented in the text form (e.g., *query results*, *knowledge pathway*). The details of the concept map and its output forms are explained in Appendix 7A.

In this study, the *concept map* and its features are to be used in the process of exploring research questions 1 and 2.

7.1 Concept Map

7.1.1 Concepts

During the preliminary analysis, 31 *concepts* were identified from the map output. The objective of the preliminary stage was to ensure that the concepts found are relevant for further analysis. This was done by examining the entire meaning of the text involved in a particular concept (through a directed-fashion provided by the software). After reviewing all 31 concepts, the analysis showed that the “security” concept added little value to the analysis. This was because the interview questions were predominantly about the “security” of IT/IS. In fact, this led to a high frequency of responses for the “security” word within the interview documents. For this reason, the “security” concept will be excluded from further analysis resulting in 30 concepts. The output and its analysis over 30 concepts are discussed in the next section.

As previously stated, 30 *concepts* were displayed (see Table 7.1) and used for analysis. The 30 concepts were ranked by count of text segments which contain the concept throughout the data.

While the relevant score (per cent) provides the number of occurrences of the *concept* as a proportion of the most frequent *concept* (Leximancer Manual, 2009), the ranked *concepts* lists are used to determine what concepts were discussed most and least within the interview documents.

From Table 7.1, “policy” was found to be the most frequent *concept* in the analysis with a relevance score of 100%.

The next concepts, “controls” and “issues” were ranked number two and three in terms of number of occurrences of the *concept* and in proportion to the most frequent “policy” *concept*. The *concept* “internal”, number four, appeared more frequently than “management” (5th rank), “level” (6th rank), “risk” (7th rank), “implementation” (8th rank), “informal” (9th rank), “ensure” (10th rank) and “technical” (11th rank).

The “staff” *concept* had a relevance score of 27% and ranked number 12 compared to the most frequent *concept*.

The *concepts* of “system”, “monitor” and “meeting” (13th rank) had a quarter of the relevance score of the most frequent *concept*.

Concept	Count (Frequency)	Relevance (Per cent)
policy	99	100%
controls	52	53%
issues	51	52%
internal	48	48%
management	45	45%
level	42	42%
risk	38	38%
implementation	35	35%
informal	29	29%
ensure	29	29%
technical	28	28%
staff	27	27%
system	26	26%
monitor	26	26%
meeting	26	26%
place	24	24%
business	23	23%
committee	23	23%
information	22	22%
aspects	21	21%
people	21	21%
employees	20	20%
important	19	19%
things	17	17%
training	17	17%
corporation	16	16%
take	16	16%
example	14	14%
plan	13	13%
factors	13	13%

Table 7.1 Concepts and its frequency and relevance score

The remaining *concepts*, in order of frequency, were “place” (14th rank), “business” and “committee” (15th rank), “information” (16th rank), “aspects” and “people” (17th rank), “employees” (18th rank), “important”(19th rank), “things” and “training” (20th rank), “corporation” and “take” (21 in rank), “example” (22 in rank) and finally “plan” and “factors” (23 in rank).

Figure 7.1 shows the visualisation of *concepts* on the map output, some concepts are clustered together and some are some distance away from other concepts. The co-location on the map indicates levels of relationship between these concepts in the data set. This visualisation is influenced by the level of co-occurrence of concepts which will be discussed in the next section.

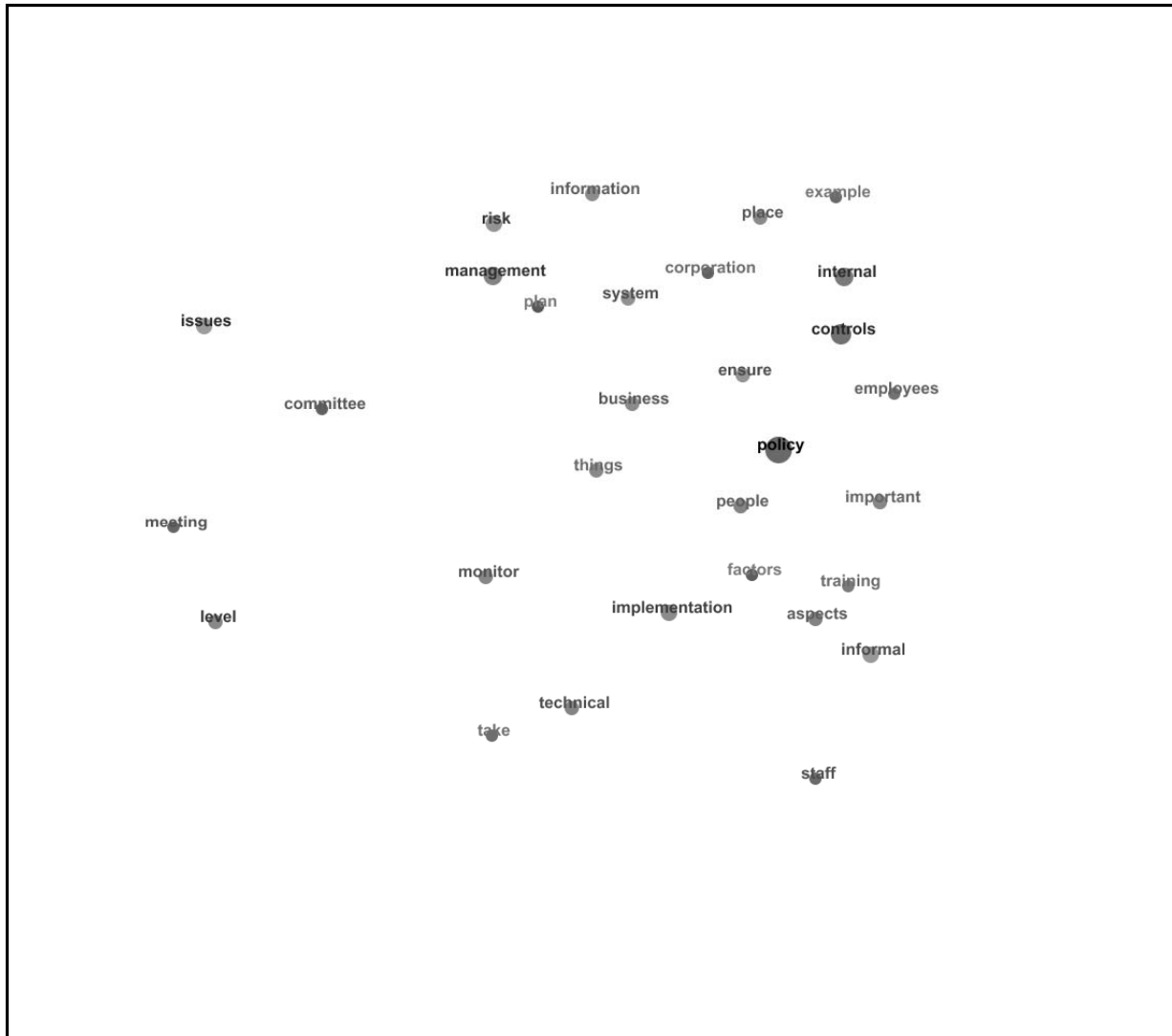


Figure 7.1 The visualisation of *concepts* on the map

7.1.1.1 Co-occurrence of Concepts

Apart from measuring the frequency and relevance score of the extracted *concepts*, Leximancer also can measure how often concepts occur close together within the text. As stated previously, co-occurrence is the degree of association between *concepts* in the text.

Examining the co-occurrence of the *concepts* is important in order to know how the *concepts* were visualised and placed on the map output. The higher the frequency in the text, the closer together in the map.

An examination of the strength of each concept with other *concepts* was done by clicking on each concept in turn. The connectedness of *concepts* on the visualisation map can be determined by either count (frequency) or likelihood (per cent). The related concept contains count (frequency) of co-occurrence of each related concept with the selected concept. While the other one, the likelihood score, presents the conditional probability of co-occurrence between two *concepts*.

Apart from using count or likelihood scores in a ranked table, the colour of the line (ray) also can be used to represent the co-occurrence between *concepts*. The brightness of the line reflects the strength of the relationship between the *concepts*.

a) Concept: Policy

The “policy” concept showed a strong co-occurrence with these *concepts*- “implementation”(21), “controls”(30) and “internal”(27). See Table 7.2. The “policy” concept also had high scores in likelihood with *concepts* of “implementation”, “controls” and “internal”

“Policy” concept had some co-occurrence with *concepts* of “aspects”, “ensure”, “informal”, “staff”, “business”, “monitor”, “place” and “management”, “issues” and “risk”. Even though the “policy” showed some occurrence with “aspects” concept the relationship between “policy” and “aspects” *concepts* was found high in the likelihood score (62%). “Issues” and “risk” *concepts* had a low likelihood score.

Concept: Policy		
Related Concept	Count (Frequency)	Likelihood(Per cent)
Aspects	13	62%
Implementation	21	60%
Controls	30	58%
Internal	27	56%
Ensure	16	55%
Informal	14	48%
Staff	13	48%
Business	11	48%
Things	8	47%
Employees	9	45%
Monitor	11	42%
Important	8	42%
Place	10	42%
Management	16	36%
Training	6	35%
Committee	8	35%
Information	7	32%
Corporation	5	31%
System	8	31%
Factors	4	31%
People	6	29%
Issues	14	27%
Risk	10	26%
Technical	7	25%
Plan	3	23%
Example	3	21%
Level	8	19%
Meeting	3	12%
Take	1	06%

Table 7.2 The co-occurrence of the “policy” with other related *concepts*

The occurrence of “policy” concept with other *concepts* also can be seen through the brighter colour of the rays (lines). The brightness of the rays was shown in the reflection of “policy” with these *concepts*: “internal”, “control” and “implementation”, Figure 7.2. “Policy” concept was contextually clustered with “internal” and “controls” *concepts* and appeared in similar contexts with “implementation”.

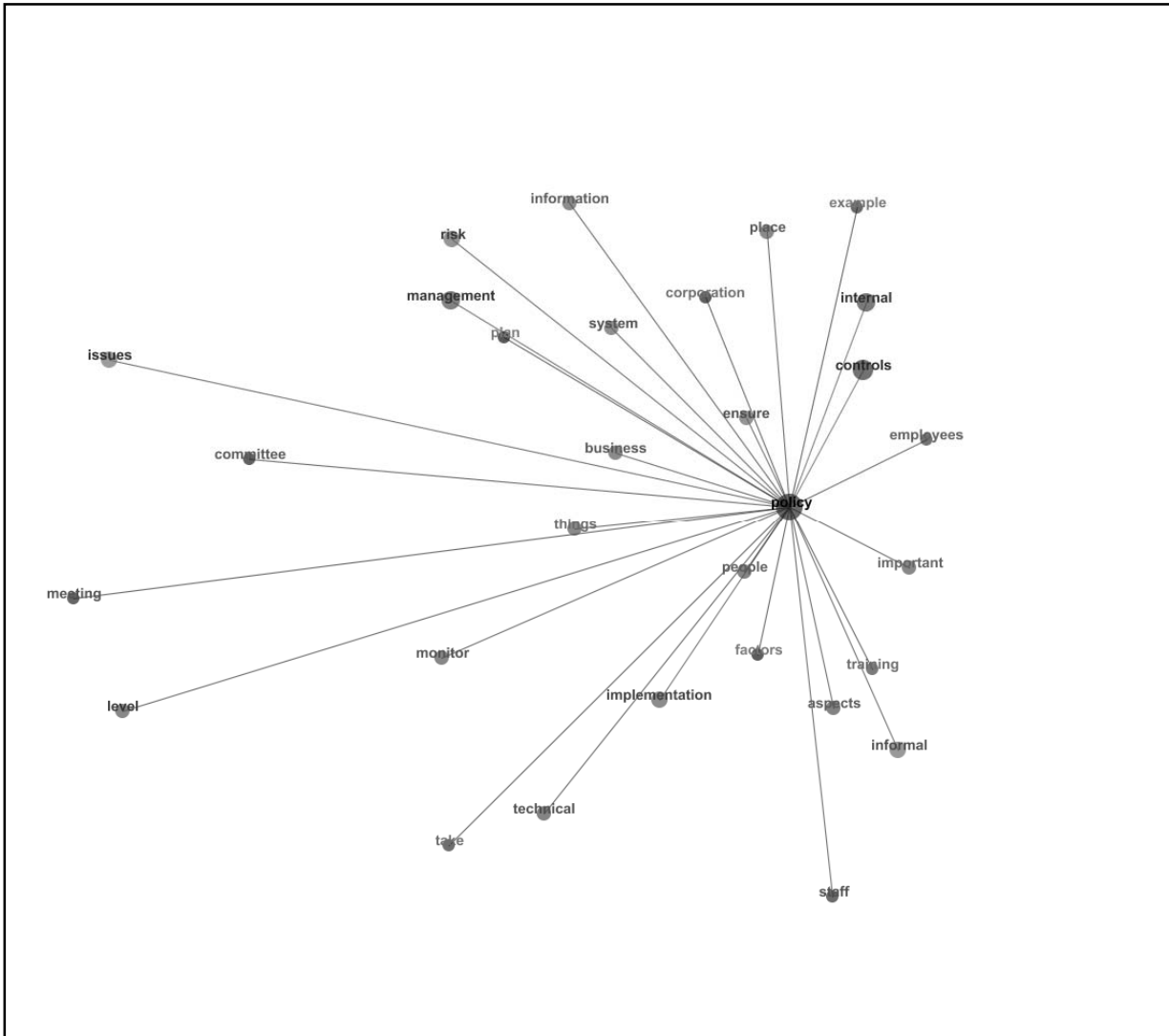


Figure 7.2 The co-occurrence of the “policy” with other related *concepts* by its brightness of ray colour

b) Concept: Controls

The “controls” concept had a strong co-occurrence with “internal”(41) and “policy”(30) *concepts*. The “controls” concept also had a high score in likelihood with “internal” concept (85%) but a low likelihood score with “policy” concept (only 30%).

The “controls” concept had some co-occurrence with the *concepts* of “place”, “ensure” and “system”. The likelihood score of “controls” concept was higher in “place” concept (42%) than “ensure”(34%) and “system” (35%) *concepts*.

Concept: Controls		
Related Concept	Count	Likelihood
Internal	41	85%
Example	6	43%
Place	10	42%
important	7	37%
things	6	35%
system	9	35%
ensure	10	34%
people	7	33%
policy	30	30%
employees	6	30%
business	6	26%
factors	3	23%
implementation	8	23%
information	5	23%
risk	8	21%
informal	6	21%
Aspects	4	19%
management	8	18%
training	3	18%
monitor	4	15%
plan	2	15%
technical	4	14%
corporation	2	13%
staff	3	11%
level	4	10%
committee	2	09%
take	1	06%
issues	3	06%
meeting	1	04%

Table 7.3 the co-occurrence between “controls” concept with others

In Figure 7.3, the “controls” concept shows the brighter ray colour with two *concepts* which were “policy” and “internal”. The *concepts* of “controls” and “internal” were contextually clustered on the map. While *concepts* of “controls” and “policy” were adjacent on the map.

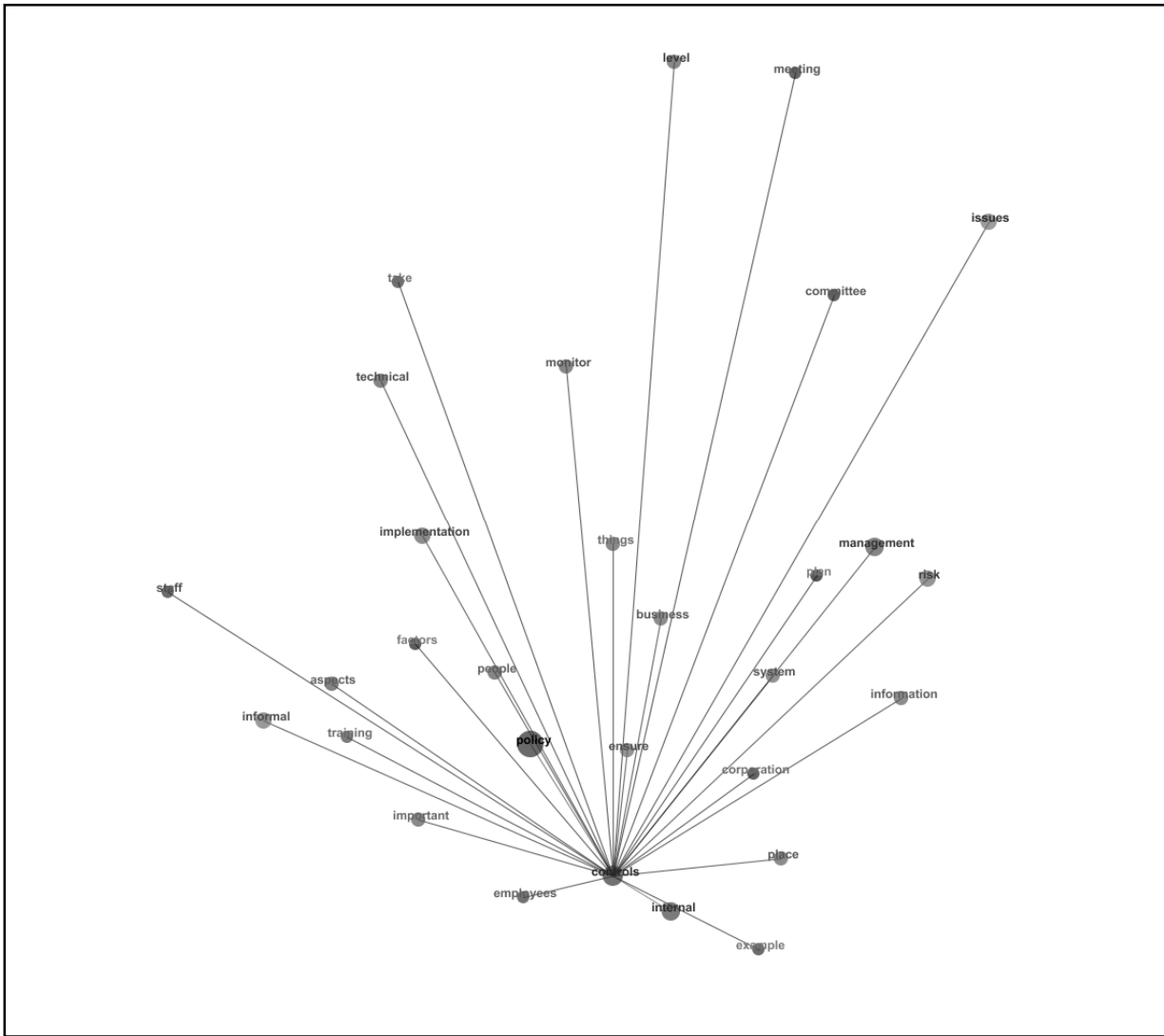


Figure 7.3 The co-occurrence of the “controls” with other related *concepts* by its brightness of ray colour

c) Concept: Issues

The “issues” concept had co-occurred frequently with *concepts* of “meeting”(13), “level”(13), “management”(13) and “policy”(14).

The relationship between “issues” and “policy” even though the co-occurrence value was high had a low score in likelihood (only 14%).While, the likelihood score of “issues” was higher with “meeting” (50%) than with “level” (31%) and “management” (29%).

The “issues” concept had little co-occurrence with other *concepts* throughout the data.

Concept: Issues		
Related Concept	Count	Likelihood
Meeting	13	50%
Plan	5	38%
Level	13	31%
Management	13	29%
Information	5	23%
Business	5	22%
risk	8	21%
system	5	19%
monitor	5	19%
corporation	3	19%
committee	4	17%
factors	2	15%
policy	14	14%
training	2	12%
ensure	3	10%
internal	4	08%
place	2	08%
staff	2	07%
example	1	07%
things	1	06%
controls	3	06%
implementation	2	06%
employees	1	05%
aspects	1	05%
technical	1	04%
informal	1	03%

Table 7.4 the co-occurrence between “issues” concept with others

In Figure 7.4, the “issues” concept had a brighter ray colour with the *concepts* “meeting”, “level”, “management” and “policy”. The concept “issues” was clustered together with “meeting” and “level”, appeared contextually with “management” and some distance away from “policy” .

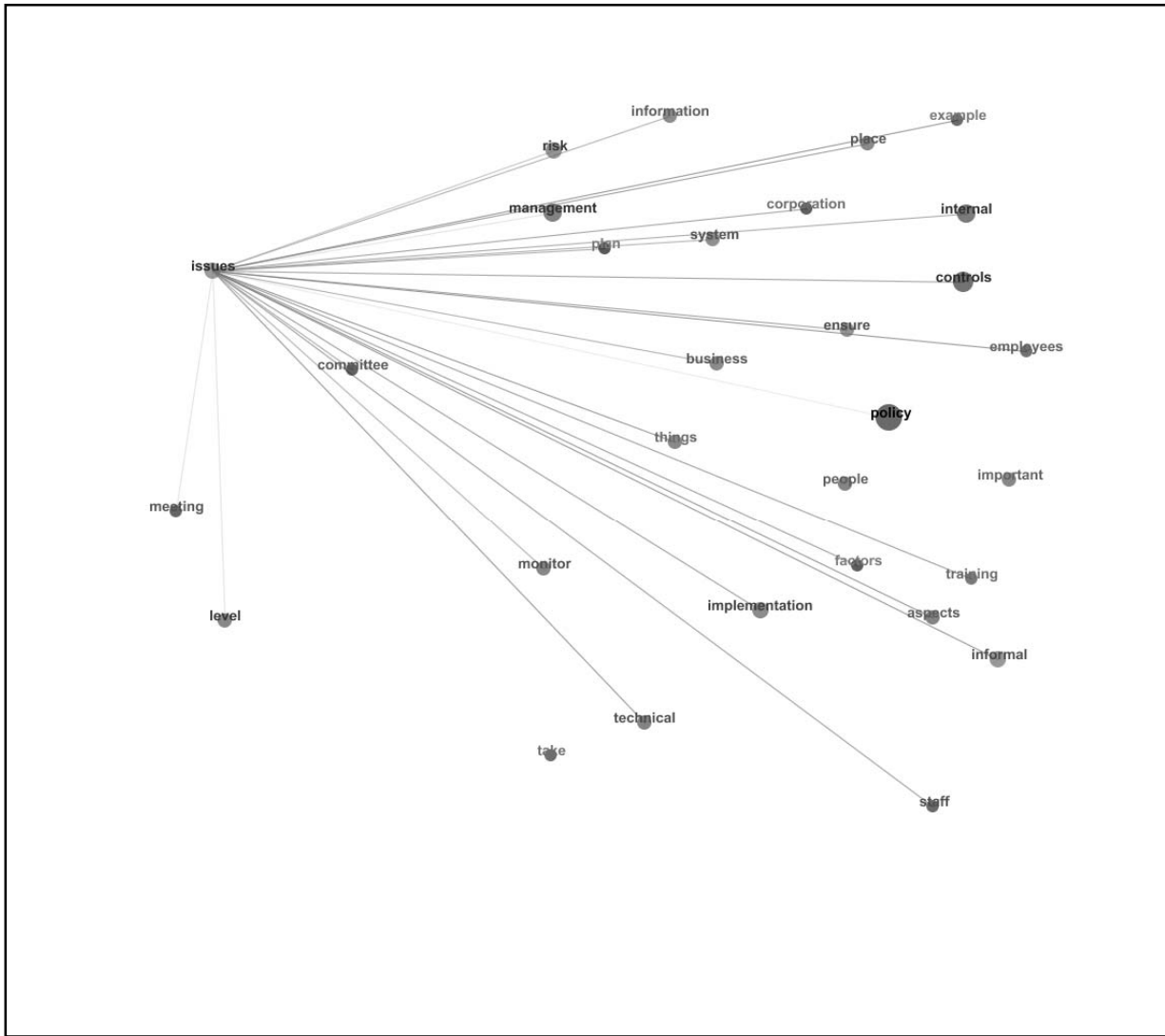


Figure 7.4 The co-occurrence of the “Issues” with other related *concepts* by its brightness of ray colour

d) Concept: Internal

The “internal” concept showed a strong co-occurrence with the *concepts* of “controls” and “policy”. The likelihood score of “internal” with “controls” (79%) was much higher than “policy” (27%).

The “internal” concept had little co-occurrence with other *concepts* within the interviews.

Concept: Internal		
Related Concept	Count	Likelihood
Controls	41	79%
Example	5	36%
Place	8	33%
Things	5	29%
Policy	27	27%
Information	6	27%
Important	5	26%
Employees	5	25%
System	6	23%
Implementation	8	23%
Ensure	6	21%
Management	9	20%
Risk	7	18%
Monitor	4	15%
Plan	2	15%
People	3	14%
Informal	4	14%
Business	3	13%
Training	2	12%
Level	4	10%
Aspects	2	10%
Committee	2	09%
Issues	4	08%
Factors	1	08%
Technical	2	07%
Corporation	1	06%
Take	1	06%
Meeting	1	04%

Table 7.5 The co-occurrence between “internal” concept with others

Figure 7.5 shows brighter rays between “internal” and “controls” and “policy”. The concept “internal” appeared adjacent to “controls” on the map but some distance away from “policy”.

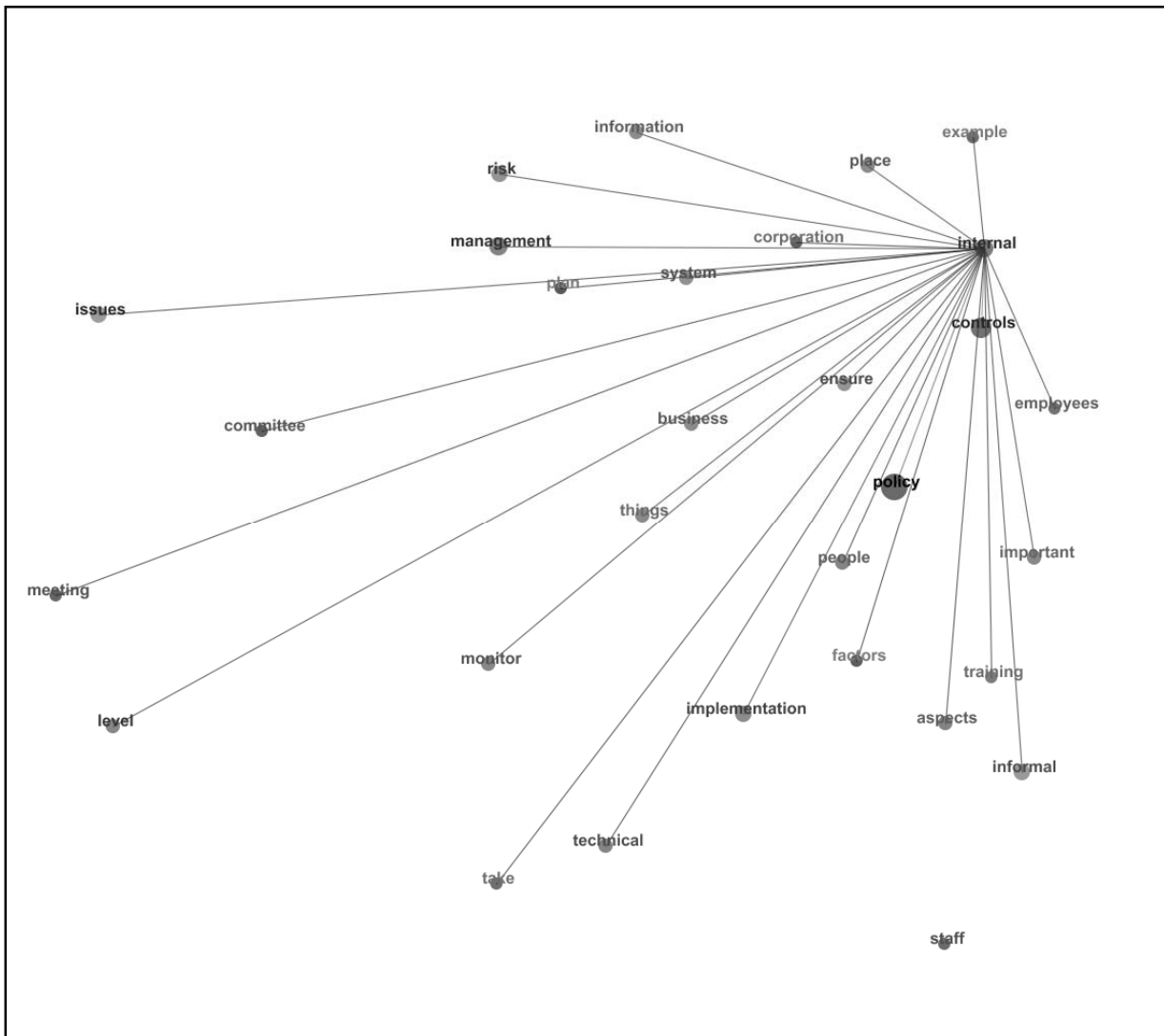


Figure 7.5 The co-occurrence of the “internal” with other related *concepts* by its brightness of ray colour

e) Concept: Management

The “management” concept co-occurred frequently with “risk”, “issues” and “policy” but the likelihood of “management” showed a low score with “policy” (only 16%).

The “management” concept had little co-occurrence with other *concepts* throughout the interviews.

Concept: Management		
Related Concept	Count	Likelihood
Risk	22	58%
Plan	7	54%
Information	10	45%
System	9	35%
Place	8	33%
Business	7	30%
Things	5	29%
issues	13	25%
corporation	4	25%
people	5	24%
factors	3	23%
internal	9	19%
take	3	19%
committee	4	17%
policy	16	16%
controls	8	15%
aspects	3	14%
ensure	4	14%
training	2	12%
monitor	3	12%
implementation	4	11%
important	2	11%
employees	2	10%
level	4	10%
meeting	2	08%
staff	2	07%
technical	2	07%
example	1	07%
informal	1	03%

Table 7.6 the co-occurrence and likelihood between “management” concept with others

The strength of the relationship of the “management” concept with others can also be determined by brightness of the rays. The brighter rays are seen with three *concepts* between “management” and “risk”, “issues” and “policy”. “Management” is clustered contextually with “risk”. Even though the “policy” concept is some distance away from “management” and “issues” they appear in similar contexts.

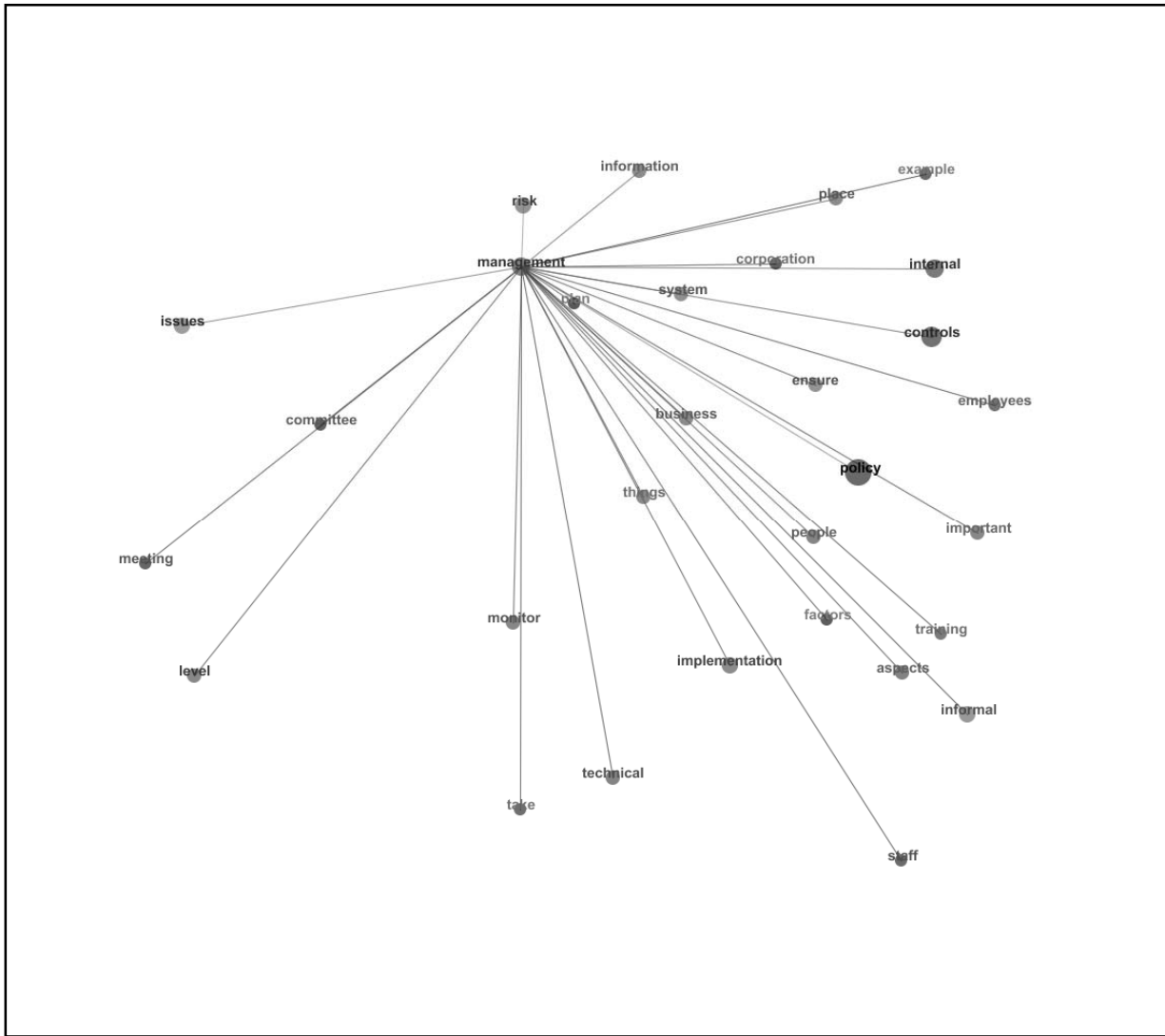


Figure 7.6 The co-occurrence of the “management” with other related concepts by its brightness of ray colour

f) Concept: Level

The “level” concept showed co-occurrence with the *concepts* of “meeting”, “issues” and “policy”. The “level” concept also had scored some in likelihood with *concepts* “meeting” (38%) and “issues” (25%) but low with the “policy” concept (8%).

Concept: Level		
Related Concept	Count	Likelihood
meeting	10	38%
take	5	31%
things	5	29%
issues	13	25%
monitor	4	15%
implementation	5	14%
staff	3	11%
technical	3	11%
people	2	10%
information	2	09%
management	4	09%
business	2	09%
committee	2	09%
internal	4	08%
policy	8	08%
risk	3	08%
controls	4	08%
system	2	08%
factors	1	08%
plan	1	08%
informal	2	07%
ensure	2	07%
corporation	1	06%
training	1	06%
important	1	05%
employees	1	05%
aspects	1	05%
Place	1	04%

Table 7.7 the co-occurrence and likelihood between “level” concept with others

Three brighter rays were found between “level” and “meeting”, “issues” and “policy” in Figure 7.7. It shows the “level” concept clustered with the “meeting” concept. The “level” concept appears close to “issues” but some distance away from “policy”.

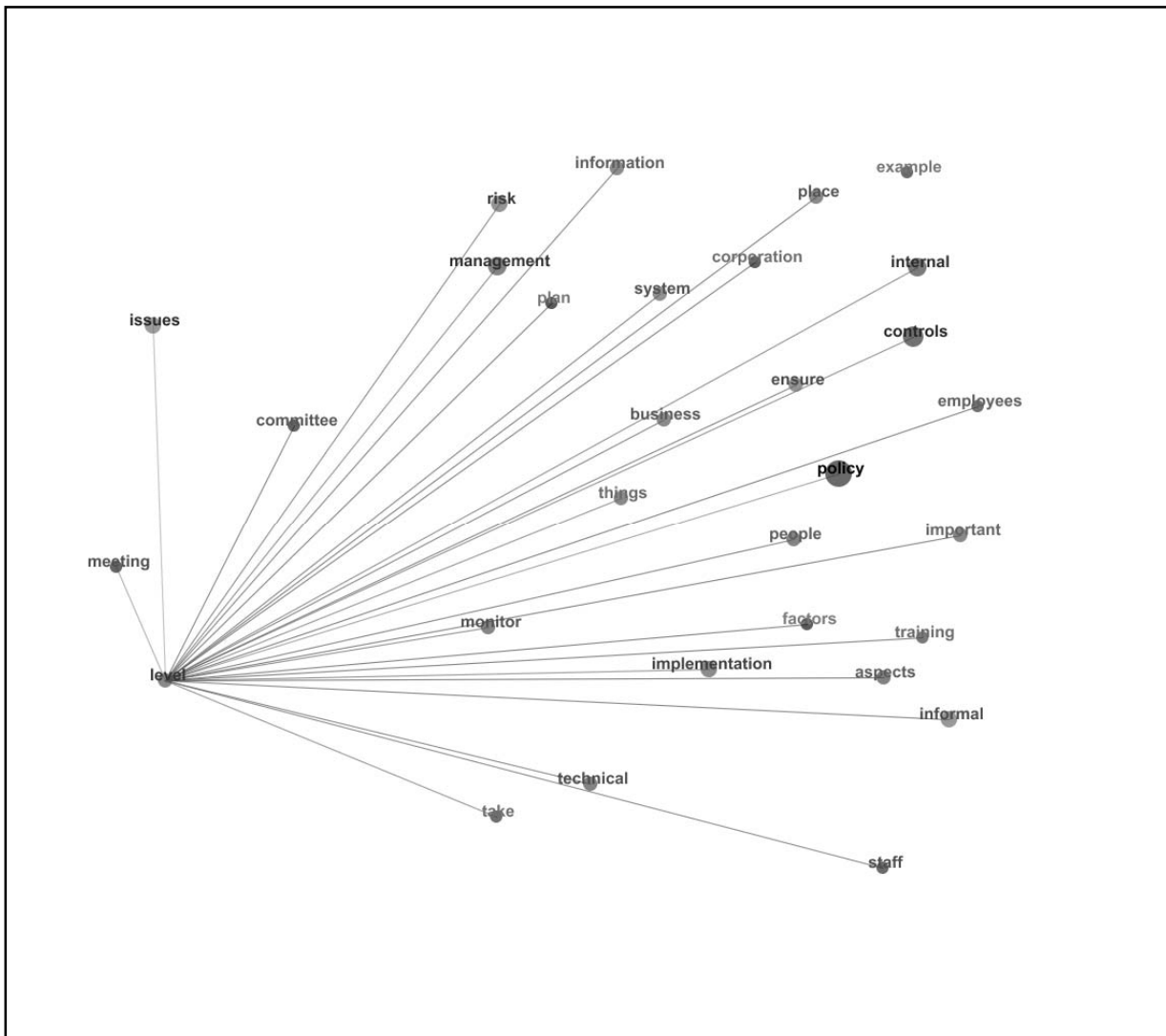


Figure 7.7 The co-occurrence of the “level” with other related *concepts* by its brightness of ray colour

g) Concept: Risk

The “risk” concept demonstrated high co-occurrence with the “management” concept and some co-occurrence with “policy”, “issues”, “controls” and “plan”. “Risk” also scored high with “management” in the likelihood measurement. Although the co-occurrence value of “risk” with “plan” was not high they showed a high score in likelihood.

Concept: Risk		
Related Concept	Count	Likelihood
Plan	8	62%
Management	22	49%
Things	6	35%
Information	6	27%
Place	6	25%
Factors	3	23%
Business	5	22%
Committee	5	22%
System	5	19%
Corporation	3	19%
Take	3	19%
Issues	8	16%
Controls	8	15%
Internal	7	15%
People	3	14%
Ensure	4	14%
Training	2	12%
Important	2	11%
Policy	10	10%
Employees	2	10%
Aspects	2	10%
implementation	3	09%
Monitor	2	08%
Level	3	07%
Example	1	07%
Meeting	1	04%
Technical	1	04%
Informal	1	03%

Table 7.8 the co-occurrence between “risk” concept with others

Figure 7.8 shows only one brighter ray, the relationship between “risk” and “management”. Both *concepts* were contextually clustered on the map.

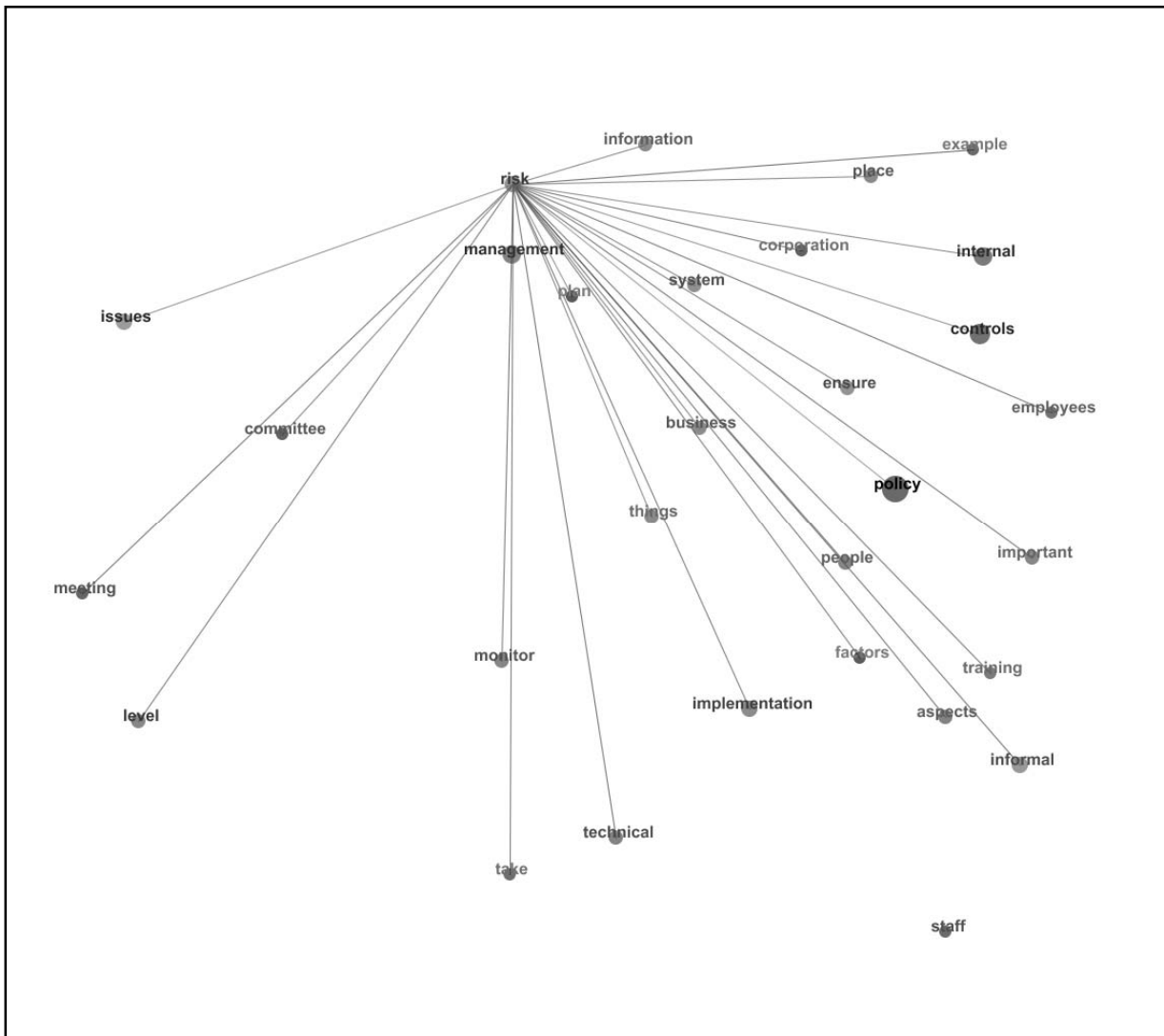


Figure 7.8 The co-occurrence of the “risk” with other related *concepts* by its brightness of ray colour

h) Concept: Implementation

The “implementation” concept had strong co-occurrence with “policy”(21), “monitor”(13), “informal”(11) and “technical”(10). “Implementation” also had a high likelihood score with “monitor” (50%). But the “implementation” concept had scored low in the likelihood measurement.

Concept: implementation		
Related Concept	Count	Likelihood
Monitor	13	50%
Factors	5	38%
Aspects	8	38%
Informal	11	38%
Important	7	37%
Technical	10	36%
Things	5	29%
Policy	21	21%
Training	3	18%
Committee	4	17%
Internal	8	17%
Controls	8	15%
System	4	15%
Staff	4	15%
People	3	14%
Example	2	14%
Ensure	4	14%
Business	3	13%
Level	5	12%
Meeting	3	12%
Management	4	09%
Risk	3	08%
Plan	1	08%
Corporation	1	06%
Take	1	06%
Employees	1	05%
Issues	2	04%

Table 7.9 The co-occurrence between “implementation” concept with others

The brighter ray was found in the relationship between “implementation” and “policy”. These *concepts* appeared in similar contexts.

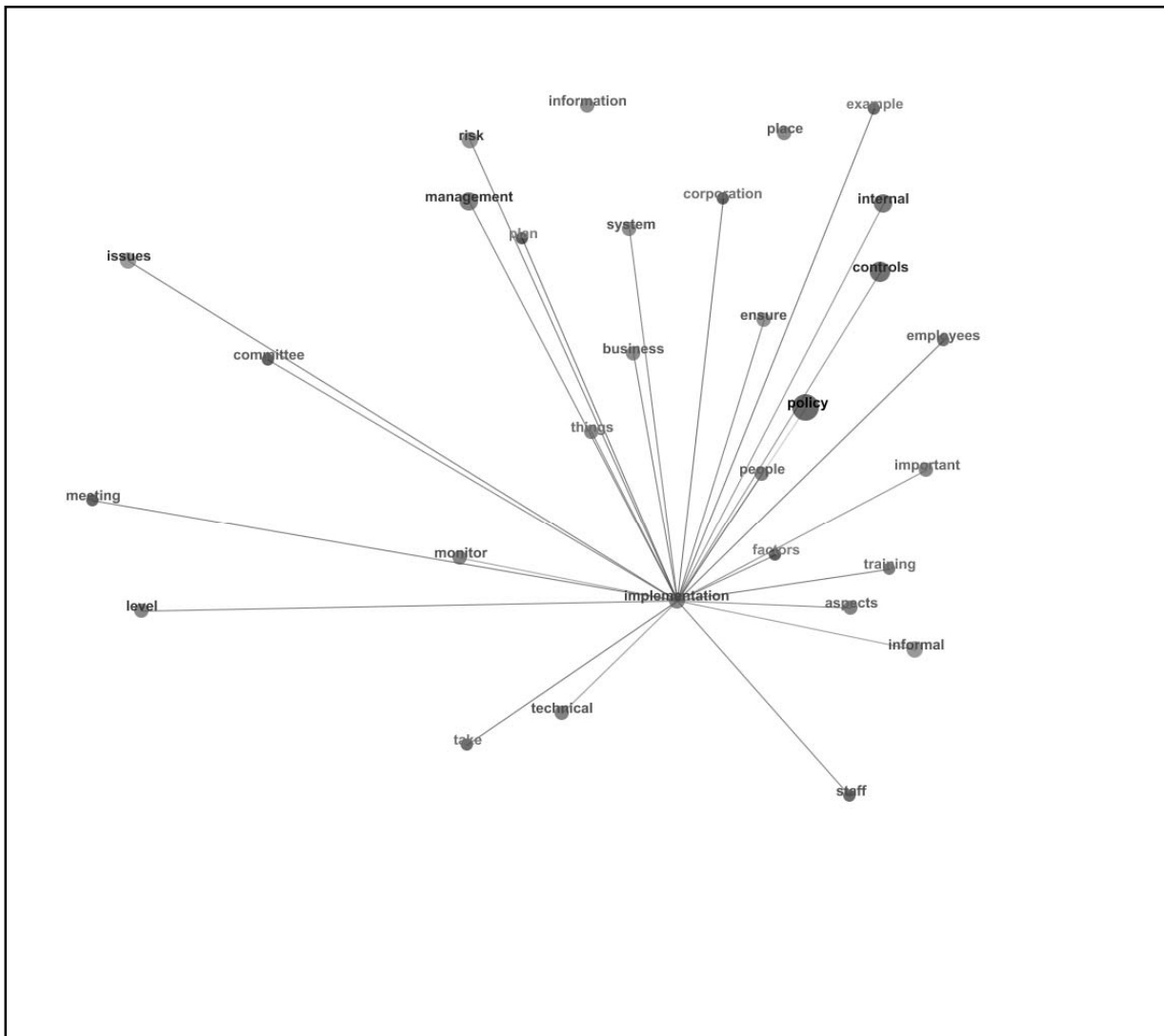


Figure 7.9 The co-occurrence of the “implementation” with other related *concepts* by its brightness of ray colour

In brief, the visualisation of *concepts* on the map is determined by co-occurrence values and also likelihood scores which have been discussed earlier. The *concepts* that appeared together frequently within the text were settled closely together on the map. *Concepts* with similar interests or topics appeared in similar contexts with the other *concepts*. Clusters of *concepts* which appear contextually normally represent a thematic group, and are discussed further in the next section.

7.1.2 Themes

Clusters of *concepts*, *themes*, are formed as a result of the co-occurrence value and likelihood score of *concepts*. In Leximancer, the dominant concept within the cluster group will represent the thematic group name. For example, the Leximancer analysis yielded five dominant themes. This can be seen through the proximity and intersection of themes between the concept groups. In order of the connectivity of the themes to others, these themes were “policy”, “management”, “informal”,

“implementation” and “monitor”. The co-location on the map indicates a greater association between the *concepts* within the data set. See Figure 7.10.

In the generic map, the “policy” theme was the major theme containing three of the primary *concepts*, “policy”, “controls” and “internal”. The remaining *concepts* impacting this theme were also identified: “ensure”, “place”, “corporation” and “example”. Connectivity Scores represent the degree to which the constituent *concepts* in each theme are connected with others on the concept map. The proximity of the “policy” theme to the themes of “management” and “informal” indicate the high level of relationship between these concept groups. In the greater association, the “policy” theme intersected with the themes of “implementation” and “business” and contained none of the *concepts* identified as being primary. The overlaps in the themes show a close association between the *concepts* within the data set.

The “management” theme contained two primary *concepts*, “risk” and “management” and three supplementary *concepts*: “system”, “information” and “plan”. The “management” theme overlapped with the “business” theme and incorporated none of the primary *concepts*.

The “informal” theme did not contain any primary *concepts* and intersected with “implementation” and “staff”. The four *concepts* which formed the “informal” theme were “informal”, “aspects”, “important” and “training”. The proximity of the “informal” theme to the “policy” theme indicates the strong relationship between these two concept groups.

The “implementation” theme contained the primary concept “implementation” intersected with the “business” theme and two dominant themes, “policy” and “informal”. The additional *concepts* identified were “people” and “factors”.

The theme of “monitor” encapsulated none of the primary *concepts* but contained the *concepts* “monitor”, “technical” and “take”. The proximity of the “monitor” theme to the “implementation” theme on the map indicates a close association between concept groups.

The “business” theme contained the *concepts* “business” and “things”. This theme had intersections with dominant themes of “policy”, “implementation” and “management”.

The “issues” theme which contained the primary concept “issues” was in a separate theme and did not intersect with any other themes. The supplementary concept identified was “committee”.

The “level” theme which contained the primary concept “level” and the additional concept “meeting” was in its separate theme and did not overlap with any other themes.

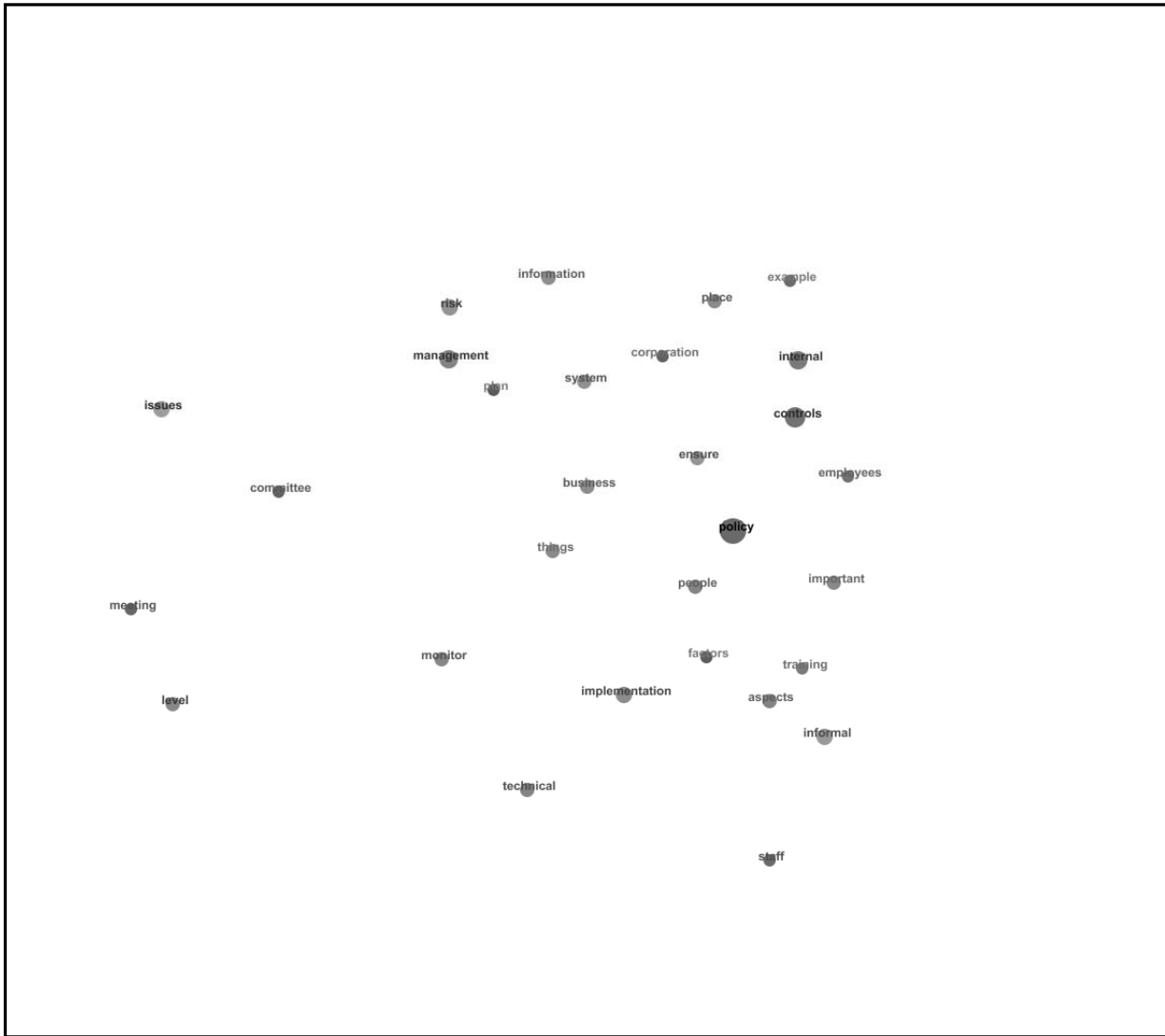


Figure 7-10 The *concepts* within the data set

7.2.1 Results (*Concepts*, Themes, Co-Occurrence) and Research Question 1

RQ1: In what way does the involvement of boards and senior management impact on the implementation of IT/IS security governance?

To answer Research Question 1, overlaps and proximity of themes and co-occurrence of primary *concepts* would indicate the types of involvement by the boards and senior managements of corporate participants. The analysis of *concepts*, the co-occurrence results between the seven *concepts* of “policy”, “controls”, “issues”, “internal”, “management”, “risk” and “implementation” suggest that the boards and senior managements of the participant organisations were involved through the implementation of IT/IS security governance in these areas. The expected IT/IS security governance components such as policies, internal controls and risk management were visible on the map.

The analysis of interviewees' comments within primary *concepts*, dominant themes and co-occurrence results highlights five ways in which the boards and senior managements were involved in the implementation of IT/IS security governance. These five areas are identified in the following sub-sections.

1) Policy relating IT/IS security

Participants were involved in the formulation and implementation of policy relating to IT/IS security. IT/IS security policy, like all other policies, is approved by the Board and senior management. Many comments supported these notions associated with IT/IS security policy in place.

The CEO of Company F stated :

"The management headed by myself, and of course the IT department and the internal audit were involved in the formulation of IT/IS security policy. We have a number of policies and procedures here, you may want to have a look the major headline of policies relating to IT/IS security- System information access control, Physical and environmental security, Network management, Back up and restoration, System back up and ownership, IT system change management, Problem management and IT system capacity management."

There are other examples of involvement in IT/IS security policies.

The CEO of Company A highlighted the security issues areas of policy covered in his corporation:

"The security issues that are included here in the policy are related to network connectivity, account management, vulnerability management, secure system development, incident management, host protection and authentication".

The CIO of Company B reported:

"We have five basic security policies that cover backup, internet use, email use, desktop appearance and data classification."

The CIO of Company D shows what his security policy covers, including mobile:

"For security areas, it covers everything, e-mail policy, information security, I mean in terms of what kind of information you can disseminate, in terms of you labelling the information, confidential, secret, internal use, and then desktop management inclusive, network, mobile. Mobile is formed under baseline, because security, inside a lot of items there, a lot of things, desktop baseline, quite several of baselines, very extensive in terms of (the area covers). We have also internet policy. In which it mentioned, all the internet facilities are meant for company purposes. In fact some of the non-business related sites are being blocked for staff to access."

As noted by the CEO of Company G:

"the security policy covers issues like access, return to operation (system down) and acceptable run time."

2) Policy, IT/IS security and internal controls

Some participants reported that IT/IS security is part of their internal controls. Internal controls were used to achieve policy relating to IT/IS security. The following comments were made by participants.

“we do have internal controls to ensure the goals of IT security policies are implemented as intended. Internal Risk Team, Internal Audit Team and IT Team are working together for achieving compliance for the user group.” (CEO, Company G)

The participants worked closely with committees like Audit and Risk to ensure that the internal controls of IT/IS security policies and procedures were complied with as described in the following notes.

“Internal controls will provide reasonable assurance that the IT/IS security procedures are complied with, e.g., regular audit by internal auditors”. (CIO, Company H),

“(because) internal controls, we would have preventive and detective controls and our audit department regularly review whether internal controls are in place, whether there is any breach of the IT policy procedures security, whether any breaches in terms of the IT, and always check and balances”. (Chief Financial Planner, Company F),

“a key control checklist is developed and it sets out the various key controls and process requirements across all functions in the organisation and this includes any internal controls related to any IT/IS security matters. The key control checklist is reported regularly to the Audit Committee who assists the Board of Directors in reviewing the effectiveness of internal controls”. (CEO, Company A).

“At the Board of Directors level, we have Risk Committee and Audit Committee to ensure policies and internal controls are in place. (CEO, Company G)

The lack of the internal controls applications over IT/IS security might devastate the company's reputation according to the CEO of Company F:

“Safeguarding sensitive information is our risk management plan to ensure our IT/IS information such as Balance Sheet, Accounting and Reporting System, MIS, Accountable Budget, other Accounts, Future Profit of Company and Forecasting Information of Market Share Price are not stolen by hackers and disgruntled employees. That is why password protection is part of our internal controls. If this is not addressed, our sensitive information might be published by irresponsible people and ultimately damaging our corporation's name due to weak security systems.”

The successful implementation aspect of internal controls over IT/IS security policy is shaped by people's behaviour as shown by the following comments by the CEO of Company G:

“The role modelling of desired mind-sets and behaviour are important aspects to achieve internal controls in the implementation of IT/IS security policies and procedures”.

3) Security issues and risk management

Security issues were seen as important as other business risks by participants. Security risk, like all other business risks, needs to be managed and mitigated in efficient and effective ways. The

business risks are the responsibilities of the board and senior management. In many cases, security issues are part of the risk management plan as described in the following comments made by CEOs and CIOs.

“Like many other matters, IT related matters are also constantly reviewed as part of the organisation’s Enterprise Risk Management programme. This includes the system recovery issues, information security issues and others. Through this process, issues related to security of IT would be reviewed and included in the business risk management plan. Subsequently, the Risk Management Team will coordinate the development of risk mitigation action plans, develop and update business continuity plans for key business risks, plan and coordinate the testing of business continuity plans, organise training and education for employees on risk management and monitor the results of key performance indicators.”
(CEO, Company A)

“IT/IS issues are part of corporation risk management plan. I need to ensure effective risk management process and System Development Lifecycle are in place of identifying, evaluating and mitigating critical IT risks covering both software and hardware aspects so as to maintain database confidentiality and system integrity”. (CEO, Company G)

“IT/IS is issue is part of risk management plan and incorporated in our risk profile, regularly we update our profile. In this risk profile actually we define the state of IT/IS security issues and we find out what would be the actions taken”. (CEO, Company F)

“These IT/IS security issues, if any, are highlighted by the risk owners within the respective departments, are referred to the Risk Management Unit meeting or Risk Management Committee meeting for discussions and solution. They will be recorded in the risk registers if deemed necessary”. (CIO, Company H)

“Ok we have a Risk Profile for Company D. When talking about IT security, in coming up with the Risk management Plan or risk profile, we need to record everything, including IT and other security issues”. (CIO, Company D)

“IT/IS security issues are part of Risk Management Plan. We have a security unit. We set up a governance unit, before this governance is part of planning”. (CIO, Company C)

4) Security issues, organisational structure and risk management

The identification of security issues was a part of the risk management process. Different corporations have different organisational structures for identifying and managing their security risks as described in the following.

“These security issues are identified mainly by the IT staff with assistance from Business Security staff in Company A Malaysia. They ensured that the decisions were appropriate to the business risks, measured against industry best practices and sat within Company A Malaysia’s existing governance and policy structures wherever possible”. (CEO, Company A)

Security issues can be identified at any committee as described below.

“We do have IT steering committee. We have four committees that look overall issues- Divisional Management Committee (overall issues), Division Planning Committee (specific issues), Operation Technical Committee (OTC) (operation issues) and Divisional Risk Committee. So if we have IT or security issues, we discuss with Division Planning Committee. The security issues are identified through the Divisional Officer during the Council Meeting, at the forum and through committee.” (CIO, Company C)

In the case of Company D, the decision process on security issues is partly shared with its parent company structure called “Corporate IT Development Unit”.

“In directly since the policy and procedures was crafted at Corporate IT Development Unit level so in a way we have to be liaising a lot with Corporate IT Development Unit, getting some directions, some inputs, some recommendation, of course we make some decisions as well, of course when come to certain issues, if we think it warrant to be brought up to Corporate IT Development Unit we will, same goes to any security issues, we think if we can manage at our own level with I-Pgroup, we will do that”. (CIO, Company D)

As IT/IS security governance is the responsibility of the Board of directors and senior management, the security issues brought up to the senior management level can be seen in the following comments by the CEO of Company A.

“These issues are identified through the organisation’s Enterprise Risk Management process whereby the Risk Management Team headed by the Finance Director and comprising senior managers from all departments in the organisation including IT, will conduct quarterly reviews of the business risks as part of their responsibilities”.(CEO, Company A)

The interviewees revealed that security issues involve human aspects, technical, lack of policy implementation and natural disasters. The following evidence of security issues was found. The CEO of Company H said:

“Security issues include virus attack, hacking, sabotage, poor access control, lack of proper backup facilities, inadequate or outdated hardware or software and natural disasters.”

In the case of Company B, virus is also part of security issues. While network management was considered as a major security issue by Company C.

In some cases, participants reported that security issues were part of the IT/IS budget. This may indicate that some of the Boards of directors and senior management really are involved in the implementation of IT/IS security governance. As the CIO of Company H reports:

“Mainly security issues included within the budget include IT training, routine expenses to maintain IT security like anti- virus, anti-spam control, firewall and updates”.

The CIO of Company E commented:

“Security issues included within the budget-unauthorised access, disclosure, modification, destruction and theft”.

And the CIO of Company D:

“..internet and antivirus are also part of the security issues included in the budget, we do have agreement with the service provider, every now and then antivirus is updated and distributed across. And this is being budgeted on yearly basis.”

5) IT/IS Security Policy, educational aspects and informal aspects

Like any other policy, the educational aspect was an important formal component to support the implementation of IT/IS security policy and to strengthen the value of informal aspects. The following presents the indicators of the formal component which are educational aspects, used by participants. For example, training was perceived as a crucial aspect for the implementation of IT/IS security in intensifying informal aspects. Evidence was found in the comments of two CEOs. The CEO of Company H said:

“Training is the most significant aspects but other informal factors such as culture, commitments, education, security awareness.. are also important”. (CEO, Company H)

Another CEO commented: *“I think very classic informal factors would be educational part, the training part”*

The orientation program was part of the IT/IS security policy:

“The orientation program is stated in the IT security policy.” (CIO, Company B)

A standard code of practice was used to reinforce informal aspects in supporting the implementation of the IT/IS security policy. A CIO stated:

“We have Code of practice to implement informal aspects. Employees need to follow code of practice to ensure employees aware with ICT security policy in this corporation. Code of practice provides the details on what to do when the lines come out”. (CIO, Company C)

In another case, the ICT baseline was identified as guidelines to toughen informal aspects:

“in short we have ICT baseline for informal aspects which cover the good ethics and educate the staff”. (CIO, Company D)

7.2.1.1 Summary

Five issues discussed were ‘policy relating IS/IT security’, ‘policy, IS/IT security and internal controls’, ‘security issues and risk management’, ‘security issues, organisational structure and risk management’ and ‘IS/IT security policy, educational aspects and informal aspects’.

With regard to ‘IS/IT security policy’, six companies had policies in place, covering various domains and areas over the protection of IS/IT technological resources. The policy areas were not only covering internal IT systems, but also extensions to internet accessibility from outside organisations, to wireless and to mobile applications. The senior management, IT department and related committees were involved in the formulation of IS/IT security policies.

In reference to 'policy, IS/IT security and internal controls', IS/IT security areas were included within corporation's internal controls. In this study, there are two types of internal controls, namely, automatic IS/IT security internal controls and non-automatic IS/IT security internal controls. Most of comments had presented the non-automatic IS/IT security internal controls. The risk committee and audit committee played a significant role in detecting and monitoring internal controls applications. The success of internal controls was influenced by informal aspects, employees values and organisational values.

In the area of 'security issues and risk management', the majority of participants claimed that the IS/IT security issues were included in the risk management plan. A number of structures/platforms in place was used to identify security issues at ground levels. These were 'system development lifecycle', 'risk register', 'risk profile' and 'security governance unit'.

While in the area of 'security issues, organisational structure and risk management', the security issues in one organisation were unique depending on the IT vision. In summary, security issues can be identified at different levels, IT and business staff, IT committee, IT department and risk management team. The security issues included in the IT budget were the maintenance of security counter-measures/controls, software service provider fees and IT training. The security countermeasures and controls comprised anti-virus, internet, anti-spam, firewall and up-dates. And the examples of security risks were unauthorised access disclosure, modification, destruction and theft.

In regard to 'IT/IS Security Policy, educational aspects and informal aspects', the educational aspect was an important element of the formal component in this thesis. The software analysis revealed that educational aspects comprised training, orientation, code of practice and ICT baseline. The educational aspect had a significant role in the development of the informal component, employee values and organisational values.

7.2.2 Results (Concepts, Themes, Co-Occurrence) and Research Question 2

RQ2: How can directing and monitoring actions in the technical, formal and informal dimensions of IT/IS security governance in corporations be implemented efficiently and effectively?

The goal of Research Question 2 was to examine the processes involved in the directing (implementation) and monitoring actions within the three dimensions of formal, technical and informal discussed in Chapters 3 and 4.

The interviewees' comments, within the *concepts* and themes of the concept map, indicate how they implement and monitor the IT/IS security policies. The findings are framed according to the three dimensions of formal, technical and informal. The security process involved two actions, directing and monitoring actions and these two actions will be analysed and reported within the formal, technical and informal dimensions.

7.2.2.1 Formal Dimension

The boards and senior management of participating companies had IT/IS security policies in place as an organisational aspect that was identified for the formal dimension. This policy governed the processes of directing and monitoring actions in IT/IS security governance. The ways in which the boards and senior management of the corporation implement and monitor the IT/IS security governance are diverse in accordance within their organisational structures. The educational aspect is part of the formal components and this aspect empowers knowledge of individuals and skills relating to organisational responsibility (organisational values) and increasing the level of human integrity, honesty and trust relating to individual responsibility (employee values).

a) IT/IS security policies

i) Implementation and monitoring actions

The CEO of Company A noted that the board of directors, senior management and management levels are responsible for policy implementation over IT/IS security in place:

“In this case, where the policy on security of IT has been passed by the Board of Directors, the CEO together with the Senior Management is responsible to ensure the implementation of the policy in the organisation”. (CEO, Company A)

In achieving security governance in IT/IS security, a Business Development Services Director (BDSD) from the senior management group worked closely with the IT Department to ensure business requirements and security were aligned with business goals.

“The Business Development Services Director heads the IT department as a member of the Senior Management in the corporation. The Senior Management is responsible to ensure the implementation of the policies and decisions of the Board of Directors, to oversee the operations as well as to develop, coordinate and implement business and corporate strategies”. (BDSD, Company H)

Monitoring of the policy implementation was done by senior management as described by the CEO of Company A.

“The Senior Management has regular up-dates through meetings on all activities from respective departments within the organisation and this enables the Senior Management to review, identify, discuss and resolve strategic, operational, financial and key management issues”.

Delegating the IT/IS security policy across all staff levels is part of the IT/IS security governance process as shown by the comments of the CIO of Company B:

“At implementation of security policies we roll out the policy to all staff. Policy is incorporated into our procedures. In what we do policy comes first, procedures follow and the things that must be done are done”. (CIO, Company B)

In another case, a CIO who is senior management representative at Company H had responsibility in the implementation and monitoring part of their IT/IS security policy. As for implementation, the CIO delegated the security policies to all levels of staff at Company H.

“CIO will plan, execute and monitor the implementation of IT/IS security policies and procedures. For the implementation, the IT/IS Security Policies are communicated to all levels of the staff in the company”. (CIO, Company H)

Monitoring at Company H was done by its internal auditors and external entities: its external auditors and the Central Bank of Malaysia (the regulator of Malaysian Financial/Insurance Act).

“Our Internal Auditors will audit the IT/IS Security Policies from time to time to ensure compliance and its adequacy. The same goes with our external auditors and also a Central Bank of Malaysia. If the policies and procedures are not followed by the employees, this will lead to disciplinary actions against the employees concerned for misconducts. The matter will be resolved at departmental/HR department level”. (CIO, Company H)

The implementation and monitoring processes of the IT/IS security policy in password control is illustrated in the following example:

“..why this guy when he left the company, he will still have the password, the department themselves all looking after plus so called the internal audit will check whether if let say a person has resigned or has moved on to another department. From human resource, make sure the password always aware and change”.(CEO, Company F)

b) Role of IT Committee and IT/IS security policy implementation

i) Implementation and Monitoring Actions

The IT committee was seen by some participants to be an ad hoc structure and thus not involved directly in the IT/IS security policy implementation. The implementation of IT/IS security policy was done by the IT department. Some corporations use different terms to represent the IT Committee.

The IT committee was only involved in planning and set up, while monitoring was done by its internal audit department according to the CEO of Company F.

“The Task Force is active in planning and setup. Once they set up the thing, the IT committee or Task Force will not doing the security policies, the implementation will be the IT Department and monitored by the internal audit department. After that IT Department and internal audit implement security policies, monitor and recommend for change in ongoing process”. (CEO, Company F)

“We have an IT steering committee to oversee IT applications development. The function of the IT steering committee is to develop solutions which are consistent with outsource risk. The IT steering committee is not responsible for the implementation of policy relating to IT security”. (CEO, Company G).

“We do have an IT committee, formed ad hoc basis based on IT projects when necessary”. (CEO, Company H)

The following comments show that participants did not require the IT Committee for the implementation of IT/IS security policy and its processes.

“We don’t need IT committee to implement IT/IS security. We have our own IT Department to formulate the IT security policy”. (CIO, Company B)

“Company A Malaysia does not have an IT committee. In this organisation, there is an IT department and the department responsible for the day to day management of the IT system and processes in the organisation”. (CEO, Company A)

However, in some cases, the IT Committee was seen to be important for the implementation of IT/IS security policy.

“IT Committee is important for the implementation of security policies and procedures. First, the IT committee sets the direction. Second, we have to ensure that it complies with the Central Bank of Malaysia’s guidelines”. (CIO, Company E)

“.. the existence of those councils/committees are influenced to the implementation of IT/IS security policy. We use active approach to secure our IT architecture”. (CIO, Company C),

“Any weaknesses identified will be table to the IT/IS steering committee and the Audit Committee (Board of Directors Level) and mitigating actions will be taken”. (CIO, Company E) and;

“ISMC has influenced the implementation of policy relating to IT security. In fact any projects with regards to IT security, let say at Corporate IT Development Unit centre which embark on a new IT security initiatives, we will ask I-Pgroup to present at Company D level ISMC”. (CIO, Company D)
(Note: The above comments used many terms in Company D; ISMC represents for IT Committee; Corporate IT Development Unit represents for its parent company; I-Pgroup means IT services was outsourced to this group.)

c) Training, other educational aspects and IT/IS security policy

i) Implementation and monitoring actions

A raft of comments supported notions associated with training and other educational aspects, which empower the informal values within the implementation over two areas, policy and technical procedures. Training was frequently mentioned by participants. Their comments about the importance of training and other educational aspects follow.

The CIO of Company H reported that the IT Department and Human Resources Department were responsible for organising training for staff:

“To implement the policies about informal aspects to IT/IS security, Human Resource and IT departments will jointly identify the needs for trainings for the respective users and arrange for it”. (CIO, Company H)

The Human Resource department was involved in providing training and briefing policies relating to IT:

“Normally new employees have to attend 2 hours training session regarding IT things, normally the Human Resource will brief on the IT/IS security policies”. (CIO, Company B)

Training and other educational aspects strengthen the informal aspects and this would lead to effective implementation of policies and technical controls.

“Informal factors are very important to support the implementation of IT security policy and controls. Successful IT security policy and controls is not just the deployment of technology (firewalls and intrusion detection systems) but is a series of essential practices that is embedded into the culture of Company A Malaysia through training, education, awareness and others. Once the IT security policy and controls are created, communicated and adopted, only then IT facilities can be effective to support and enable business requirements in a secure manner”. (CEO, Company A)

The board and senior management are responsible for cultivating IT/IS security awareness in the culture of corporations through training and other educational approaches.

“We all in management as a CEO would be responsible to make sure people are aware, we must provide training, we must update ourselves, we must send people for awareness courses or we provide information like through mail or whatever so that you can up-date yourself. Like Financial Reporting Standard (FRS), the comments by auditors, of course to make sure we are, the culture we want to cultivate is aware especially new staff. (CEO, Company F)

The orientation program was an example of educational aspects to reinforce informal aspects for new employees, where IT/IS security policies are normally briefed to create awareness on the importance of IT/IS security. This notion is described in the following comments.

“For informal aspects, normally new employees have to attend orientation program. In the orientation program, the employees are being informed about the corporate policies including IT security policies”. (CIO, Company B)

Another interesting example of educational aspects was found using an on -line system. E-learning was conducted to increase informal values among employees in regard to IS/IT security:

“..e-learning training is compulsory, but it does not subject to any particular topic, that basically to inculcate people to browse e-learning to find all the modules that we can learn but there is a topic on ICT security that they can cover. We don’t simply say we should take security course but there is a specific course in our e-learning and staff is encourage to explore themselves”. (CIO, Company D).

Lack of training and other educational aspects could lead to security incidents and ultimately to loss of business reputation.

“Training is an important aspect to reduce security incidents. And security incidents could lead to bad reputation of corporation”. (CIO, Company B)

Lack of awareness is also associated with accountability issues within IT/IS security governance.

“If the employees lack training and awareness, they are not accountable. This may lead to unmoral behaviour such as cheating and abusing of information. If the employees are not trained, they are not aware and also not compliance with IT policies and procedures.” (CEO, Company F)

“Internal employees are threat to this organization if they are lack of education, training and awareness. For example, user-name gets shared among employees. Clearly the accountability is

immediately lost. Lack of awareness, educate, once you educate but people still do it, that's means accountability issue". (CEO, Company G)

7.2.2.1.1 Summary

IS/IT security policy involved several ways of 'directing actions' implemented across the management levels between the giver(supervisor) of the responsibility and the holder of responsibility. At the strategic level, the senior manager (supervisor of responsibility) had responsibility to acquire information in terms of business needs and security requirements from the IT Department/other departments (holder of responsibility) in order to align with business goals. At the operational level, the CIO (giver of responsibility) rolls out and communicates the policy to all staff (holder of responsibility). In terms of the 'monitoring actions', the organisation had relied on the audit results by internal auditors rather than emphasising the role of supervision between higher level (supervisor of responsibility) and lower level (holder of responsibility). The organisation depends on the human resources department to detect and set/reset the status of individuals according to designation, access and authorisation rights and the validity.

The second area was related to 'role of IT Committee and IT/IS security policy implementation'. The IT committee in one organisation had a unique role depending on its IT vision. Briefly, the roles of IT committee within the comments had three different views. First was the IT committee played an ad#hoc structure during planning and set-up and was not responsible for the security policy implementation. Second was the IT committee was significantly important before or during the security policy implementation. And third, the IT department had a major role to draft, upgrade security policies and strategies, check the progress of IS/IT security processes but the IT committee was not needed by a few organisations.

The next area was concerned with 'training, other educational aspects and IT/IS security policy'. Training was the most popular strategy used by organisations to attain educational aspects. The IT department and human resource department had significant roles in providing training and explaining about security policies. Training and other educational strategies including awareness courses, orientation programme, e-learning may strengthen the informal component, to lead to a better result of policy and security counter measures/controls implementation.

7.2.2.2 Technical Dimension

a) Technical and IT/IS security policy

i) Monitoring Actions

Technical implementation is strongly derived from IT/IS security policy. The boards and senior management of participating corporations did show how they monitor and review the progress of technical implementation in achieving IT/IS security policy at different levels of management.

Documentation reports from the IT Department and IT Committee were used by the CEO of Company H for monitoring.

“We monitor the progress of technical implementation based on the reports from IT department and IT committee”. (CEO, Company H)

At the senior management level of Company H, the CIO used operational reports to monitor the achievement of policy and procedures:

“To monitor the involvement of technical role, we are based on the result of operational reports. Successful implementation of policy and procedure or financial result are indicators of successful implementation”. (CIO, Company H)

Every case is different in the monitoring technical implementations.

“For the monitoring part of technical implementation, in any case, we do follow a proper project implementation methodology where a Project Plan will be developed and there will be ongoing tracking and monitoring. Prior to the implementation stage, the project’s objective would have been defined and the IT/IS Committee would have to approved it”. (CIO, Company E)

The CIO of Company C monitored the technical implementation through unit and proper organisational structure.

“We monitor the technical implementation through unit, we have reference structure, ..we just see and monitor and get the report, for example Electronic Resource Planning (ERP) operation, ERP has their own security systems, before business division did their own, since the system requires updates, they just pass up to us and we do the monitor part”. (CIO, Company C)

At Company D monitoring the technical implementation is done by its technical group through technical meetings.

“During the ISMC meeting we do have a technical discussion with I-Pgroup,.. as far as my position is concerned, I am not holding a technical position, basically my role is not supposed to be very technical because we have I-Pgroup”. (CIO, Company D)

In Company F technical implementation was monitored by the IT committee during the preparatory part of system implementation.

“During the planning and setup, the technical implementation is monitored by the Task Force then it is reported to the management, once the system is stable, then we go alive, we drop the manuals, whatever things that unnecessary or duplication whatever, then we go alive on IT/IS network”. (CEO, Company F)

b) Technical roles (in sharing issue)

In many cases, participants did not have issues in sharing technical roles with other staff groups. For example, the CEO of Company F said:

“ .no problem in sharing technical roles among other employees, I think the technical here referring here to only the IT. Because the IT people they themselves are aware of the requirements. So you talk about business goals and security controls, and referring to corporation, so if they understand what is the goal, get them involved in preparing our policies, then it should not be a problem”. (CEO, Company F)

The following shows the remaining comments in regards to the technical roles issue.

“We don’t have difficulty in sharing roles with other senior managers from other departments. Each department has their own roles-technical and human resources”. (CIO, Company C)

“No. We don’t have a difficulty in sharing technical roles”.(CIO, Company H) “We don’t have a difficulty in sharing technical roles among other employees”.(CEO Company H)

“No. I don’t have difficulty in sharing technical roles”.(CEO, Company G)

7.2.2.2.1 Summary

The technical dimension was concerned with two areas, first was ‘technical and IT/IS security policy’ and second was ‘technical roles in sharing issue’.

In the area of ‘technical and IS/IT security policy’, the technical implementation including security procedures was the result of IS/IT security policy. The monitoring actions over the technical implementation had covered structures (entities), method of monitoring and artefacts. The entities involved in the monitoring activities were IT department, IT committee, business division and technical group (third party service). Project implementation methodology was a method used to monitor the progress of implementation of IT projects. While monitoring artefacts comprised operational reports from departments/committees, financial results reports and Electronic Resource Planning operation reports.

The second area, ‘sharing technical roles’ had referred to the integration of different discipline/experts in resolving security problems from different units/departments. Some participants claimed that they had no issues/no difficulties in sharing the technical roles with others because each department had its own vision and goal.

7.2.2.3 Informal Dimension

a) culture and integrity of people

i) Implementation action

Norms and cultures that exist may influence security practices within an organisation. Good corporate governance would lead to good practices and bad corporate governance would lead to bad practices, depending on the supervisor of responsibility and the holder of responsibility. For example, communication to all staff levels was an important part of the informal aspect in achieving IT/IS security policies and procedures. A senior manager at Company E highlighted that:

“Informal aspects that incorporated in the implementation of policies and procedures relating to IT security are communication to all levels of the company..” (CIO, Company E)

Security culture can be cultivated if the supervisor of responsibility and the holder of responsibility follow the policies effectively. For example, password management is part of IT/IS security policy, if practised effectively, the security culture would improve and develop.

“password management, which is a policy now, to become policy you have to create the passwords with 6 characters, but something like, the good practices of you, don’t simply put your password on the table, sometimes people tend to put password and stick on the wall, right.” (CIO, Company D)

Integrity and being professional were concerned with employees values of informal aspects.

“..in terms of integrity, informal, we adopt how to be professional, if you are professional then the rest will take care, you are professional accountant, professional lawyer, professional IT, you will comply because you are or you want to be a professional.”(CEO, Company F)

The board of directors and senior management worked closely with the Human Resources Department in implementing informal aspects across departments for achieving the policy relating to IT/IS security.

“CEO is responsible to ensure basically, every operation in the company runs smoothly. CEO will delegate the authority to various departments concerned for instance Human Resource department to execute and report to CEO on managing the informal factors”. (CEO, Company H)

ii) Monitoring action

Some comments supported notions associated with the monitoring of the informal dimension.

The weekly statistics report at operational level (by IT group) was used as a tool for monitoring security matters.

“In fact, during the weekly meeting, from time to time, we do request I-Pgroup to provide some statistics with regards to ICT security issues. From there we could gather information and monitor. And later decide on the best moving forward action”. (CIO, Company D)

Monitoring activities on IT/IS security matters were also conducted during the quarterly meeting with the IT committee, board of directors and senior management.

“we see how many issues discussed pertaining to ICT security, the same time during the quarterly ISMC, we will see whether if the issues on service level or incidents in regards to security, if lower, we are doing a good job”. (CIO, Company D)

Commitment and managerial reports at various management levels of the corporation were part of IT/IS security governance in the monitoring action.

“We monitor the goals of policy relating to informal aspects based on the reports from Human Resource department, IT department and IT committee”. (CEO, Company H).

At the senior management level of Company H, monitoring involved documentation, reporting and observation of people’s behaviour and commitment.

“The monitoring of informal aspects is based on the observance of the respective Head of Departments on their staff behaviour and commitment. The respective Heads will produce exception reports on those staff whose behaviour and commitment are in doubt”. (CIO, Company H)

Indices were used to monitor the implementation of informal aspects.

“To monitor the implementation of informal aspects, we use KRAs and KPIs. KRAs and KPIs will be set and Action Required (AR) will be assigned. Daily or weekly or monthly or quarterly reviews or meeting with relevant managers or departments”. (CIO, Company E)

However in one case, informal aspects were very subjective and were not subject to monitoring activities.

“Monitoring informal aspects is very subjective area. We don’t monitor the goal of policy, we only monitor whether we have complied, we don’t monitor whether the security has breached or not be breached, we don’t monitor whether the goal of policy, informal part, very difficult to monitor the results affected by informal aspects”. (CEO, Company F)

7.2.2.3.1 Summary

The Informal component referred to culture, norms and beliefs including employee values and organisational values. The interview data highlighted the culture and employee values. Culture is cultivated through reinforcement. The two examples of culture were ‘communication to all levels of employees’ and ‘do not put your password on table, stick on the wall’. The culture can be cultivated if the characteristics of individuals had been empowered. The highlighted characteristics were integrity and professionalism.

The monitoring action of the informal component contained three elements which were entities (structure), monitoring activities and artefacts. The entities involved in the monitoring action were identified, these include IT department, technical group, board of directors and senior management, human resource department, IT committee and heads of departments. Monitoring activities related to observation of people is behaviour and commitment and conduct meeting. And artefacts of the monitoring action highlighted were weekly statistic reports, reports from department/committee, KRAs, KRIs, daily or weekly or monthly or quarterly review

Chapter 8 Data Analysis: Manual Content Analysis of Interview Data

8.1 Introduction

Some concerns about the data/processes of Leximancer analysis in Chapter 7 were raised during a supervision meeting, the recommendation was made to support the software analysis of the interviews by carrying out an analysis manually. The way to determine the themes and issues in the software analysis was different to the manual analysis. As can be seen in Chapter 7, themes were determined by frequency of occurrence, while in the manual analysis themes are derived from the literature. Interestingly, it is believed that this dual analysis does not only strengthen the understanding of the interview data but also provides support for the themes used in the literature.

Interviews were undertaken with eight Malaysian Publicly Listed Companies to identify the issues that relate to IS/IT Security Governance in Malaysia.

The discussion in this chapter is divided into three parts: Part 1, discusses the data source (8.2) and the development of results (8.3); Part 2 reports on data analysis (8.4); and Part 3 relates the data to the IS/IT Security Governance Model (8.5). The reporting analysis in Part 2 was based on input from Part 1 and Part 3 was based on input reported in Part 2. It is important to note, Part 2 and Part 3 are inter-related, where Part 3 is dependent on Part 2.

In Part 2, interview data were analysed manually where the richer and higher quality data are important for achieving the IS/IT Security Governance Model. The data analysis in this chapter is primarily based on the IS/IT Security Governance Model developed in Chapter 4. A number of themes related to IS/IT Security Governance Model were explored. The themes identified in the IS/IT Security Governance Model are linked to the issues noted by interviewees to build a rich picture of IS/IT security governance. Part 2 also discusses the role of the board and senior management in directing and monitoring the IS/IT security actions and controls from the Formal, Technical and Informal components and the interactions. Quotations were selected to provide the evidence relating to the directing and monitoring activities of the three components and the interactions.

Basically, the selection of quotations in Part 2 was made according to the nature of research questions. Across -case analysis was used to answer Research Question 1 and single-case analysis was used to answer research question 2.

Later, in Part 3, the quotations (or interview data statements that) reported in Part 2 are re-selected by matching the data and with the elements developed in the IS/IT security governance model (Chapter 4). The goal of Part 3 is to see how much data supports the model.

Across -case and single -case are both discussed in Parts 2 and 3.

Part 1

8.2 Data Source: background of interview participants

Twelve interviews from eight companies of Malaysian Publicly Listed Companies were conducted during the data collection stage in 2009; four CEOs who represent the board and management, five CIOs and two other senior managers who represent the senior management team and one junior manager who represents the operational level. The data shown in Table 8.1 are based on the interviews taken in 2009. Using the sample design developed in Chapter 5, there were three groups based on the market capitalisation rankings in 2008: Group A, Group B and Group C. From eight companies, three companies came from Group A and another five came from Group B, but none from Group C. The identities of all companies were removed and renamed with a new identifier.

The three companies which came from Group A were re-identified as Companies A, C and D, and the five from group B were re-identified as Companies B, E, F, G and H.

As for Group A, five participants were involved including one board of director/senior management-CEO, three senior managers with two CIOs and one Business Development Service Director and one junior manager. The CEO of Company A had 20 years experience in the field and 3 years experience as a CEO. All the senior managers of Group A had approximately 10-20 years experience in the field.

In Group B, seven participants were involved in the interview process, three CEOs represented the board/senior management group and senior managers represented by three CIOs and one Chief Financial Officer. The CEO of Company F had 13 years experience as a CEO, one of the most experienced CEOs in this study. The CEO of Company G had worked in the field for 4 years and only 2 years experience as a CEO. The CEO of Company H worked as a CEO for 7 years. While all senior managers in Group B had approximately 10 years experience in their field, except for CIO of Company H who had approximately 2 years experience.

Each company has a different background in industry. The data show that there were six industries: Financial and Insurance, Construction, Plantation, Communication Services, Manufacturing and Mining. The Financial and Insurance industry was represented by two companies from Group B: E and G. The Construction industry had two companies in Group B: B and H. In the Communication Services industry, one company was identified from Group A, C. In the other industries like Mining, one company was identified from Group A which is D. The Manufacturing industry was represented by one company from Group A, A. And one company from Group B, F, represented the Plantation industry.

Original Name (not revealed)	New Identifier	Group Type	Industry	Participant		
				Role	Length of service (approximate) (until 2009)	Duration of interview
Company 1	Company A	A	Manufacturing	CEO	20 years experience in the industry, 2 years experience as a CEO since 2007	Nil (Email interview)
				Business Development Service Director	18 years, worked since 1990	Nil (Email interview)
				Junior IT Manager	Approximate 5 years experience in field	Nil (Email interview)
Company 2	Company B	B	Construction	CIO	Approximate 10 years experience in field	Approximate 1.30 hours
Company 3	Company C	A	Communication Services	CIO	Approximate 10 years experience in field	Approximate 50 minutes
Company 4	Company D	A	Mining	CIO	Approximate 10 years experience in field	Approximate 2 hours
Company 5	Company E	B	Finance and Insurance	CIO	Approximate 10 years experience in field	Approximate 50 minutes
Company 6	Company F	B	Agriculture/Forestry/Fishing	CEO	13 years as a CEO, since 1997	Approximate 1.30 hours
				Chief Financial Officer	Approximate 10 years experience in field	Approximate 1.30 hours
Company 7	Company G	B	Finance and Insurance	CEO	2 year experience as a CEO, appointed 2008, worked since 2006	Approximate 1 hour
Company 8	Company H	B	Construction	CEO	7 years as a CEO, appointed 2003	Nil (Email interview)
				CIO	Approximate 2 years experience in field	Approximate 1 hour

Table 8.1 Data source and background of participants

Eight interviews were conducted face-to-face and four interviews were conducted through e-mail conversations. The face-to-face interviews took between 50 minutes and two hours. The interview transcripts can be seen in Appendix 8B.

8.3 The development of results

There were two major steps involved in the manual table analysis. First, the topics of the Table (top columns) were developed after adopting the themes identified in Chapter 4, the IS/IT Security Governance Model covering the Formal, Technical and Informal components themes and research questions. Second, the interview data were organised and analysed on a row basis; the data were analysed by matching the themes (Chapter 4), ticking the box and determining the research question type. The matrix box may have more than one tick, where a single issue may have more than one theme. The research questions are important for determining the technique of data analysis to be used. In analysing the interview data, two types of analysis technique were needed. The first technique was across-cases analysis and the second technique was single-case analysis. The selection of technique used was dependent on the Research Question.

The across-cases analysis will be used to answer Research Question 1 because the objective of Research Question 1 was to discover the evidence about the development of IS/IT security aspects with regard to the Formal, Technical and Informal components, if any.

Research Question 1: *In what way does the involvement of Boards and Senior Management impact on the implementation of IS/IT Security Governance in the Formal, Technical and Informal components?*

The single-case analysis was employed in order to achieve the objectives of Research Question 2, where the research study is analysing the interaction of components within a single case. The single-case technique is able to reveal the complexity of the component interactions.

Research Question 2: *How can directing and monitoring actions in the technical, formal and informal components of IT/IS security governance in corporations be implemented efficiently and effectively?*

Part 2

8.4 Data Analysis and Results

Interview data are analysed in this chapter, reflecting the model of IS/IT security governance developed in Chapter 4. In this chapter the themes identified in the model are linked to the issues noted by interviewees to build a rich picture of IT/IS security governance.

8.4.1 Themes

In developing the conceptual framework fourteen themes were identified, these are shown in Tables 8.2a and 8.2b. There are three dimensions to these themes- formal, technical and informal- which are then sub-divided to reflect each of the themes underlying IS/IT security governance. Tables

8.2a and 8.2b show that the issues identified from interviewees are divided into primary and secondary issues.

ISSUES			Model of IS/IT security governance – Themes							
			Formal Aspects (Organisational Aspects)							
Primary	Secondary	Source	Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
			Policy	Strategic vision & security importance	Security internal controls	Compliance /Legal Requirements/ Regulation	Organisa-tional Structure	Commit-tee	Security Risk & its Manage-ment	Education, training, seminar, orientation

Table 8.2a The relation between themes and issues

ISSUES								
			Technical Aspects IT/IS security			Informal Aspects		
Primary	Secondary	Source	Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
			Techni-ques & Controls	System Develop-ment	Internet/ Network Security	Staff integrity/ ethicality/ accountability	Culture, commit-ment	Human issues-lack of aware-ness, stupidity

Table 8.2b The relation between themes and issues

Each of the dimensions and themes underlying that dimension is now discussed.

8.4.1.1 Formal Dimension Themes

The formal dimension contains themes that are concerned with the development of formal governance structures of IT/IS security indicating the involvement of boards and senior management in governing IT/IS security. The formal themes identified from the literature review in Chapter 2 were “policy”, “strategic vision and security importance”, “security internal controls”, “compliance/legal/regulation requirements”, “organisational structure”, “committee”, “security risk management” and “education, training, seminar and orientation”.

The first formal theme “Policy” identifies whether corporations have IT/IS security policies in place and also identifies the policy development areas. IT/IS security policy is an important formal structure because its primary objective is to achieve business strategy and leads to the procedures to implement the IT/IS security.

The second formal theme “strategic vision and security importance” identifies the relationship between IT/IS security needs and business requirements in order to achieve strategic vision, in particular, to minimise operational business risk.

The third formal theme, “security internal controls”, relates to whether there were internal controls being applied within IT/IS security areas. Internal control is a mechanism used by organisations to measure the achievement over certain corporation policies or procedures implementation. This theme particularly identifies the internal controls application by corporations over IT/IS security policies and procedures.

The fourth formal theme “compliance/legal/regulation requirements” identifies if corporations need to comply with any external controls regarding to IT/IS security. This kind of requirement is important because it would influence how the boards and senior management make decisions in IT/IS security matters such as policies.

The fifth formal theme “organisational structure” reflects the responsibility of senior management in the implementation of IT/IS security. This theme also identifies the specific roles of senior managers in relation to technical implementation.

In the sixth formal theme ‘Committee’ identifies whether committees play a significant role in the IT/IS security implementation. Committees identified in this framework were the IT Committee, Risk Management Committee and Audit Committee.

The seventh formal theme “security risk and its management” identifies if IT/IS security was part of the risk management plan. This theme also looks into the development of risk assessment processes in order to minimise operational risk and to ensure that the strategic vision is accomplished effectively. The role of boards and senior management and examples of security issues are included.

The eighth formal theme, “education, training, seminar and orientation”, concerns building the knowledge and skills of employees. This theme identifies if corporations have integrated appropriate training into the IT/IS implementation or in the corporation’s policies. Building knowledge and skills in IT/IS security is important because education empowers human core values such as being honest and creates security awareness, apart from improving knowledge and skills.

8.4.1.2 Technical Dimension Themes

The technical dimension contains themes that reflect security controls development and implementation and the responsibility of boards and senior management. Boards and senior management are accountable for the success or failure of planning, development, implementation and maintenance of security controls. Three technical themes were identified, “techniques and controls”, “system development” and “internet or network security”.

The first technical theme “techniques and controls” identifies whether corporations have embraced security controls within the IT/IS system. Techniques and controls were designed to enforce certain security controls on particular domains/platforms in order to achieve security policies requirements.

The second technical theme “system development” identified whether corporations have incorporated the security elements in the development of IT/IS.

The third technical theme “internet or network” identifies the inclusion of security controls in the use of internet and network within corporations. The emergent technologies such as wireless and mobile internet have exposed corporations’ private networks to threats and vulnerabilities.

8.4.1.3 Informal Dimension Themes

The informal dimension reflects themes embracing human aspects in regard to levels of knowledge and skills, awareness, level of human integrity in IT/IS security implementation. Integrity refers to levels of honesty by staff. The informal dimension suggests that the boards and senior management have responsibility to integrate human aspects in respect to education, awareness and human integrity in the technical implementation of IT/IS security policies and procedures, because security issues/incidents are largely caused by human errors, lack of integrity and lack of awareness. Three themes were identified: “staff integrity/ethicality/accountability”, “culture/commitment” and “human issues-lack of awareness/stupidity”.

The first informal theme “staff integrity/ethicality/accountability” examines whether corporations have emphasised the role of human integrity, ethicality or accountability within IT/IS security implementation. These aspects are concerned with core values and characteristics of personnel and lack of them could bring about intended actions such as stealing information and destroying business information.

The second informal theme ‘culture/commitment’ identifies whether corporations have established a security culture within the organisation. Security culture reflects good practices of IT/IS security policies and procedures. For example, employees do not share passwords and user names with other employees in the access to IT/IS system in a corporation. In this regard, commitment of staff is needed to bring the success of policies and procedures and its practices into the culture.

The third informal theme “security awareness” examines whether corporations have put emphasis on this aspect. Security awareness reflects the extent to which security policy and procedures are read and understood by all employees. Employees may be likely to disregard and break the policy, procedures or outlines that are already in place due to lack of awareness.

8.4.2 Issues

In reviewing the responses, issues were identified relating to each of the themes. An issue is a matter raised by interviewees in real practice. The objective of the conceptual framework was to examine whether these themes are reflected in practice and underlie IT/IS security governance. Often a single issue may embrace all dimensions. Embracing more than one dimension depends on the nature of the issue. For example, the issue of protecting business information from security breaches may require a policy (formal), security controls/technologies and its procedures of implementation (technical) and may require cultural change within the organisation such as employee values and organisational values (informal). These issues are discussed below in the context of the theme(s) to which they have been related. Issues have been divided into primary and secondary issues. Primary

issues are the main topics that were raised by interviewees and these were then further divided by characteristics of the main issue which are called secondary. In the next sections issues identified are discussed in the context of the themes to which they relate.

8.4.2.1 Primary Issues and Secondary Issues

The primary issues identified from the interviews were categorised into six groupings: “business needs”, “policy development”, “implementation”, “monitoring”, “share role” and “security issues and budget”. Under each of these major issues a number of secondary issues was identified.

8.4.2.1.1 Primary Issue: Business Needs

A range of ‘business needs’ issues was identified. Business needs describe issues related to IT/IS security requirements within business operations. These ranged from the identification of strategy, to the safeguarding of assets, to risk, to compliance, to informal factors and to internal controls application. Ten secondary issues were identified from the data. It was found that these issues related to themes in each of the dimensions discussed in the conceptual framework. The number of responses in each category is shown in Tables 8.3a and 8.3b which show the responses of companies in the issues by dimensions.

ISSUES			Themes							
Primary	Secondary	Source	Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
			Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal Requirements/Regulation	Organisational Structure	Committee	Security Risk & its Management	Education, training, seminar, orientation
Business needs			15	16	15	6		29	42	24
	Protection/Safeguard	A D G, F	5	10					2	
	Risk	A, B, C, D, E, F, G, H		1				2	18	
	Business/strategic goals	A B C G	1		2				4	
	Compliance	E, F, G	2		2	3		1	1	1
	Internal controls procedures & processes	A B D E F G H		1	8				1	
	Policy & Informal factors	A, B, C, D, E, F, G, H	6			3				21
	Govern in IT	A C D F G	1	4	2				3	
	Responsibility of Senior Management	A, G, H			1				4	1
	Role of Committee	A B C, D, E, F, G, H,						21	9	
	Role of Department	A, B, D, F, H						5		1

Table 8.3a The primary issue of 'business needs' and its secondary issues

ISSUES								
Primary	Secondary	Source	Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
			Techniques' & Controls	System Development	Internet/ Network Security	Staff integrity/ ethicality/ accountability	Culture, commitment	Security awareness
Business needs			10		1	12	2	5
	Protection/ Safeguard	A D G, F	1					
	Risk	A, B, C, D, E, F, G, H						
	Business/ strategic goals	A B C G						
	Compliance	E, F, G				1		1
	Internal controls procedures & processes	A B D E F G H						
	Policy & Informal factors	A, B, C, D, E F G, H	9		1	11	2	4
	Govern in IT	A D F G						
	Responsibility of Senior Management	A, G, H						
	Role of Committee	A B C, D, E F, G, H						
	Role of Department	A, B, D F, H						

Table 8.3b The primary issue of 'business needs' and its secondary issues

8.4.2.1.1.1 Secondary Issues

The 10 secondary issues are now discussed with reference to Tables 8.3a and 8.3b.

1) Protection/Safeguarding of Information

Four companies recognised the importance of the protection/safeguarding of the assets of the corporation in the formal and technical dimensions. In the formal dimension, themes identified that related to this issue were: 1st formal theme 'policy'; 2nd formal theme 'strategic vision and security importance'; and 7th formal theme 'security risks and its management'. The technical theme that related to this issue was 1st technical theme 'techniques and controls'. The areas that embraced employees in the issue of protection/safeguarding of information include "integrity", "availability", "confidentiality", "protection of business information", "safeguard the systems" and "recovery". The following discussion of issues is presented according to related dimensions. (See Appendix 8A for details).

The protection of business information is perceived important at the board level due to corporations being dependent on IT/IS. In regards to the issue of protection/safeguarding of information, 5 responses were identified in the 1st formal theme 'policy', 10 responses identified in the 2nd formal theme 'strategic vision and security importance' and 2 responses identified in the 7th formal

theme ‘security risk and its management’ by interviewees. IT/IS security is important in order to achieve the maximum use of IT/IS for wealth benefits and cost cuts in business. As one CEO noted and identified in the 2nd and 7th issues of the formal dimension and 1st issue of the technical dimension:

“CEO F: Our corporation is highly dependent on IT and most of our systems are electronically digitally set up, I mean we have IT on our Finance Integration of Financial Statement Information Accounting, we have Integrated Financial System which is linked very closely with our Plantation Management System and also linked directly to our Human Resource Information Systems (HRIS). So among the three of these, software and the systems we have used for accounting systems will be used directly for reporting in our corporation. We have Management Information Systems (MIS), reporting on critical issues and using all this stuff, so security of IT/IS it is very important to us”.

Interviewees emphasised that confidentiality was an important area of IT/IS security processes in business operations. Protecting confidential information of business was one of the core components of security aspects. If the confidential information is compromised, the business operation will be interrupted and cause losses to corporations. The following quotations are examples of responses made by two CEOs as identified in the technical and formal dimensions:

“CEO F: Data that are transmitted to and from these systems – Human Resource Information Systems (HRIS), Accounting, Plantation includes mail, engineering and all these are highly confidential” and “CEO H: Protecting confidential information is a business requirement”

Apart from confidentiality and integrity, availability is another important component of IT/IS security. Availability is a process of ensuring information is available to authorised persons when required. One example can be seen in the following response by a CEO:

“CEO F: it is very important for us to make sure that people with relevant authorities are allowed to see and access information and also to input the right source documents.”

Achieving all three IS/IT security elements, confidentiality, integrity and availability, is an important process of IT/IS security governance. If one of these three security elements was compromised, it would risk business information and ultimately business reputation. Two CEOs have addressed these three elements of IS/IT security in their responses. For example one CEO pointed out:

“CEO A: Like any other business organisation, Information Technology (IT) facilities are important to Company A Malaysia. Company A Malaysia is dependent upon the continued availability, integrity and confidentiality of the services provided by its IT facilities for the successful operations of its business and the protection of its business information. Hence it is important for the IT facilities to be secured for these purposes”.

There was one response identified in the 1st technical theme ‘techniques and controls’ in respect to the issue of protection/safeguarding information. Security control was identified as an important technique to achieve IT/IS security. Business information should not be altered or modified by irresponsible people. For example, one response by

“CEO F: We take great care to safeguard our system adopting firewalls and security systems like “Tom Access” where at certain levels we use passwords to enter the systems.”

2) Risk

Risk is perceived to be an important secondary issue of 'business needs' by all corporations, as identified in the 2nd, 6th and 7th formal dimension themes. In respect to risk, one response was identified in the 2nd formal theme 'strategic vision and security importance', 2 responses in the 6th formal theme 'committee' and 18 responses were identified in the 7th formal theme 'security risk and its management'. Risk strategy is needed to minimise the risks caused by the use of IT/IS. It was recognised within responses that the areas include "risk managing", "risk management", "risk profile", "risk-business plan", "risk register" and "IT/IS security risks".(See Appendix 8A).

There were many responses regarding the importance of risk management in IT/IS security risk by all companies, as identified mostly in the seventh formal theme. Three CEOs and three CIOs had reported IT/IS security risks were part of their business risks management plan. As with other risks, security risks issues need to be identified and mitigated effectively and efficiently to increase shareholder value and profits. As one CEO noted in the following response identified in the 2nd formal theme and 7th formal theme:

"CEO A: Company A Malaysia believes that effective management of risks associated with all aspects of the organisation's business is critical for sustained growth and continued enhancement of shareholder value. Like many other matters, IT related matters are also constantly reviewed as part of the organisation's Enterprise Risk Management programme."

Like other business risks, IT/IS risks were the responsibility of the Risk Management Committee. The role of the committee is to manage the risks according to the risk level decisions set out by the board, as noted by one CIO and identified in the 6th and 7th formal themes,

"CIO E: It is part of our annual Enterprise Risk Management and Departmental workshop where we identify all types of risks including IT/IS security risks, and if it is classified as an extreme risk or if the Risk Management Working Committee decides that the risk has to be look into, mitigating actions will be put into place and will be monitored".

The Chief Information Officer of Company B, reported that managing IT/IS security risk was part of standard activity to be worked out in the corporation. In fact, this company had a specific committee in place to deal with IT/IS risks,

"The committee looks after the business, I am a member of the Risk Management Committee. And we have an IT Risk Management Committee."

IT/IS security risks were seen to be important by all interviewees. Security issues related to confidentiality, integrity and availability were risks to business. In particular, the board and senior management had responsibility and accountability for risks due to confidentiality, integrity and availability issues. As indicated by a CEO and identified in the 7th formal theme:

"CEO H: CEO is ultimately responsible and accountable for all operations of the company that include to ensure that an effective and efficient framework is in place to manage the IT/IS security risk. IT/IS security issues do form a part of the company's business Company H plan. Security issues include virus attack, hacking, sabotage, poor access control, lack of proper backup facilities, inadequate or out-dated

hardware or software, natural disasters and etc. Security issues are included in the risk register of the company”.

Other issues identified were,

“CEO A: the system recovery issues, information security issues and others”.

There were 3 responses in respect of the established IT/IS security risk profile. The existence of this profile has indicated the active involvement of the senior management in IT/IS security. As noted by one Chief Information Officer:

“CIO D: Ok, we have a Risk Profile for Company D. When talking about IT security, in coming up with the Risk Management Plan or risk profile, we need to record everything, including IT and other security issues”.

Similarly, a Chief Financial Planning Officer claimed that

“CFP F: IT/IS issue is part of risk management plan and incorporated in our risk profile, regularly we update our profile”.

Nevertheless, some interviewees had addressed the contingency plans with regard to security disasters. The action plans relating to security threats were needed as part of the business continuity plan as the following response suggests:

“CEO F: We have Risk Management in place to back up our system to store our data at one local Bank Centre. The online process will be switched off to Manual process. Normally it takes a short period of time.”

3) Business/Strategic Goals

Four corporations believed that the implementation of IT/IS security was driven by business/strategic goals as identified mainly in the formal dimension themes. Formal dimension themes that related to this issue were 1st formal theme ‘policy’, 3rd formal theme ‘security internal controls’ and 7th formal theme ‘security risk and its management’. The areas identified from interviewees were “requires governance focus”, “sustain growth and shareholder value”, “competitive edge over competitors”, “creates values to customers”, “balance between profits and risks” and “corporation reputation”.

There was one response identified in the 1st formal theme ‘policy’, 2 responses in the 3rd formal theme ‘security internal controls’ and 4 responses identified in the 7th formal theme ‘security risk and its management’. Although IT/IS have been used for generating profits and revenues or minimising costs, effective and efficient security governance over IT/IS is also a critical success factor for business. The trade-off between risks and profits needs to be taken into consideration. This is because in spite of using IT/IS for making strategic impacts, corporations need also to protect business information and IT/IS infrastructure. This issue was addressed by one CEO with a background in Finance/Insurance Industry, which was identified in the seventh formal theme:

“CEO G: I, as a CEO, I am supposed to be responsible for IT/IS security risks. The CEO of Company G primarily focusing on the strategic level of group IT infrastructure development, provide leadership and support to the effectiveness of IT governance structure. Making the transformation IT development to continuously improve the competitive edge over its competitors and creates values to the customers, agents and policyholders at large. A central role of the CEO of Company G is to ensure that decision making stays grounded in the facts where we play a critical role in ensuring an appropriate balance between near-term profit initiatives and risk (i.e., compliance with statutory guidelines and requirements, competition, customer satisfactions and operational efficiency).”

Previous responses indicate that the decisions on IT/IS security investment need to be balanced with business risk requirements.

In IT/IS security governance, business requirements were identified from bottom to board and senior management levels within departmental/management levels. Corporate governance has enhanced the scope of business requirements into a wider and integrated perspective rather than looking at a single department perspective (e.g., IT Department requirements only). Two interviewees mentioned the reforms of IT/IS security perspectives in their organisation, which were identified in the 1st and 3rd formal themes. For example, one Chief Information Officer noted:

“CIO C: We have a specific ICT security policy. We do plan for three things – site plan, service plan and governance plan. In the past our focus has been planning and services, now our focus is governance”.

Bad reputation of the corporation such as security incidents was the consequence of poor corporate governance. Good corporate governance relates to the effective and efficient application of internal controls over IT/IS security policies and procedures to ensure those objectives are achieved accordingly. The following shows the response made by one CIO, as identified in the 3rd Formal Theme:

“CIO B: Yes, if lack of internal controls on security, it will damage corporation name”.

Thus, effective internal controls may function as a strategic tool to achieve business goals.

4) Compliance

Three corporations recognised the importance of compliance within IT/IS security implementation. Even though the Stock Exchange and Malaysian Code of Corporate Governance did not have requirements on IT/IS security, IT/IS security governance remains important in some corporations. The importance of IT/IS security compliance was identified in the formal dimension themes (1st, 3rd, 4th, 6th and 7th) and informal dimension themes (1st, 3rd and 4th).

Two responses were identified in each of the 1st ‘policy’ and 3rd ‘security internal controls’ formal themes, three responses in the 4th formal dimension theme ‘committee’ and one response identified in each of the 6th formal theme ‘organisational structure’ and 7th formal theme ‘security risk and its management’. Three areas of compliance that the interviewees noted were regulation, policies and procedures, and confidentiality of information.

Interviewees emphasised security compliance as important for their business needs. For instance, one CEO stated as identified in the 7th formal theme:

“CEO F: So our organization actually emphasize quite and focus on compliance confidentiality of information, and those things, they are very stringent in that area because security is part of risk management”.

Furthermore, according to the CEO of Company F, they were required to comply with Stock Exchange Requirements and the Financial Regulation Act by Malaysian Act on finance matters:

“CEO F: No ISO, we don’t have ISO for IT/IS, we only comply to the Bursa Malaysia Listing Requirements and of course our external auditors in their certain features that are important in our IA and Financial Reporting Standard (FRS), we have to comply with two structures of reporting. FRS, probably we have a copy of that. The whole of Malaysian has to comply the Financial Accounting Act”.

Even though the Stock Exchange Requirements do not impose IT/IS security the Financial Act regulation has included confidentiality of information as identified in the 4th formal theme,

“CFP F: Just want to clarify FRS is widely the scope on financial, financial reporting, so it is not specific on security issues, even Bursa Malaysia requirements, they always talk how the company to recall the confidential of information”.

Complying with security policies and procedures was also a business requirement according to interviewees. Compliance and internal controls were closely related to each other because the main purpose of internal controls is to guarantee that the objectives of certain policies/procedures are achieved effectively and efficiently. Two CEOs indicated the use of internal controls to achieve compliance with policies. One CEO pointed out:

“CEO G: Yes, we do have internal controls to ensure the goal of IT security policies are implemented as intended. Internal Risk Team, Internal Audit Team and IT Team are working together for achieving compliance for the user group”.

External control/regulation was also taken into consideration in the formulation of IT/IS security policies and procedures. This is, however, dependent on industry type and business goals of the corporation as each case is unique. For example, one Chief Information Officer stated , as identified in the 1st and 4th formal themes:

“CIO E: First, I will have to ensure that we have an IT/IS Security Policies and Procedures, and it has to adhere to the Central Bank of Malaysia’s Guidelines. The Central Bank of Malaysia’s is the Malaysian Central Bank. Our business which is insurance industry is under the Central Bank of Malaysia’s Act. The IT/IS Security Policies will be reviewed and approved by the IT/IS Steering Committee. The IT/IS Security Policies are communicated to all levels of the staff in the company. Our Internal Auditors will audit the IT/IS Security Policies from time to time to ensure compliance and its adequacy.”

In this case, the business security policies had been aligned with external regulations such as the Bank of Malaysia Act. As a result, compliance was needed in business operations in Company E.

There was one response identified in each of the 1st informal theme ‘techniques and controls’, the 3rd informal theme ‘human issues-lack of awareness, stupidity’ and the 8th formal theme ‘education, training, seminar, orientation’. Non-compliance with certain policies or procedures was due to lack of people’s integrity and awareness. The relationship of both elements-non-compliance and human elements-can be seen in one response, as identified in the 1st, 3th and 4th informal themes:

“CEO F: If the employees lack training and awareness, they are not accountable. This may lead to unmoral behaviour such as cheating and abusing of information. If the employees are not trained, they are not aware and also not compliant with IT policies and procedures”.

5) Internal controls procedures and processes

There were 7 companies who had applied internal controls to achieve IT/IS security policies as identified in the 2nd, 3rd and 7th formal dimension themes.

One response was identified in each of the 2nd formal theme ‘strategic vision and security importance’ and 7th formal theme ‘security risk and its management’ and eight responses were identified in the 3rd formal theme ‘security internal controls’. Many areas that related to internal controls procedures and processes within interviews were identified which include “auditing”, “IT related matters review”, “control environment”, “correct resources available”, “achieving goal of IT/IS security policy”, “exception report”, “avoiding security breaches”, “IT security procedures” and “governance role”. A CEO expressed, as identified in the 3rd formal theme:

“CEO F: Yes. We have internal controls to ensure the goals of IT/IS security policy are achieved as intended. All the compliance, physical and environmental security even the physical security whether your laptop can move around and be seen by anybody also part of internal controls”.

There was a number of ways internal controls had been used in IT/IS security. As noted by one CIO and also identified in the 3rd formal theme:

“CIO B: Internal controls are used in avoiding security breaches”.

In addition, according to the CIO of Company B, exclusive technical security reports assisted him to address and mitigate the potential for any security breaches effectively in daily operations.

Good internal controls rely on the tone of the board and senior management and ensure that the investment of resources is correctly used to achieve its goals. The CEO of one corporation confirmed the vital role of the board and senior management to control the environment successfully, identified in the 3rd formal theme:

“CEO A: Yes, Company A Malaysia has a system of internal control which includes the establishment of an appropriate control environment and framework. The Board of Directors are the owner of the system of internal control as they establish the tone at the top of the organisation, ensuring that the importance of internal control is understood and that the correct resources are available”.

Internal controls are important to IT/IS security governance to ensure that certain goals and objectives are accomplished effectively. In the case of Company D, the IT department had a major role

to make sure that the internal controls were applied in IT/IS controls, as identified in the 3rd formal theme:

“CIO D: I believe internal controls is very important, that’s why the existence of my department in COMPANY D in the first place, COMPANY D management decided that we need to have one dedicated unit, we need to have a representative, a department to manage the governance, internal controls in all IT issues, ICT controls. That’s why the department was established in early 2005, 2004 we outsourced”.

Many methods could be used in corporations for reporting the IT/IS security internal controls. One CEO noted as identified in the 3rd formal theme:

“CEO H: We do have internal controls in place. The Board of Directors will be informed through exception reports from management when necessary”.

In the corporation’s structure, the participants worked closely with committees like Audit and Risk to ensure that the internal controls of IT/IS security policies and procedures were complied with which is described in the following quotation.

“CEO F: we are actually very concerned about the risk managing part and our auditors and external auditors actually look to our IT/IS security and comment on whether we have enough controls and also when we have back up”.

6) Policy and informal factors

All companies have indicated the importance of informal aspects to achieve policy and technical implementation as identified in all dimensions themes. In the formal dimension, themes identified that related to this issue were 1st formal theme ‘policy’ and 4th formal theme ‘compliance/legal requirements/regulation’. Technical dimension themes that related to this issues were 1st technical theme ‘techniques and controls’ and 3rd technical theme ‘internet/network security’. In the informal dimension, this issue was identified in all three informal themes-1st ‘staff integrity/trust/ethicality’, 2nd ‘culture, commitment’ and 3rd ‘human issues-lack of awareness, stupidity’.

There were six responses identified in the 1st formal theme and three responses identified in the 4th formal theme. In the technical dimension, nine responses have been identified in the 1st technical theme and one response identified in the 3rd technical theme. In the informal dimension, this issue was identified in 11 responses of 1st informal theme, two responses of 2nd informal theme, four responses of 3rd informal theme and 21 responses of 8th Formal theme.

Informal factors were an important human aspect to support the implementation of IT/IS security policy and technical implementation. Many human aspects areas were identified regarding IT/IS security concerns. The identified areas were culture, communication to all level of staff, codes of ethics/practices, being professional, human aspects are critical success factors, accountable, core values, human integrity, human aspects, morale, trust and ethicality. Educational programmes that came from the 8th formal theme such as training, awareness, induction programme, seminar and orientation programme will strengthen the values; organisational and individual. All of these areas embraced by interviewees were tied to the IS/IT Security Governance Model developed in Chapter 4.

One CEO addressed, as also identified in the 1st formal theme, the 8th formal themes, the 1st technical theme and the 3rd informal theme:

“CEO A: Informal factors are very important to support the implementation of IT security policy and controls. Successful IT security policy and controls is not just the deployment of technology (firewalls and intrusion detection systems) but is a series of essential practices that is embedded into the culture of Company A Malaysia through training, education, awareness and others. Once the IT security policy and controls are created, communicated and adopted, only then IT facilities can be effective to support and enable business requirements in a secure manner”.

Education, training and awareness were perceived to be a crucial aspect of employees for the implementation of IT/IS security in the formal aspects, evidence was found in the responses of six interviewees. For instance, the CEO of Company F noted, as identified in the 8th formal theme, 1st technical theme and the 3rd informal theme:

“CEO F: I think very classic informal factors would be educational part, the training part. Yes, the training, IT awareness that is probably the biggest informal like let say I am very IT oriented, you talk about IT/IS could be aware of it, but some people may not, so there will be very diverse level of understanding, when you talk about security controls and firewalls, but if everybody is aware of all the IT aspects in the business operation, then make it simple for the IT people, when they talk everybody understands. but once the IT goes into the jargon of coils and things like that, what is coils, they start wondering or interpreting of that, when you talk about whether we have enough firewalls, safeguard our back up setting. We built in mitigating factors to mitigate risk such as firewalls”.

The responses by the CEO of Company F emphasised that the relationships between education, training and awareness were important to all employees to ensure that IT/IS security is successfully implemented at all levels/departments efficiently.

Specifically, one educational programme related to IT/IS security was imposed in the IT/IS security policy, which was identified in the 1st formal theme and the 8th formal theme:

“CIO B: Yes. The orientation program is stated in the IT security policy”.

IT/IS security governance, in fact, requires the informal aspect to deliver the policies and procedures in corporations. In IT/IS security governance, communication to all levels of staff was part of the governance process. This example can be seen in the following response identified in the 1st, 4th and 8th formal themes:

“CIO E: Informal aspects incorporated in the implementation of policies and procedures relating to IT security are communication to all levels of the company, staff induction program, staff training, attending seminars, update or reviews of the Central Bank of Malaysia’s guidelines or compliance”.

Apart from education, training and awareness in place, the informal aspect is also concerned with human values. Four interviewees emphasised the importance of human values in the IT/IS security implementation. For example, accountability and integrity were important core values for technical implementation, as identified in the 1st technical dimension and the 1st informal theme:

“CEO G: Of course. Informal factors are important to support the implementation of IT/IS security because if people are not accountable and lack of integrity, the system processes would be compromised. I think the core values, such as integrity are fundamental and everything”.

The human aspect was recognised as a critical success factor to the implementation of IT/IS by one CEO, as identified in the 1st informal theme:

CEO H: Yes, human aspects are always the critical success factors that determine the success or failure of any IT implementation”.

A standard code of practice was used to achieve informal aspects in supporting the implementation of IT/IS security policy. There were two responses regarding the use of a code of practice in corporations. For example, one CIO stated, as identified in the formal themes (1st, 4th and 8th), technical themes (1st and 3rd) and informal themes (3rd):

“CIO C: We have a Code of practice to implement informal aspects. Employees need to follow the code of practice to ensure that employees aware with ICT security policy in this corporation. Code of practice provides the details on what to do when the lines come out. For example, the widely use of advanced technologies such as wireless and mobile for Internet access when they are outside the corporation's network system”.

In another case, the ICT baseline was identified as guidelines to follow for the implementation of informal aspects, as also identified in the 1st informal theme and 8th formal themes:

“CIO D: in short we have ICT baseline for informal aspects which cover the good ethics and educate the staff”.

7) Governance in IT/IS

Five companies had IT/IS governance within their business operations, as identified in the formal dimension themes. Themes identified related to this issue were 1st formal theme ‘policy’, 2nd formal theme ‘strategic vision and security importance’, 3rd formal theme ‘security internal controls’ and 7th formal theme ‘security risk and its management’. In regard to this issue, there was one response identified in the 1st formal theme, 4 responses were identified in the 2nd formal theme, three responses in the 3rd formal theme and two responses in the 7th formal theme.

The areas identified were “operation of business”, “dependent on IT”, “IT infrastructure development”, “IT governance structure” and “governance body”. These four companies had a high level use of IT/IS for achieving business goals which was evidenced in the identified areas. For example, the CEO of Company F pointed out and identified in the 2nd formal theme, where the following interview data of Company F were repeated and referenced in this secondary issue because IT governance is about the alignment between business needs and IS/IT requirements. The IS/IT such as Finance Integration of Financial Statement Information Accounting, Integrated Financial System and Plantation Management System are required for fulfilling the primary activities of business. The example of IT governance is illustrated here:

“CEO Company F: Our corporation is highly dependent on IT and most of our systems are electronically digitally get up, I mean we have IT on our Finance Integration of Financial Statement Information Accounting, we have Integrated Financial System which is linked very closely with our Plantation Management System. And also linked directly to our Human Resource Information Systems (HRIS). So among the three of this, software and the systems we have used for accounting systems will be used directly for reporting in our corporation”.

A governance body or organisational structure is a component of IT Governance. This body is responsible to align IT/IS requirements with business goals. There were three responses on governance structure. For example, one CIO who was from a top 50 company had played his role in this respect as identified also in the 1st formal theme and 3rd formal theme:

“CIO D: a department to manage the governance, internal controls in all IT issues, ICT controls”.

Leadership is another component of IT Governance to make it happen. The active role of boards and senior management is greatly needed in IT Governance because all strategic decisions such as budgets and risks are in their capacity. The evidence of IT Governance implementation was seen in the response by one CEO, as identified in the 7th formal theme:

“The CEO of Company G primarily focusing the strategic level of group IT infrastructure development, provide leadership and supports to the effectiveness of IT governance structure. Making the transformation IT development to continuously improve the competitive edge over its competitors and creates values to the customers, agents and policyholders at large”

8) Responsibility of senior management

Three interviewees recognised that senior management have responsibility and accountability in all business operations in respect to the IT/IS security agenda, as identified in the formal and technical dimensions themes. In the formal dimension themes, one response was identified in the 3rd formal theme, four responses were identified in the 7th formal theme and one response identified in the 8th formal theme.

The areas identified were “leadership”, “tone of the top” and “responsible and accountable to all operations”. Three senior managers indicated their roles in IT/IS security. For instance, one CEO described as identified in the 7th formal theme:

“CEO H: CEO is ultimately responsible and accountable for all operations of the company that include to ensure that an effective and efficient framework is in place to manage the IT/IS security risk”.

9) Role of Committee

Eight interviewees commented on the importance of involvement of committees in IT/IS security governance as identified in the formal dimension themes. In the formal dimension, themes identified that related to this issue were 6th formal theme ‘committee’ and 7th formal theme ‘security risk and its management’. 29 references were identified in the 6th formal theme and 9 references identified in the 7th formal theme.

Few committees and roles were identified to have involvement in IS/IT security governance. Six areas of role of committee were identified which include “Risk Management Committee”, “IT Risk Management Committee”, “the need for IT Committee for security policy implementation”, “IT steering committee at corporate level”, “audit committee has role in monitoring IT implementation” and “IT security issues to be addressed in steering committee”.

The Risk Management Committee played a significant role in IT/IS security according to all interviewees. The following responses show the inclusion of IT/IS security issues by the Risk Management Committee which also involved boards and senior management. As noted by one CEO as identified in the 6th and 7th formal themes:

“Like many other matters, IT related matters are also constantly reviewed as part of the organisation’s Enterprise Risk Management programme. This includes the system recovery issues, information security issues and others. These issues are identified through the organisation’s Enterprise Risk Management process whereby the Risk Management Team headed by the Finance Director and comprising senior managers from all departments in the organisation including IT, will conduct quarterly reviews of the business risks as part of their responsibilities”.

In the case of Company B, a governance body called IT Risk Management Committee was responsible for IT/IS security issues. The following response was identified in the 6th and 7th formal themes:

“CIO B: Yes, IT/IS security is part of Risk Management Plan. Our company has a Risk Management Committee, it is now a standard activity. I am a member of the Risk Management Committee. And we have IT Risk Management Committee”.

Six companies had an IT steering committee in place. The IT steering committee benefited its corporation in many ways. For example, as noted in the following CEO’s responses and identified in the 6th formal theme,

“CEO F: Yes, we do have IT Steering Committee. We have our IT, it is like a Task Force where we look at, it looks like IT Steering Committee, for example we have to implement the Integrated Financial Management System. We will form the Task Force to see what are the requirements in terms of size, speed, operational interoperability how dependable the system and all that. In the meantime, IT Department and Internal Audit will monitor ongoing implementation of IT/IS security at Planning and Setup stage”.

Three interviewees described the important role of the IT Committee in the policy formulation and implementation. For example, one CIO noted, as identified in the 6th formal theme:

“CIO E: Yes, we do have an IT/IS Steering Committee. First, the IT/IS committee sets the direction. Second, we have to ensure that policy complies with the Central Bank of Malaysia’s guidelines. Thirdly, we have to ensure its compliance. Fourthly, we need to review it periodically as mentioned earlier on”.

However, 3 interviewees mentioned that the IT committee was not responsible for policy implementation. The IT committee was rather concerned with ad hoc or temporary IT projects and developments in these three corporations such as one CEO noted, as identified in the 6th formal theme:

“CEO G: We have IT steering committee to oversee IT applications development. The function of IT steering committee is to develop solution which is consistent with outsource risk. IT steering committee is not responsible to the implementation of policy relating to IT security”.

10) Role of Department

Four companies perceived the important role of departments in IT/IS security governance, as identified in the formal and informal dimensions themes. There were five responses identified in the 6th formal theme ‘communication channels’ and one response was identified in the 8th formal dimension theme.

There were two departments mentioned by interviewees responsible in IT/IS security processes; IT department and Human Resources. The IT department was responsible in the policy formulation and implementation relating to IT/IS security as claimed by four interviewees. The identified areas were “IT department has a role in IT/IS security policy implementation”, “IT department has a role in operational management of IT processes” and “human resource”. For instance, as stated and identified in the 6th formal theme:

“CEO A: In this organisation, there is an IT department and the department responsible for the day to day management of the IT system and processes in the organisation”.

In Company B, the IT department and Human Resource department worked closely to ensure that IT security policies are implemented effectively. As the IT department was charged with security policy implementation, the Human Resource department was responsible in informal aspects for the accomplishment of policy, as identified in the 6th formal theme and the 8th formal theme.

“CIO B: Training is not stated in the IT security policy, the training comes from the Human Resource Department”.

8.4.2.1.2 Primary Issue: Policy Development

The primary issue ‘policy development’ was identified in the formal and technical dimensions themes, the secondary issues reflect the specific issues relating to the dimensions themes to which they relate as can be seen in Tables 8.4a and 8.4b. Policy development involves issues reflecting policy formulation, identification of IT/IS security issues and the development of IT/IS security policies areas within corporations. There were seven secondary issues identified, these include “role of IT staff”, “role of boards”, “role of other department”, “risk”, “policy formulation”, “policy review by external party” and “identification of policy development areas”.

ISSUES											
	Primary	Secondary	Source	Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
				Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal Requirements/Regulation	Organisational Structure	Committee	Security Risk & its Management	Education, training, seminar, orientation
2	Policy Development			49						4	
		Role of IT staff	A, F, H	4							
		Role of boards	A, C F G	7							
		Role of other department	H, A, G	4							
		Risk	A H	2						2	
		Policy Formulation	A E	4							
		Policy review by external party	C	1							
		Identification of Policy development areas	A B, C, D, F G H	27						2	

Table 8.4a The primary issue of 'policy development' and its secondary issues

	Issue								
	Primary	Secondary	Source	Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
				Techniques & Controls	System Development	Internet/ Network Security	Staff integrity/ trust/ ethicality /accountability	Culture, commitment	Human issues- lack of awareness, stupidity
2	Policy Development			14	1	11			
		Role of IT staff	A, F,H						
		Role of boards	A,C F G						
		Role of other department	H,A,G						
		Risk	A H						
		Policy Formulation	A E						
		Policy review by external party	C						
		Identification of Policy development areas	A B, C, D,F G H	14	1	11			

Table 8.4b The primary issue of 'policy development' and its secondary issues

8.4.2.1.2.1 Secondary Issues

1) Role of IT staff

Three companies claimed the significant role of IT staff within the policy development process of the corporation as identified in the formal dimension theme. There were four responses identified in the 1st formal theme ‘policy’; two areas have been embraced by interviewees— policy formulation and identification of issues.

Three interviewees commented that policy development requires involvement by IT staff. In respect to policy formulation, two interviewees commented on the involvement of the IT department in the formulation process. The following example was identified in the 1st formal theme:

“CEO F: The management headed by myself, and of course the IT department and the internal audit are involved in the formulation of IT/IS security policy”.

IT staff also had responsibility for the identification of security issues. Two responses were received in this regard. For example, one CEO noted, as identified in the 1st formal theme:

“CEO A: These security issues are identified mainly by the IT staff with assistance from Business Security staff in Company A Malaysia. They ensured that the decisions were appropriate to the business risks, measured against industry best practices and sat within Company A Malaysia’s existing governance and policy structures wherever possible”.

2) The role of boards

The role of boards in policy development was perceived to be important by five companies as identified within the formal dimension. Seven responses were identified in the 1st formal theme ‘policy’. In regards to the role of boards, the areas of this issue were identified which include “policy approval”, “policy formulation headed by CEO”, “security issues identified by audit committee”, “policy formulation involved by internal audit” and “security issues identified by risk committee”.

The boards were ultimately responsible to approve security policies because they are concerned with minimising business risks. For example, one CEO pointed out, as also identified in the 1st formal theme:

“CEO A: All policies in Company A Malaysia have to be approved by the Board of Directors and similarly the policy in relation to the aspect of security of IT. Generally, aspects of security in Company A Malaysia are governed by the Business Security Policy and this includes the aspect on security of IT”.

The board, including the Risk Committee and Audit Committee, were also involved in the identification of security issues in all levels. For example, as noted and identified in the 1st formal theme:

“CEO G: The same groups again, users, risk managers and IT team (Mgroup), and also Executive Directors and all the boards. To find the relevant committees, that may be either committee of the boards, Risk Committee and Audit Committee”.

3) Role of other departments

According to three companies, the contributions of other departments are also desired in the policy development apart from the IT department and the board. This issue was identified in the 1st formal dimension theme with four responses. The recognised areas include “involvement by Human Resource”, “by other departments”, “identified by business security staff” and “identified by risk manager”. Policy development in IT/IS security requires more integrated perspectives as security issues are not only technology and organisational problems but also a human problem. Three interviewees commented on the important role of other departments as identified in the 1st formal theme:

“CEO H: IT, Human Resource and representatives from other departments with an interest are involved in the formulation of IT/IS security policy”.

IT/IS security implementation requires an integrated perspective from all levels/departments because IT/IS has been used to support core business operations. The intense use of IT/IS across departments has also increased IT/IS risks if not managed effectively. Thus, active involvement and input from all departments are crucially important.

4) Policy review by external party

Advice from external parties was also needed in the policy formulation by Company C. This issue was identified in the 1st formal dimension theme ‘policy’ within one response. For example, as one CIO noted and identified in the 1st formal theme:

“CIO C: Yes we wrote ICT security policy ourselves, then we got an external party to double check the ICT security policy, then we put it to the board to approve it”.

5) Identification of policy development areas

Seven companies had recognised the use of IT/IS security policies to protect business information as identified in the formal and technical dimensions themes. In the formal dimension, 27 references were identified in the 1st formal dimension theme ‘policy’ and two references in the 7th formal theme ‘security risk and its management’. In the technical dimension, there were 14 responses in the 1st technical theme, one response in the 2nd technical theme and 11 responses in the 3rd technical theme.

A number of development areas was identified within this secondary issue. The recognised areas include network connectivity, account/access management, vulnerability management, secure system development, incident management, host protection and authentication, mobile and wireless access, e-mail, desktop management, IT system management, data classification, software, internet, back up, information security and internal use. As pointed out by one CEO and identified in the 1st, 2nd and 3rd technical themes:

“CEO A: The main objective for the establishment of this aspect of security in the policy is to protect the interests of Company A Malaysia by applying appropriate measures to the organisation’s IT assets and processes. The security issues that are included here in the policy are related to network connectivity, account management, vulnerability management, secure system development, incident management, host protection and authentication”.

Every corporation has unique requirements for security areas. Two CIOs commented that their corporations required policy on mobile and wireless access. The need for mobile/network policy in their corporations was due to the huge number of employees accessing private networks using such devices. For instance, one CIO as identified in the 3rd technical theme commented:

“CIO C: Yes IT security policy does cover the use of mobile and wireless access by employees”.

Without policy and internal controls in place, this would increase security threats and vulnerabilities to business information and IT/IS assets either by internal employees or outsiders. For example,

“CIO C: From technical perspective, the use of mobile and wireless access creates conflicts or back door entry”.

Three interviewees claimed the importance of e-mail and internet policy as part of controls to ensure that their employees were always aware of the freedom to use of internet facilities within the work-place. For example, as noted by one CIO and identified in the 3rd technical theme:

“CIO B: We have five basic policies that cover backup, internet use, e-mail use, desktop appearance and data classification”.

In addition to the internet use at the work-place, another CIO reported he had increased the security level:

“CIO C: In fact some of the non-business related sites are being blocked for staff to access”.

Three CEOs recognised the vital need of access or account management policy to be implemented in their corporations. In one corporation, systems privilege set out by the senior management may control access to certain information according to group levels such as:

“CEO F: not all the IT staff would have access to the Accounts File Directory and all to Account, only certain staff doing the payroll system and IT manager sometimes IT manager don’t have the equipment”.

The following shows that the policy relates to access in Company F, as identified in the 3rd technical theme:

“CEO F: We have a number of policies and procedures here, you may want to have a look at the major headline, System information access control, Physical and environmental security, Network management, Back up and restoration, System back up and ownership, IT system change management, Problem management and IT system capacity management”.

8.4.2.1.3 Primary Issue: IS/IT Security Implementation

The implementation process of IS/IT security has been discovered relating to several areas. The primary issue of IS/IT security implementation was mainly identified from all formal themes, many responses were received in the policy theme (Formal Theme 1), some in the security internal controls theme (Formal Theme 3) and in the educational them (Formal theme 8). References were also identified in all Informal themes and one theme was identified in the internet/network security theme

(Technical Theme 3). There were eight secondary issues identified in the interview data, these are “the protection of IS/IT business assets”, “policy process and roles”, “policy process and informal factors”, “protection and controls”, “identification of security issues”, “auditing”, “risk management”, and “policy achievement and internal controls”. See Tables 8.5a and 8.5b.

	ISSUES			Themes							
	Primary	Secondary	Source	Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
				Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal Requirements/Regulation	Organisational Structure	Committee	Security Risk & its Management	Education ,training, seminar, orientation
3	Implementation		A,B,C, D,E,F, G,H	38	3	17	1	3	2	6	11
		Protection of IT & Business Assets (Data, Information, Architecture)	B,F,G, H	8				1			
		Policy process & roles	B,E,D, F,H	6	1	2	1		1		2
		Policy process & informal factors	B,D,F, G		2						7
		Protection & Controls	B,D, F,G	1		4		1		1	
		Identification of security issues	C,D	1		2		1	1		
		Auditing	A,E,F	2		2					
		Risk Management	A,B,C, F,D,E, G,H	1 6		2				12	
		Policy achievement & Internal controls	A,D,E, F,H	4		5				2	2

Table 8.5a The primary issue of ‘implementation’ and its secondary issues

	ISSUE		Source						
	Primary	Secondary		Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
				Techniques & Controls	System Development	Internet/Network Security	Staff integrity/trust/eth-icality/account-ability	Culture, commit-ment	Human issues-lack of awareness, stupidity
3	Implemen-tation		A,B,C,D, E,F,G,H				2	2	3
		Protection of IT & Business Assets (Data, Information, Architecture)	B,F,G,H						
		Policy process & roles	B,E,D,F, H						
		Policy process & informal factors	B,D,F,G				2	2	3
		Protection & Controls	B,D, F,G						
		Identification of security issues	C,D						
		Auditing	A,E,F						
		Risk Management	A,B,C,F, D,E,G,H						
		Policy achievement & Internal controls	A,D,E,F, H						

Table 8.5b The primary issue of ‘implementation’ and its secondary issues

8.4.2.1.3.1 Secondary Issues

1. “the protection of IS/IT business assets”:

Four participants stated their involvement in the protection of IS/IT business assets. The data show that the IS/IT business assets are referred to as security of network, business data and information, compliance, password management, the role of user groups for the IT systems and business development.

The CIO of Company B stated that the organisation has protected the IT systems from viruses and spams using an intranet network system, as identified in the Technical Theme 3,

“CIO B: Our control system now identifies and deletes viruses automatically even on thumb drives. Virus is part of our security issues. Yes, it cleans the system immediately giving us protection. We have good intranet protection and protection from outside including from spam. At one stage we got over hundred thousand spam in one month. This is another serious security issue in this corporation”.

Interestingly, the CEO of Company F raised the security concerns over its information assets and business strategy information, as he noted:

“CEO F: Well, what management and myself and those is become compulsory to implement policy for the IT department and the rest of the relevant related like finance, information on marketing, business development, the whole have to comply”.

Compliance with the security policy is part of check and balance in Corporation F:

CEO F: Under IT policy, they have to follow the section required in order to comply with the security controls or whatever safeguards, check and balances”.

The following statements show how the Bell La Padula theory was applied in Company F, it keeps confidential data secret, where a computer user with a low level clearance should not be able to read files marked as a computer user with a high clearance, as identified by CEO of Company F:

“like Director of Corporate Services will have to look at whether someone can access to her security or password to communicate to Bursa Malaysia, it is only she that can access and start transmitting statement communicating to Bursa Malaysia based on what the board has agreed to sanction and all that to make statements announcement and all that just example, this is very tight.

Normally, the security risks relating to IT are identified at the level of end-user of the systems. The role of end-user is very critical in achieving IS/IT security because the end-user of the system is responsible to protect the secret data and confidentiality of data and information received from their internal employees, clients or external stakeholders. With effective supervisory roles between the supervisor and holder of the responsibility, the organisation may reduce the risks such as information leakage, data loss, data theft, financial losses and business reputation damage. When the interviewees were asked about who is the owner of the end-user (user group) in their organisations, the CEO of Company G said:

“CEO G: Depending on the nature, the work portion, users are always responsible, the owner of the system who always responsible for the system, usually the owner is the user group”

The end-user of the system or the holder of responsibility has a critical role in ensuring that the confidentiality, integrity and availability of IS/IT systems are not compromised because the identification of risk is always sourced and identified at the end-user level. The one who is the owner of the risk as the one who is responsible to implement the technical procedures of IS/IT security policy, as highlighted by the CEO of Company H:

“CEO H: The respective risk owner with guidance from IT department is responsible for implementation of aspects of the policy.”

2. “policy process and roles”

The data have revealed ‘who’ plays the roles and ‘what’ activities are involved in the implementation of policy processes. Five participants have shown their entity roles and their policy activities in various areas, as identified in the Formal themes and Informal themes. In the case of Company B, based on the policy obligation, the CIO has given the security responsibility to all employees within the technical procedures:

“CIO B: At implementation we roll out the policy to all staff. Policy is incorporated into our procedures. In what we do policy comes first, procedures follow and the things that must be done are done. We publish our policies to all staff in our IT repository”.

Roles of each individual and responsibilities are defined:

“CIO B: Yes. Roles are defined within the policy. Responsibility and data owners are identified. Data owners are referred to throughout our policy”.

Another interesting finding was in Company E, since this company has a financial and insurance background, where the contents of policies need to adhere to the regulations of an external body- the Central Bank of Malaysia’s Guidelines:

“CIO E: First, I will have to ensure that we have an IT/IS Security Policies and Procedures, and it has to adhere to the Central Bank of Malaysia’s Guidelines. The Central Bank of Malaysia’s is the Malaysian Central Bank. Our business which is insurance industry is under the Central Bank of Malaysia’s Act”.

In the case of Company E, the IT Department led by the CIO worked closely with the IT Steering Committee in the formulation of policy before delegating the responsibilities to all levels of employees. For example,

“The IT/IS Security Policies will be reviewed and approved by the IT/IS Steering Committee. The IT/IS Security Policies are communicated to all levels of the staff in the company.”

In another case, the researcher interviewed a subsidiary corporation of a publicly listed operating company, Company D, where most strategic decisions and policy developments were crafted at the parent company level. According to the CIO of Company D, the IS/IT security strategies and policies came from the corporate IT unit of the parent company but in some circumstances the CIO of Company D still has responsibility in decision making and resolving lower levels issues. As stated by the CIO of Company D:

“CIO D: In directly since the policy and procedures was crafted at Corporate IT Development Unit level so in a way we have to be liaising a lot with Corporate IT Development Unit, getting some directions, some inputs, some recommendation, of course we make some decisions as well, of course when come to certain issues, if we think it warrants to be brought up to Corporate IT Development Unit we will, same goes to any security issues, we think if we can manage at our own level with I-Pgroup, we will do that. If it involves something at the group level, then we will incorporate and do further collaboration on this issue with the person in charge at Corporate IT Development Unit ..”.

To identify the security issues and problems at ground level, Company D used a forum for discussing the security matters and the CIO explained the role of the department (at parent level) in dealing with the IT security issues. For example, The CIO of D stated:

“and then we use a forum, for budget, for security, discussed security concerns with Corporate IT Development Unit. At Corporate IT Development Unit we have a group in charge of security, we have a group in charge of service level, we have a group in charge of the governance, a group in charge of

customer relations, we have a group in charge of planning or budgeting, so we have 4 or 5 departments in Corporate IT Development Unit itself, and so if we have security issues, we channel them to the security department in Corporate IT Development Unit who is focusing on ICT security and those policies coming from them” (CIO, Company D)”.

The achievement of IS/IT security is dependent on the commitment received from all departments/sections within the organisation, including the Human Resources Department. It was found that three companies have mentioned the role of human resources in achieving IS/IT security, identified from the Formal and Informal Themes. The human resource role is important especially when new staff report for duty, several resources need to be provided to new staff such as computer desktop and resources, computer access passwords and training. For example, the CIO of Company B said that his IT department is working closely with Human Resources to provide the training relating to IS/IT security policy:

“CIO B: Training is not stated in the IT security policy, the training comes from the Human Resource Department”.

After delegating the responsibilities and security roles to all staff, all heads of department and supervisors of sections should report progress relating to the implementation of the technological areas and procedures and informal factors including the Human Resource Department, such as:

“CEO H: CEO is responsible to ensure basically, every operation in the company runs smoothly. CEO will delegate the authority to various departments concerned, for instance, Human Resource department to execute and report to CEO on managing the informal factors.”

Apart from that, the Human Resource Department is also responsible to manage the resources when the staff member leaves. In Company F, the Human Resource Department should work closely with IT department to ensure the database privileges and access to computer resources have been updated and changed effectively after the resignation took place:

“CEO Company F: the department themselves all looking after plus so called the internal audit will check whether if let say a person has resigned or has moved on to another department. From human resource, make sure the password always aware and change”.

The role of human resources is significantly important to ensure that the passwords over the IT systems and network have been deleted to prevent unauthorised access and other types of suspicious/irresponsible activities.

3. “policy process, educational and informal factors” bold

The interview data show that educational aspects such as training, orientation programmes and induction programmes have influenced the state of informal factors of the organisation and individuals, as identified in the Formal themes. When a CEO and CIO were asked about their views relating to informal factors, most of the answers given predominantly related to educational aspects rather than to culture, trust, beliefs including organisational values and employee values. For example, the CIO of Company B stated the importance of educational aspects including orientation programme and training for achieving policy:

“CIO B: Normally new employees have to attend orientation program. In the orientation program, the employees are being informed about the corporate policies including IT security policies. Normally new employees have to attend 2 hours training session regarding IT things, normally the Human Resource will brief on the IT/IS security policies. Training is an important aspect to reduce security incidents. And security incidents could lead to bad reputation of the corporation”.

Similarly, the other interviewee emphasised the importance of educational aspects such as training, awareness, orientation and induction programme, as mentioned by the CEO of Company F:

“CEO F: We all in management as a MD would be responsible to make sure people are aware, we must provide training, we must update ourselves, we must send people for awareness courses or we provide information through mail or whatever so that you can update yourself. Like FRS, the comments by auditors, of course to make sure we are, the culture we want to cultivate is aware especially new staff. We have orientation, we have induction programme and all that that would help us ensure the awareness is want to be.”

Interestingly, in one organisation, the educational aspect such as awareness programme is conducted quarterly,

“they do have some sort quarterly session like IT security awareness, in fact recently they have ICT security awareness 3 months ago and made for everybody to come, this is something I-Pgroup together with Corporate IT Development Unit, it is open to everybody (CIO, Company D.”

Due to the advance of network, the similar organisation, Company D has utilised the Internet to enable their staff to learn security materials through the on-line mode:

“CIO D: Yes, e-learning training is compulsory, but it does not subject to any particular topic, that basically to inculcate people to browse e-learning to find all the modules that we can learn but there is a topic on ICT security that they can cover. We don’t simply say you have to take security courses and complete it, but those smart enough, know that ICT courses are quite simple, we do have, but we don’t simply say we should take security course but there is a specific course in our e-learning and staff is encourage to explore themselves”.

Apart from that, the CIO of Company D mentioned the use of the website for conveying the information relating to IS/IT security such as:

“CIO D: In fact on the ICT website, there are a few slides basically on security caution subject, very simple slides for everybody just to ensure the do’s and don’ts are make known, do not put your password, not to say only password per say, but also to email, not simply accepting email or forwarding it.”

Only two corporations have touched on informal aspects which relate to culture or integrity:

“CEO G: Imbue a culture that is aligned with the Board approved corporate strategy, mission, values, objectives, policies and procedures; and fosters risk awareness culture.”

And

“CEO F: Culture and company and all that, they know that our own ethics, knows our culture and company, and our expectation that must be, integrity must not be questionable, once we know we trust them, we must be able to empower them”.

4. “protection and controls”

In this study there are two definitions of internal controls: first, internal control refers to the automatic IT security systems; second, internal controls refers to non-automatic controls like the lists of progress over security counter-measures/security controls (logs or reports), management tools (security incidents report), educational controls (training or awareness). One corporation has given an example of the first type of internal control—automatic IT security systems. As can be seen in Company B, intrusion detection system was the example of automatic IT security systems internal control:

“CIO B: Internal controls are in place to alert us to security breaches. Our controls are mainly related to intrusions – the machine shuts down on a third attempt to intrude. We have in place a password security system and user verification process... We are able to identify how the machines are being used. We can identify when they are not being used appropriately. This is good internal control. We can monitor software on the machines. We authorize the use of the software. We configure the machines so additional software cannot be loaded. Vista is part of our internal control”.

The second type of internal control refers to non-automatic IT security systems or more to the management approach, which enables management to check the progress of certain IT systems implementations to ensure that the goal is achieved. To check this, Company D used Service Level Agreements (SLA). This can be illustrated in the following quotation:

“CIO D: We do have Service Level Agreement (SLA) with I-Pgroup. SLA is employed part of our internal control mechanism. So SLA is actually covering services and others as well, services could be securities, for example, SPAM mail, this incident will be highlighted to I-Pgroup and IP Security Office (IPSO) will pick up this matter and try to resolve it within the specific SLA.

To improve the target level, the management may undertake consecutive management strategies such as weekly meetings, so that this gives the opportunity to the lower management levels to resolve the security issues at that level, this would automatically reduce the risks of organisations. For example,

I think this month, if I am not mistaken, they have to settle a few major issues within 3 working days and be able to resolve this. So during Information Services Management Committee (ISMC) meeting for Company D level, for every quarter, we will ask them to present SLA report for that particular quarter”.

Since the second type of internal control is a non-automatic approach, the management should react and resolve the internal controls results in an effective way such as Company D has used the Service Level Agreement report to indicate the achievement target level of security counter-measures/controls services implementation. According to the CIO of Company D, the holder of the responsibility (the third party) should be able to achieve the SLA target and devise security solutions. If some management (supervisor of responsibility) target level was not achieved, the holder of the responsibility is required to explain why. But, there was no further explanation how the supervisor of responsibility responds and advises solutions in this matter.

“CIO D: At that juncture we should know if there is incident of security or anything and how fast the response and the mitigation process, it will be highlighted during that meeting and of course we’re talking about SLA, and as external party that dealing with our service of course they have to meet certain SLA, if there is any variance, let say they have to meet 90% SLA, if there is variance lower or the difference, for example for that particular quarter they only achieve 70%, then they have to explain why, to the committee, and this covers IT security and anything. If there are late in rectifying the problem, they have to explain if they don’t meet the SLA”.

5. “identification of security issues”:

Identifying the security issues will help management to recognise which management level is responsible (e.g., department) and who are the supervisors of the responsibility and the holders of the responsibility relating to the security issues. From the interviews, security issues were identified in a cascaded way (bottom-up approach), as identified mostly in the formal themes. For example, the security issues are first identified at the ground level. In the case of Company C, the IT Steering Committee helps the organisation to identify security issues at ground levels:

“CIO C: They will identify these issues at the forum, the divisional level and through committee. Ok, yes we do have an IT steering committee. We have four committees that look at overall issues- Divisional Management Committee (overall issues), Division Planning Committee (specific issues), Operation Technical Committee (OTC) (operation issues) and Divisional Risk Committee. So if we have IT or security issues, we discuss with the Division Planning Committee. I am on the risk committee as well”.

Then, later if some security issues cannot be resolved at the lower levels and require involvement from other departments, the higher level meeting will take place, such as in Company C, the issues will be discussed at the council meeting:

“CIO C: Yes, I mention about this security issues in the Council meeting if any. The security issues are identified through the Divisional Officer during the Council Meeting. Technical roles, they leave it to us. Normally we go to the Council meeting, we have our specific roles, Human Resources have their own, technical by our own”.

Similarly, the security issues were identified using the bottom-up approach in Company D. It is important to highlight that Company D is a subsidiary company (Operating Unit) is ruled by Company P in terms of governance and strategic planning, but operational activities are done by Company D. It was identified that there were two stages of meetings in Company D: first a weekly meeting and second monthly or quarterly meeting. The lower level meeting was conducted with IT unit (I-Pgroup),

“CIO D: In fact at my level we do have operational weekly meeting with I-Pgroup, at the working level. So in this weekly meeting we discuss every single subject with regards to ICT”.

At the second stage, the meeting was conducted with IT unit (I-Pgroup) and also with the representative from the parent company called ISMC, such as:

“CIO D: On every month or quarterly, we have meeting with ISMC. Yes every Thursday, we have meeting with ISMC. By right supposed to be done this evening. If we can’t, we do on Friday; we try to make it every week. So any issues relating to IT security will be highlighted. With this operational

meeting, we have a direct access to all I-Pgroup support and management. If the issue deemed to be highlighted at that level, we will use this operational meeting to highlight it to their management.”

According to the CIO of Company D, if the security issues cannot be resolved at the operational level, he will highlight and bring up the issues at governance level, reporting to the parent company during the quarterly meeting with ISMC for decision making, solutions and risk tolerance:

“CIO D: The ISMC has quarterly (minimum) meeting. If there is a need to have it, we will do every two months, sometimes we do every two months sometime we do quarterly, that will be discussing on any IT security issues, services, governance or whatsoever with regards to ICT matter of Company D. At Company D level, ISMC is chaired by Mrs A and alternate chairman is myself. This meeting is focusing on decision making with regards to IT for COMPANY D alone. ISMC at Company D, is specifically for Company D. We have this meeting.”

It is important to note that Company D is a subsidiary company, ` along with another three subsidiary companies, where all governance decisions and strategies are decided at the parent company. The quarterly meeting is conducted between subsidiaries and parent company to discuss issues and inputs including IS/IT security issues:

“CIO D: What will happen in the meeting, for Company D we have offices across Malaysia. We don’t focus Company D head office alone. Normally we do videoconferencing during the ISMC with all the major regional offices of Company D. One at Segamat, one in Kerteh, in Kerteh we have two videoconferencing sites, During the Company D ISMC meeting, all the regions shall give input as far as IT security issues are concerned and on any other ICT issues and direction. So at Company P Holdings level, we do have, at Company D level we also do have”.

6. “auditing IT policy”

Auditing policies and procedures relating to IS/IT security are important tasks to examine whether the internal controls of certain goals are achieved. Internal controls are used by organisations to measure whether some goals such as policies and procedures have been achieved or not, including the issues relating to IS/IT security. Only three companies have touched on the role of audit to check whether internal controls relating to IS/IT security are adequate or not, as identified in the 3rd Formal theme. For example, a senior manager of Company F:

“CFP F: Yes, because internal controls we would have preventive and detective controls and our audit department regularly review whether internal controls are in place whether there is any breach of the IT policy procedures security, whether any breaches in terms of the IT, and always check and balances”.

In another corporation, the discussion about internal controls application relating to IS/IT security was still general and did not mention specifically what IT areas are audited:

“CEO A:.. a key control checklist is developed and it sets out the various key controls and process requirements across all functions in the organisation and this includes any internal controls related to any IT/IS security matters. The key control checklist is reported regularly to the Audit Committee who assists the Board of Directors in reviewing the effectiveness of internal controls.”

In another case, even though the auditors play a significant role in auditing the implementation of IT security policies, this single approach does not guarantee to resolve security issues. Resolving people issues should require much more on preventive and automatic approaches compared with the detective and remedies approaches, as already discussed in Chapter 2. The following statement presents the case of Company E which Company E relied on detective and remedies controls rather than preventive approaches:

“CIO E: The IT/IS Security Policies are communicated to all levels of the staff in the company. Our Internal Auditors will audit the IT/IS Security Policies from time to time to ensure compliance and its adequacy. The same goes with our external auditors and also the Central Bank of Malaysia’s. Any weaknesses identified will be tabled to the IT/IS steering committee and the Audit Committee (Board Level) and mitigating actions will be taken. The IT/IS security policies will be reviewed every year to take account of the changing business, technology, operational, internal and external environment”.

7. “risk management”,

Risk management is the heart of corporate governance and IS/IT security governance is part of the corporate governance responsibilities. Risk management relating to IS/IT security should be taken care of by those organisations which strategically use IS/IT for supporting business operations and, therefore, minimising the IS/IT risks should be prioritised. A number of areas relating to risk management was identified from the Formal themes, including IS/IT security issues included in the risk management process and the IS/IT security issues included in the risk profile.

All eight organisations claimed that they included IS/IT security risks within the risk management process, as identified in the Formal themes. The data were presented by CEOs and came from Group A. For example, the CEO of Company G noted the important task in ensuring that the risks relating to software and hardware be identified, evaluated and mitigated to minimise any unintended/deliberate actions from both human and technological issues:

“CEO G: Yes. IT/IS issues are part of the business risk management plan. I need to ensure effective risk management process and System Development Lifecycle are in place of identifying, evaluating and mitigating critical IT risks covering both software and hardware aspects so as to maintain database confidentiality and system integrity”.

The CEO of Company G stated that his IT security vision, apart from ensuring confidentiality and system integrity, is also concerned with the availability of systems so that the business may resume without much disruption and potential losses:

“CEO G: And also I need to ensure the IT securities policies are in place and to be reviewed for effective disaster recovery process and business continuity management. The business operation to be resumed without major disruption and inconvenience caused to the customers, agents and policyholders”.

The data show that the general statement about IT was part of the organisation’s risk management activities in sustaining growth and enhancing shareholder value:

“CEO A: Like many other matters, IT related matters are also constantly reviewed as part of the organisation’s Enterprise Risk Management programme... Through this process, issues related to security of IT would be reviewed and included in the business risk management plan. ”

Three companies claimed that they had IT profiles in place but only one company provided details. Acquiring the data about IT profiles is significant in this study because this might indicate that organisations have IS/IT security governance in place. For example, the CIO of Company D presented some of the processes involved in ensuring that the IT risk profile worked and achieved the goal of risk management including continuous assessment, mitigation and maintenance:

“CEO D: The risk profile is developed by the team and discussed with the Risk Management Team. Risks are prioritized in the ICT profile by this team. ICT risk is one of the critical areas in which risk needs to be mitigated but needs to be assessed in the context of the risk profile. Corporate IT Development Unit regularly assesses ICT risk and our ICT risk”.

“CIO D: We have ICT risk profile which consists of security, planning, anything to do with ICT, Corporate IT Development Unit has a group actually developed and maintained and ensuring all the ICT profile risks which have been developed during the workshop attended by various OPUs over Company P Holdings for that profile to be addressed accordingly. So we do have ICT risk profile currently inside the Corporate IT Development Unit if you talking about ICT per se, if you talking about risk management per se for specific business, for any business in Company P Holdings, we do take account ICT. If there is a need which could jeopardize the business, then they will come in”.

The model of this study suggests that only certain issues would be brought up to governance level, the ones that cannot be resolved at the lower level due to certain causes (e.g., budget issues, lack of employee values).

8. “policy achievement and internal controls”.

Five companies mentioned the internal controls tools they use to measure the policy achievement and how far goals have been achieved. A number of forms of internal controls has been identified from Formal themes. For example, in Company A, a Control- Self- Assessment process was used for managing internal controls and risk management in the organisation:

“CEO A: Central to the organisation’s internal control and risk management system is its Control Self Assessment process which it has developed and continues to improve over time. The Control Self Assessment process is a process that we put in place as part of the organisation’s internal control and risk management system”.

A key control checklist was the example of internal controls used for IS/IT security matters to achieve the goal of the Control Self Assessment process exercised:

“CEO A: a key control checklist is developed and it sets out the various key controls and process requirements across all functions in the organisation and this includes any internal controls related to any IT/IS security matters. The key control checklist is reported regularly to the Audit Committee who assists the Board of Directors in reviewing the effectiveness of internal controls”.

Different organisations have different control tools to measure policy achievement. In Company D, the Service Level Agreement (SLA) was used as part of the internal controls mechanism:

“CIO D: We do have Service Level Agreement (SLA) with I-Pgroup. SLA is employed as part of our internal control mechanism. So SLA is actually covering services and others as well, services could be securities for example SPAM mail, this incident will be highlighted to I-Pgroup and IP Security Office (IPSO) will pick up this matter and try to resolve within the specific SLA. I think this month if I am not mistaken, they have to settle a few major issues within 3 working days and able to resolved this. So during ISMC meeting for COMPANY D level, for every quarter, we will ask them to present SLA report for that particular quarter.”

Another form of internal control mechanism is identified, namely, Key Performance Indicators (KPI) which may be used for measuring the informal aspect of employees. Two companies mentioned that they use KPIs for measuring the goal of informal factors:

“CIO E: Same as the formal factors and it is part of the KPIs of the relevant managers or department” and “CIO D:.. we’re talking about COMPANY D per se, we do enforce KPI for staff to take e-learning courses”.

8.4.2.1.4 Primary Issue: Monitoring

The next primary issue is monitoring, which refers to a reflective process, where the giver of the responsibility may detect, examine, fix or measure certain responsibilities/tasks to assess whether the holder of the responsibility has discharged the job effectively and efficiently. The responses were mostly in the formal themes and the least were found in informal themes. The majority of responses was identified in the Educational theme (Formal theme 8), some in the policy theme (Formal theme 1), security internal controls theme (Formal theme 3), organisational structure (Formal theme 5) but few were found in the committee theme (Formal theme 6) and there was a low response in all the Technical themes. There are three secondary issues identified from the Formal and Informal themes including monitoring actions, protection and policy achievement and internal controls. See Tables 8.6a and 8.6b.

	ISSUE		Source								
	Primary	Secondary		Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
				Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal Requirements/Regulation	Organisational Structure	Committee	Security Risk & its Management	Education ,training, seminar, orientation
4	Monitoring		A,B,C,D, E,F,G,H	11		4		5	2		18
		Monitoring Actions	A,C,D, E F G H	7		3		1	2		2
		Protection	B	2							2
		Policy Achievement & Internal Controls	D,E, F, G, H	2		1		4			12

Table 8.6a The primary issue of ‘monitoring’ and its secondary issues

	ISSUE		Source						
	Primary	Secondary		Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
				Techniques & Controls	System Development	Internet/ Network Security	Staff integrity/ ethicality /accountability	Culture, commitment	Human issues-lack of awareness, stupidity
4	Monitoring		A,B,C,D, E,F,G,H				1	1	1
		Monitoring Actions	A,C,D, E F G H				1	1	1
		Protection	B						
		Policy Achievement & Internal Controls	D,E, F, G, H						

Table 8.6b The primary issue of ‘monitoring’ and its secondary issues

8.4.2.1.4.1 Secondary Issues

Tables 8.7a and 8.7b show the sub -table about the secondary issues of Monitoring. The results of sub analysis will be presented in this section.

	ISSUE			Source								
	Primary	Secondary	Sub-Issue		Forma 1 Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
					Policy	Strate- gic vision & security import- ance	Secu- rity internal cont- rols	Comp- liance/ Legal Requi- rements/ Regula- tion	Orga- nisat- ional Struc- ture	Com- mittee	Security Risk & its Mana- gement	Educati- on, training, seminar, orienta- tion
4	Moni- toring	Monitoring Actions	Regular updates through meetings	A,C,D, E	√√√√							√
			Audit process by Audit committee	FC,E,D	√√√		√		√	√√		
			Reporting	G,B,H			√√					√
		Protection	Security controls-the use of Hardware appliance	B	√							
			Availability	F								√
			Complying with security policies	F	√							√
		Policy Achieve- ment & Internal Controls	KPIs	D,E								√√
			KRIs	E								√
			Check and balances	F			√					
			Using Gant Chart	G					√			
			Policy achievement	G	√							
			Tracking	E								√
			Report from IT Department	H,E,F	√				√√			√√
			Report from IT committee	F,H								

			Report from software Providers	F								√
			Subjective measurement	F,G								√√
			The way of interaction to each other	G								√
			Engagement between internal users and customers	G								
			Report from Human Resource	H,E,F					√			√√

Table 8.7a The sub analysis of secondary issues over the primary issue of monitoring

	ISSUE									
	Primary	Secondary	Sub Issue	Source	Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
					Techniques & Controls	System Development	Internet/ Network Security	Staff integrity/ ethicality /account-ability	Culture, commitment	Human issues- lack of awareness, stupidity
4	Monitoring	Monitoring actions	Regular updates through meetings	A,C,D, E						
			Audit process by Audit committee	F,C,E, D						
			Reporting	G,B,H				√	√	√
		Protection	Security controls-the use of Hardware appliance	B						
			Availability	F						
			Complying with security policies	F						
		Policy Achievement & Internal Controls	KPIs	D,E						
			KRIs	E						
			Check and balances	F						
			Using Gant Chart	G						
			Policy achievement	G						
			Tracking	E						
			Report from IT Department	H,EF						
			Report from IT committee	F,H						
			Report from Software Providers	F						
			Subjective measurement	F,G						
			The way of interaction to each other	G						
			Engagement between internal users and customers	G						

			Report from Human Resource	H,E,F						
--	--	--	----------------------------	-------	--	--	--	--	--	--

Table 8.7b The sub analysis of secondary issues over the primary issue of monitoring

1. Monitoring actions

In Tables 8.7a and 8.7b, monitoring actions refer to ‘regular up-dates through meetings’, ‘audit process by audit committee’ and ‘reporting’.

‘Regular up-dates through meetings’

According to four companies, a regular meeting is a form of action that was used for identifying and checking the progress of certain implementations. For example, the following statement provides ‘who’ is involved in the supervision process, such as between CEO and the Corporate IT Development Unit, between Corporate IT Development Unit and I-Pgroup:

“CIO D: The Board of Director and CEO monitor security policies through Corporate IT Development Unit. At the Corporate IT Development Unit level, they do have a monthly meeting with I-Pgroup, monthly meeting with I-Pgroup security teams, called it IPSO-IP security office, focusing on issues relating to IT security. ”

The giver of the responsibility should be able to supervise and consult the lower levels, the holder of the responsibility if some deficiencies occur. But, in most cases, the structure of supervision was too generic, the interviewees did not provide the specific information to the lower levels:

“CIO E: In terms of how do the Board and Senior Management monitor IT/IS security, the IT/IS steering committee meets every 2 months and the Audit Committee also meet every alternate month”.

‘Audit process by audit committee’

The data reveal that the audit committee plays a significant role in monitoring the IS/IT security implementation process, this action was demonstrated by four companies, as identified in the formal themes.

“CEO F: Yes, of course our internal audit always monitor whether we actually comply to whatever, even our internal security policies”.

Most of the responses have touched generic areas relating to the auditing process including the entities and internal controls but there were no further details about IT/IS security areas, such as:

“CIO D: And talking about Internal controls as well we do have audit, internal audit, we have our parent group internal audit department in Company P Holdings level, GIA, (Group Internal Audit) will do some checking, they will audit us, in fact, last financial year, December, we were audited by GIA, so they will cover everything with regards to internal control. Every year, we also have external auditors come in to Company D, this is Company D per se, in fact last external audit was done in January this year. So they (GIA) came in November, after they’re about to finish then our external auditor came in. So last financial year, we were quite busy with audit, the internal and external auditors came simultaneously, so they will cover everything, so far we don’t have any issues.”

‘Reporting’

Reporting is another area of monitoring action. Three companies stated that the reporting activity was part of the monitoring process. Among the three companies, the CIO of Company B has given a lower level example how the report was used for monitoring purposes.

“CIO B: I have two teams of IT people. One group looks after infrastructure (network, internet, desktop, security, data centre) and another group prepares a monthly report to me. The team is alerted hourly on potential breaches of security. Normally, we do give the report to the CEO because it is a relevant control. We do give the CEO the report of the spam, number of spam comes in, every Monday we give him, say last week how many spam comes in, this week how many, just a summary, I can show it to you on the computer.”

2. Protection

One goal of monitoring is protection, referring to software and hardware. It was found that one company used hardware to monitor including to stop and block suspicious and unintended activities by employees:

“CIO B: To monitor the policy and procedures, we have security controls in place to identify breach of policy, let us say the internet policy. We also have a hardware appliance that allows us to block access to websites we do not wish staff to access”.

3. policy achievement and internal controls

The final monitoring action identified is the policy achievement and internal controls, mainly identified in the Formal themes. Five companies used several tools/methods and sources of information from several parties as part as their internal controls and policy achievement. In measuring the policy achievement only three companies have used tools/methods as part of their internal controls such as Key Performance Indicators (KPIs) as identified:

“CIO E: To monitor the implementation of informal aspects, we use Key Results Areas (KRAs) and KPIs. KRAs and KPIs will be set and Action Required (AR) will be assigned. Daily or weekly or monthly or quarterly reviews or meetings with relevant managers or departments.”

The Gantt Chart is used by Company G for measuring and monitoring the milestones and achievement, as identified:

“CEO G: By using the Gantt Chart, we know what we have done and what sources we need.”

Tracking IT projects using implementation methodology was identified:

“CIO E: In any case, we do follow a proper project implementation methodology where a Project Plan will be developed and there will be ongoing tracking and monitoring. Prior to the implementation stage, the project’s objective would have been defined and the IT/IS Committee would have to approved it. Of course the budget would have to be approved too.”

While four of the five companies used sources from parties and individuals for policy achievement and internal controls such as the interview statement, one CEO mentioned that monitoring includes sources from various entities--unit/department, software providers and databases:

“CEO F: Monitoring is undertaken through Audit Team, IT team (Our Firewall Alert System), Software Providers and HR (to our Payroll System, Plantation Management System, FRS, Human Resource Information System) and also Task Force”.

The Human Resource department plays a role in IS/IT security implementation, three companies mentioned the monitoring process by Human Resources, for example,

“CEO H: We monitor the goals of policy relating to informal aspects based on the reports from the Human Resource department, IT department and IT committee.”

8.4.2.1.5 Primary Issue: Shared roles in security issues

The other primary issue is related to shared roles among the employees across departments/units, as can be seen in Tables 8.8a and 8.8b. There was no information related to operational levels or lower level involvement in shared roles. The data were general, not specific. All the responses were formal themes, the majority identified in the organisational structure (Formal theme 5) and little in the policy (Formal theme 1) and security internal controls (Formal Theme 3).

	ISSUE		Source	Themes							
	Primary	Secondary		Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
				Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal Requirements/Regulation	Organisational Structure	Committee	Security Risk & its Management	Education, training, seminar, orientation
5	Share roles		C,D,F,G,H	1		1		12			
		Technical role	F,G,H,C,D					7			
		Governance role	C,D,F	1		1		5			

Table 8.8a The primary issue of ‘share roles’ and its secondary issues

			Source							
	Primary	Secondary		Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3	
				Techniques & Controls	System Development	Internet/Network Security	Staff integrity/ethicality/accountability	Culture, commitment	Human issues-lack of awareness, stupidity	
5	Share roles		C,D,F,G,H							
		Technical role	F,G,H,C,D							
		Governance role	C,D,F							

Table 8.8b The primary issue of ‘share roles’ and its secondary issues

8.4.2.1.5.1 Secondary Issues

Tables 8.9a and 8.9b will provide sub-analysis on secondary issues relating to the primary issue of share roles.

	ISSUE			Source	Themes							
	Primary	Secondary	Sub-Issue		Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
					Policy	Strategic vision & security importance	Security internal controls	Compliance/ Legal Requirements/ Regulation	Organisational Structure	Committee	Security Risk & its Management	Education, training, seminar, orientation
5	Share roles	Technical role	Technical Roles	F,G,H, C,D					√√√√√			
			Services focus	C					√			
			Security Controls	F					√			
		Governance role	Governance focus	C,D					√√			
			Understand Business goals	F	√		√		√			
			No interference to each other	C					√			
			Using the same language	D					√			

Table 8.9a The sub analysis of secondary issues over primary issue of 'share roles'

	ISSUE									
	Primary	Secondary	Sub-Issue	Source	Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
					Techniques & Controls	System Development	Internet/ Network Security	Staff integrity/ trust/ ethicality /accountability	Culture, commitment	Human issues-lack of awareness, stupidity
5	Share roles	Technical role	Technical Roles	F,G,H, C,D						
			Services focus	C						
			Security Controls	F						
		Clear governance role	Governance focus	C,D						
			Understand Business goals	F						
			No interference to each other	C						
			Using the same language	D						

Table 8.9b The sub analysis of secondary issues over primary issue of ‘share roles’

Two secondary issues were recognised: technical roles and governance role, identified from formal themes. When asked their opinions relating to this issue, shared roles in security issues between their department and another department, the representatives of five companies said it was not an issue because each party has its own requirements and obligations.

1) Technical roles

In terms of the technical roles, one example was identified:

“CEO F: No, no problem in sharing technical roles with others, I think the technical here referring here to only the IT. No, we don’t have problems, because the IT people themselves are aware of the requirements. So you talk about business goals and security controls, and referring to the corporation, so if they understand what are the goals, get themselves involved in preparing our policies, then it should not be a problem. Let us say, you just come in, we have policies, we have internal controls and

all that, and we have compliance procedures, I don't think, any employees would not somehow cooperate either".

2) Governance role

With regard to the governance role, two CIOs were involved in IS/IT security governance. It is important to highlight that both CIOs came from the top 50 publicly listed companies in Malaysia. According to the CIO of Company C, his department is dealing with governance and services:

"CIO C: We don't have problems in sharing roles with others. The ICT roles are governed by my department. We don't interfere with each other. In this corporation we do both, governance and services. Many security issues have been identified during the services process."

However, the second CIO said that his department deals with the governance role only and does not provide services because the IT services have been out-sourced to a third party.

"CIO D: Again, I think our role is basically, we are doing the governance, we are not doing services, because for services we have outsourced to the third party. In terms of technical, it's not a technical role I am holding, I am more holding the governance role".

8.4.2.1.6 Primary Issue: Security Issues and Budgets

The primary issue, security issues and budgets, are two important elements of the IS/IT security governance study. Budgets may be approved after the organisation has a clear IT vision and security goals requirements. In IS/IT security governance, security controls/solutions will be provided according to the needs of the IT vision, where the aim of the IT vision is to provide the technological resources based on business needs. The responses were identified mainly from all the technical themes and some identified in the 2nd formal theme: strategic vision and security importance. See Tables 8.10a and 8.10b. Only four companies provided information relating to IS/IT security issues and budget approval from the board.

	ISSUE		Source	Themes							
	Primary	Secondary		Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
				Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal Requirements/Regulation	Organisational Structure	Committee	Security Risk & its Management	Education, training, seminar, orientation
6	Security issues & Budget		B,C,D,E		17						
		Protection & Business Assets	B, C,D,E		12						
		Protection & Security Controls	B, C,D		5						

Table 8.10a The primary issue of ‘security issues and budget’ and its secondary issues

			Source						
	Primary	Secondary		Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
				Techniques & Controls	System Development	Internet/Network Security	Staff integrity/ethicity/accountability	Culture, commitment	Human issues-lack of awareness, stupidity
6	Security issues & Budget		B,C,D,E	18	1	15			
		Protection & Business Assets	B, C,D,E	12		10			
		Protection & Security Controls	B, C,D	6		5			

Table 8.10b The primary issue of ‘security issues and budget’ and its secondary issues

8.4.2.1.6.1 Secondary issues

When asked about the security issues included in the corporation’s budget, four companies provided examples of security areas covered in the budget. In this analysis, two secondary issues were identified; security vision/IT vision and security controls.

1. Security vision/IT vision

In regard to security vision, one specific example was gained from the CIO of Company C who explained the need for security counter-measures in place for securing the IT architecture:

“CIO C: Security issue included in the budget is network management issue. There are two problems with thumb drive, first information security and second how much information is being copied from thumb drive. To resolve thumb drive issue we use firewall, operating systems are firewalled.”

Even though the question was asked about the IS/IT security vision, the CIO provided the background of the budget relating to IT infrastructure and the IT budget. The statement by the CIO of Company B shows that their organisation has special capital for IT.

“CIO B: Yes the IT budget is approved by the board. Normally we do yearly for IT budget request, say, what I plan to do, how much I need to spend, how much I recover for it, for example, 1.5 million, we got to justify, if the board agrees. Normally, my budget is not so big, unless I introduce new systems, applications, for infrastructure I done it years ago, now no need to, just basic maintenance”.

2. Security controls

Security vision and security controls are inter-related because the counter-measures/controls are based on the direction of the security vision, this lead to a single interview statement which may reflect more than one issue, as shown in Tables 8.11a and 8.11b. For example, two companies used firewalls Company C and Company D, in protecting their IT architecture. Company D used security counter-measures such as firewall and anti-viruses to protect their applications (e.g., internet) and infrastructure and both of the counter-measures were included in the yearly budget.

“CIO D: Yes, we have, for example, the firewall. When you’re talking about security issues it should involve infrastructure as well as the application. Yes, internet and antivirus are also part of the security issues included in the budget, we do have an agreement with the service provider, every now and then antivirus is up-dated and distributed across. And this is being budgeted on a yearly basis”.

	ISSUE			Source	Themes							
	Primary	Secondary	Sub-Issue		Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
					Policy	Strategic vision & security importance	Security internal controls	Compliance/ Legal Requirements/ Regulation	Organisational Structure	Committee	Security Risk & its Management	Education ,training, seminar, orientation
6	Security issues & Budget	Protection & Business Assets	Safeguard Network & IT architecture	C, D, E		√ √ √						
			Confidentiality	C, E		√ √						
			Information security	C, E		√ √						
			Integrity	E		√						
			Audibility	E		√						
			Board approval	E, B		√ √						
			New systems/ applications or basic maintenance	B		√						
		Protection & Security Controls	Firewall	C,D		√ √						
			Internet	D		√						
			Antivirus	D		√						
			Agreement with service provider	D		√						

Table 8.11a The sub analysis of secondary issues over the primary issue of ‘security issues and budget’

	ISSUE			Source	Themes					
	Primary	Secondary	Sub-Issue		Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3
					Techniques & Controls	System Development	Internet/ Network Security	Staff integrity/ ethicality/ accountability	Culture, commitment	Human issues- lack of awareness, stupidity
6	Security issues & Budget	Protection & Business Assets	Safeguard Network & IT architecture	C, D, E	√ √ √		√ √ √			
			Confidentiality	C, E	√ √		√ √			
			Information security	C, E	√ √		√ √			
			Integrity	E	√		√			
			Audibility	E	√		√			
			Board approval	E, B	√ √	√	√			
			New systems/applications or basic maintenance	B	√					
		Protection & Security Controls	Firewall	C,D	√√		√√			
			Internet	D	√		√			
			Antivirus	D	√		√			
			Agreement with service provider	D	√		√			

Table 8.11b The sub analysis of secondary issues over the primary issue of ‘security issues and budget’

8.4.2.1.6.2 Summary

The primary issue of ‘security issues and budgets’ was discussed in two secondary issues; first was ‘protection and business assets’; and second was ‘protection and security controls’. The primary issue was mainly identified in the formal theme and technical theme, there were no data available in the informal themes.

Part 3

8.5 Relating the data to IS/IT Security Governance Model

In Part 3, the data reported in Part 2 are matched to the IS/IT Security Governance Model developed in chapter 4. Part 3 comprises a number of themes similar to the themes developed in the IS/IT Security Governance Model. The themes identified in the IS/IT Security Governance Model are linked to the issues noted by interviewees to build a rich picture of IS/IT security governance.

8.5.1 Themes of the Model of IS/IT security governance and Research Questions

In the IS/IT Security Governance Model eight major themes were identified across the three components. Themes of the model are different to the themes identified in the manual content analysis and in the Leximancer software analysis. In the Formal component, the four themes underling this component were IS/IT Security Vision, IS/IT Security Management Strategy, IS/IT Security Policy and IS/IT Security Standards. The Technical component comprised two themes, Technological Areas and IS/IT Security Procedures. The Informal component consists of two themes, Organisational Values and Employee Values.

The issues identified in the interview are broken into three primary issues. The primary issues identified from the interviewees were Business Needs, Implementation and Monitoring. Business Needs refer to the development of IS/IT security elements in the three components such as vision, policy, management strategies, procedures, commitment and roles. Implementation is concerned with the IS/IT security processes and Monitoring is the process of ensuring the effectiveness and efficiency of the IS/IT security processes. The sequence of discussion will be case by case because every single case is different.

In Part 3, the research questions are important for determining the analysis technique to be used. In analysing the data, two techniques were needed. The first was across-cases analysis and the second was single-case analysis. The across-cases analysis will be used to answer Research Question 1 because the objective of the Research Question 1 was to discover the evidence over the development of IS/IT security aspects with regard to the Formal, Technical and Informal components.

The single- case analysis technique will be employed to achieve the objectives of Research Question 2, where the research study is analysing the interaction of components within a single case. The single -case technique reveals the complexity of the component interactions.

a) Formal Component Themes

The Formal component describes themes that are concerned with the development of formal governance structures of IS/IT Security indicating the involvement of the board and senior management in IS/IT security. The Formal themes identified from the IS/IT Security Governance Model in Chapter 4 were IS/IT Security Vision, IS/IT Security Management Strategy, IS/IT Security Policy and IS/IT Security Standards.

The first Formal theme, IS/IT Security Vision, identifies the relationship between the IS/IT security needs and technological business requirements in order to achieve the strategic vision and objectives of the organisation, in particular to minimise operational business risk.

The second Formal theme identifies the strategies relevant to the nature of business, availability of resources, organisational culture and environment. There were four sub themes identified underlying the IS/IT Security Management Strategy theme, these include Security Risk Management, Security Internal Controls, Committees and Education, Training and Awareness Programme.

- Firstly, the first sub theme, Security Risk Management identifies if the IS/IT security issue was discussed and was part of the corporate risk management plan. This sub theme also looks into the development of risk identification, assessment and mitigation processes in order to minimise operational risk and to ensure strategic vision and objectives are accomplished effectively. Apart from that this sub theme examines the examples of security issues provided by the participants.
- The second sub theme, Security Internal Control, identifies if internal control had been applied within IS/IT security areas. This theme particularly identifies the internal controls application by corporations over the IS/IT Security Policies and IS/IT Security Procedures.
- The third sub theme, Committee, identifies whether committees play a significant role in the directing and monitoring of IS/IT security. Committees identified in this framework were IT committee, Risk Management Committee and Audit Committee.
- The fourth sub theme, Education, Training and Awareness Programme, looks at the development of Formal strategies relating to human needs. These Formal strategies are important for the development of Informal component including Organisational Values and Employees.

The third Formal theme “IS/IT Security Policy” identifies whether corporations have IS/IT security policies in place and also identifies the policy development areas. The IS/IT Security Policy is an important Formal component because its primary objective is to achieve the IS/IT Security Management Strategy and leads to the implementation of IS/IT Security Procedures.

The fourth Formal theme of IS/IT Security Standards identifies if corporations need to comply with any standards relating to IS/IT security. There were two types of standard: internal standards developed by organisation and external standards developed by official bodies nationally or internationally or industry requirements in regards to IS/IT security. The IS/IT Security Standards may help boards and senior management in the directive processes relating to IS/IT security matters such as IS/IT Security Policy or IS/IT Security Procedures.

b) Technical Component Themes

The Technical component describes themes related to the development of the Technological Areas and IS/IT Security Procedures. The Technical component is a realisation of the Formal component derived mainly from the IS/IT Security Vision, IS/IT Security Management Strategies, IS/IT Security Policies or IS/IT Security Standards.

The Technological Areas theme identifies if the corporation used the IT infrastructure, business data and business information systems for achieving business operations. This theme also examines the use of the emergent technologies by corporations such as wireless and mobile internet. The wide use of wireless technologies and mobile internet exposes the corporation's private network to threats and vulnerabilities, if not managed effectively and efficiently by the Board and Senior Management. The Technological Areas theme is important as it identifies the potential risk areas for the development of the second theme, IS/IT Security Procedures.

The IS/IT Security Procedures theme looks at the development of IS/IT security software, hardware or security solutions which provides the IS/IT security steps or processes for achieving the Technological Areas. The IS/IT Security Procedures are designed to enforce certain security controls on particular domains or platforms in order to achieve the security policies or related requirements. The theme also identifies the inclusion of security controls if the corporation has used the Internet, wireless technologies or mobile internet for supporting business operations.

c) Informal Component Themes

The Informal component reflects themes embracing people and human aspects in regards to the implementation of IS/IT Security Policies and IS/IT Security Procedures. There were two types of Informal component, Employee Values and Organisational Values. The Employee Values theme concerns the personal and ethical values of employees, while the Organisational Values theme relates to structures of responsibility held by employees derived from the Formal component such as the IS/IT Security Policy and the Technical component such as the IS/IT Security Procedures.

The contemporary processes of IS/IT security not only preserve the confidentiality, integrity and availability of the IT systems but also engage people and human aspects such as commitment and involvement of the board and senior management, culture and norms, responsibility of employees, people's integrity and trust. The Board and Senior Management should play role in cultivating the security culture by integrating people and human aspects within the Formal component (IT/IS Security Policies) and Technical component (IS/IT Security Procedures).

8.5.2 Data Analysis and Research Questions

The analysis used depended on the Research Questions and Research Objectives. To answer Research Question 1, the multiple cases analysis technique was used to find as much information relating to IS/IT security aspects across cases. The second technique, single-case analysis was used to answer Research Question 2, to study and validate the model of component interaction within a single case study.

8.5.2.1 Data Analysis and Research Question 1

The statements of the issues of each company were analysed and related to the associated themes. The development of IS/IT security aspects with regard to the Formal Component Themes, Technical Component Themes and Informal Component Themes within the companies will be presented.

8.5.2.1.1 Formal Component Themes

a) IS/IT Security Vision

IS/IT Security Vision is the first layer of the Formal Component that needs to be established to achieve the IS/IT Security Governance Model. The IS/IT Security Vision was very important to define because it identifies the critical resources including the IS/IT assets and business data which have potential risks to business and need to be secured. Understanding the vision enables the board and senior management to provide effective management strategies in order to achieve it.

In the case of Company A, IS/IT facilities were used for supporting the business operations, that is why the security over its IS/IT facilities and business data also need to minimise any unintended risks.

“Like any other business organisation, Information Technology (IT) facilities are important to Company A Malaysia. Company A Malaysia is dependent upon the continued availability, integrity and confidentiality of the services provided by its IT facilities for the successful operations of its business and the protection of its business information. Hence it is important for the IT facilities to be secured for these purposes (CEO, Company A)”.

Company F utilised the business information systems for supporting integration of departments and functional areas of the organisation and also the entire organisation. The protection over the business information systems resources and business data need to be prioritised,

“Our corporation is highly dependent on IT and most of our systems are electronically digitally get up, I mean we have IT on our Finance Integration of Financial Statement Information Accounting, we have Integrated Financial System which is linked very closely with our Plantation Management System. And also linked directly to our Human Resource Information Systems (HRIS). So among the three of this, software and the systems we have used for accounting systems will be used directly for reporting in our corporation. Data that this transmitted to and for these systems - HRIS, Accounting, Plantation includes mail, engineering and all these are highly confidential. (CEO, Company F)”.

The primary goal of IS/IT Security Vision is to safeguard the IS/IT resources and business data. The IS/IT Security Vision needs to be correspond with the risk level of the IS/IT resources and business data in supporting the business operations. In the case of Company G, even though some of the business processes are still automatic in parts, the management still had a clear IS/IT Security Vision and risk management strategy in place.

“In our business, some processes like transactions are automatic in parts. If certain parts are IT based, security is very important to this corporation. If the online based systems compromised, the business will

resume and risk management plan like disaster recovery process and business continuity strategy will take place to restore necessary data (CEO, Company G)".

Securing the business data was part of business requirement in the following case,

"Security is important because information is an invaluable assets of the company for the management to understand the operating environment, making the correct decision and hence gain a competitive advantage in the business world. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement (CEO, Company H)".

b) IS/IT Security Management Strategy

In achieving IS/IT Security Vision, strategies need to be formulated in accordance with the nature of business, availability of resources, organisational culture and structure and also the environment in which it operates. The data have revealed two main IS/IT Security Management Strategies, Risk Management and Internal Controls.

c) Risk Management

Risk management strategy was used by participants to identify, assess and mitigate risks relating to IS/IT. IS/IT Security issues were seen as important as other business risks. For example, IS/IT security issues were included as part of the risk management plan.

"Like many other matters, IT related matters are also constantly reviewed as part of the organisation's Enterprise Risk Management programme. This includes the system recovery issues, information security issues and others. Through this process, issues related to security of IT would be reviewed and included in the business risk management plan. And the other comment related to the inclusion of IS/IT risks within the risk management plan, "IS/IT security issues is part of Risk Management Plan. We have a security unit. We set up a governance unit, before this governance is part of planning". (CIO, Company C).

After identifying which technological areas need to be secured, the management headed by the Risk Management Team outlined the strategies to achieve its IS/IT Security Vision,

"Subsequently, the Risk Management Team will coordinate the development of risk mitigation action plans, develop and update business continuity plans for key business risks, plan and coordinate the testing of business continuity plans, organise training and education for employees on risk management and monitor the results of key performance indicators." (CEO, Company A)

In the IS/IT Security Governance Model, the IS/IT security risks were the responsibilities of the board and senior management.

"IS/IT issues are part of corporation risk management plan. I need to ensure effective risk management process and System Development Lifecycle are in place of identifying, evaluating and mitigating critical IT risks covering both software and hardware aspects so as to maintain database confidentiality and system integrity". (CEO, Company G).

IS/IT Security issues were included in the Risk profile of the company, to demonstrate the state (e.g., low, medium or high risk) of the specific issue and subsequent strategy to be undertaken,

“IS/IT is issue is part of risk management plan and incorporated in our risk profile, regularly we update our profile. In this risk profile actually we define the state of IS/IT security issues and we find out what would be the actions taken”. (CEO, Company F).

The other function of Risk Profile was to record all information with regard to IT and security issues,

“Ok we have a Risk Profile for Company D. When talking about IT security, in coming up with the Risk management Plan or risk profile, we need to record everything, including IT and other security issues”. (CIO, Company D).

The identification of security issues was a part of risk management process. Different corporations have different approaches in terms of channels or organisational structures used for identifying and managing their security risks. According to the IS/IT Security Governance Model, the risks need to be identified from the use of Technological Areas and Business Information Systems as aligned with IS/IT Security Vision.

The security risks can be identified from the users or owner of the system,

“These IS/IT security issues, if any are highlighted by the risk owners within the respective department, are referred to the Risk Management Unit meeting or Risk Management Committee meeting for discussions and solution. They will be recorded in the risk registers if deemed necessary”. (CIO, Company H).

Risk assessment and mitigation was handled by the Risk Management Committee. Security issues can be identified through IT committees where the issues will be brought by the Head of Division for assessment and mitigation actions,

“We do have IT steering committee. We have four committees that look overall issues- Divisional Management Committee (overall issues), Division Planning Committee (specific issues), Operation Technical Committee (OTC) (operation issues) and Divisional Risk Committee. So if we have IT or security issues, we discuss with Division Planning Committee. The security issues are identified through the Divisional Officer during the Council Meeting, at the forum and through committee.” (CIO, Company C).

Interestingly, IT staff and non-IT staff were involved in the security risk identification process to ensure the decision on business risks was according to standards and aligned with policy,

“These security issues are identified mainly by the IT staff with assistance from Business Security staff in Company A Malaysia. They ensured that the decisions were appropriate to the business risks, measured against industry best practices and sat within Company A Malaysia’s existing governance and policy structures wherever possible”. (CEO, Company A).

In some cases, like the subsidiary reporting to the parent, the decision process on IS/IT security still depends on the directions provided by the parent company. If the security issues cannot be managed at the subsidiary level, the process had to be brought up at the parent company level. The

parent company has authority over its subsidiaries. The following case is identified as a subsidiary depending on the parent company for some major directions,

“Indirectly y since the policy and procedures was crafted at Corporate IT Development Unit level so in a way we have to be liaising a lot with Corporate IT Development Unit, getting some directions, some inputs, some recommendation, of course we make some decisions as well, of course when come to certain issues, if we think it warrant to be brought up to Corporate IT Development Unit we will, same goes to any security issues, we think if we can manage at our own level with I-Pgroup, we will do that”. (CIO, Company D).

Responsibility for IS/IT security risks is shared between the senior managers, heads of department or junior managers from all sections through the Risk Management process.

“These issues are identified through the organisation’s Enterprise Risk Management process whereby the Risk Management Team headed by the Finance Director and comprising senior managers from all departments in the organisation including IT, will conduct quarterly reviews of the business risks as part of their responsibilities”.(CEO, Company A).

During the risk identification activity, security risks relating to IS/IT can be identified from many sources including personnel, management group, management levels or committees, to identify risk areas. The security issues comprised various elements from people issues, to management issues in IS/IT security implementation, to natural disasters. Following is some of the evidence of security issues found across cases. Social issues include,

“virus attack, hacking, sabotage, poor access control (CEO, Company H)”. The identified management issues were “lack of proper backup facilities, inadequate or outdated hardware or software (CEO, Company H)” and “network management (CIO, Company C)”.

Before risk mitigation takes place, risk analysis and assessment activity need to be conducted to provide the state of the potential risk areas and their relative importance. The risk mitigation activity concerns the action plan and contingency planning in response to identified risks. The mitigation process involved IS/IT security counter-measures and controls and requires strong financial support from the board and senior management. For example, in some cases security issues have been accounted for within the IS/IT budget.

“Mainly security issues included within the budget include IT training, routine expenses to maintain IT security like anti- virus, anti-spam control, firewall and updates (CIO, Company H)”.

“Security issues included within the budget-unauthorised access, disclosure, modification, destruction and theft”. (CIO, Company E).

As commented by CIO Company D:

“..internet and antivirus are also part of the security issues included in the budget, we do have agreement with the service provider, every now and then antivirus is updated and distributed across. And this is being budgeted on yearly basis.”

The findings indicate some of the Boards of Directors and Senior Management gave a strong support in mitigating business risks relating to IS/IT.

d) Risk Management and Internal Controls

The IS/IT Security Governance Model highlights that internal controls are part of the risk management process. The model considers three main stages of risk management activities; risk identification, risk analysis and assessment, and risk mitigation. The model identifies internal controls had inter-related processes with the third stage, risk mitigation, concerned with the action plan in response to identified risks. Internal controls can be placed within the risk mitigation process by establishing IS/IT security internal controls such as password controls, security reports, audit reports, virus scanning reports, log reports and security technical reports. To capture the real world views, interviews examined the IS/IT security internal controls used by organisations to mitigate risks.

Security internal controls can be divided into four types, deterrence, preventive, detective and remedy controls. Deterrent applies a passive approach likes policy and security awareness. Preventive uses an active approach such as password controls. If the preventive control has been ignored, the detective countermeasures will take place such as security reports or virus reports. The remedy control can be used if all of these three controls fail such as termination and warnings. One company used preventive and detective controls as part of achieving security internal controls,

“internal controls we would have preventive and detective controls and our audit department regularly review whether internal controls are in place whether there is any breach of the IT policy procedures security, whether any breaches in terms of the IT, and always check and balances”. (Chief Financial Planner, Company F),

IS/IT security internal controls may vary. One participant mentioned the security internal controls used in his organisation were hardware control and password control. Both types of control were considered as preventive controls to mitigate the security risks,

“To monitor the policy and procedures, we have security controls in place to identify breach of policy, let say the internet policy. Internal controls are in place to alert us to security breaches. We also have a hardware appliance that allows us to block access to websites we do not wish staff to access. Our controls are mainly related to intrusions – the machine shuts down on a third attempt to intrude. We have in place a password security system and user verification process (CIO, Company B)”. (CIO, Company B)”.

Similarly, the use of password counter-measures for security internal controls were used in another corporation.

“Safeguarding sensitive information is our risk management plan to ensure our IS/IT information such as Balance Sheet, Accounting and Reporting System, MIS, Accountable Budget, other Accounts, Future Profit of Company and Forecasting Information of Market Share Price are not stolen by hackers and disgruntled employees. That is why password protection is part of our internal controls. If this is not addressed, our sensitive information might be published by irresponsible people and ultimately damaging our corporation’s name due to weak security systems” (CEO, Company F).

The detective control, the key control checklist, was identified as a security internal control used for reviewing effectiveness of the IS/IT security implementation,

“a key control checklist is developed and it sets out the various key controls and process requirements across all functions in the organisation and this includes any internal controls related to any IS/IT security matters. The participant worked closely with the Audit Committee in reporting the results of key control checklist, “The key control checklist is reported regularly to the Audit Committee who assists the Board of Directors in reviewing the effectiveness of internal controls” (CEO, Company A).

Another detective control, audit report, was used for reviewing the effectiveness of the IS/IT security procedures,

“Internal controls will provide reasonable assurance that the IS/IT security procedures are complied with e.g. regular audit by internal auditors”. (CIO, Company H),

The successful implementation of internal controls over IS/IT security policy was shaped by people’s desired mind-sets and behaviour as the following comments by the CEO of Company G:

“The role modelling desired mind-sets and behaviour are important aspects to achieve internal controls in the implementation of IS/IT security policies and procedures”.

Internal controls are a mechanism that can be used by IT Group, Risk Management Group and Internal Audit Group to ensure the IS/IT security policies and procedures are complied with.

“we do have internal controls to ensure the goal of IT security policies are implemented as intended. Internal Risk Team, Internal Audit Team and IT Team are working together for achieving compliance for the user group.” (CEO, Company G).

“CIO D: We do have Service Level Agreement (SLA) with I-Pgroup. SLA is employed as part of our internal control mechanism. So SLA is actually covering services and others as well, services could be securities for example SPAM mail, this incident will be highlighted to I-Pgroup and IP Security Office (IPSO) will pick up this matter and try to resolve within the specific SLA. I think this month if I am not mistaken, they have to settle a few major issues within 3 working days and able to resolved this. So during ISMC meeting for COMPANY D level, for every quarter, we will ask them to present SLA report for that particular quarter. At that juncture we should know if there is incident of security or anything and how fast the response and the mitigation process, it will be highlighted during that meeting and of course we’re talking about SLA, and as external party that dealing with our service of course they have to meet certain SLA, if there is any variance, let say they have to meet 90% SLA, if there is variance lower or the difference , for example for that particular quarter they only achieve 70%, then they have to explain why, to the committee, and this covers IT security and anything. If there are late in rectifying the problem, they have to explain if they don’t meet the SLA”.

e) IS/IT Security Policy

The IS/IT Security Policy document is a platform for communicating the board’s IS/IT Security Vision and the IS/IT Security Management Strategy. Basically, IS/IT Security Policies are statements designed to maintain the security of IS/IT assets and business data in terms of confidentiality, integrity

and availability. The existence of IS/IT Security Policy indicates the commitment of senior management to IS/IT Security.

IS/IT security policy, like all other policies, involved the board of and senior management. It was identified the senior management headed by CEO, IT group and Auditors were involved in the formulation and implementation of policy relating to IS/IT security.

“The management headed by myself, and of course the IT department and the internal audit involved in the formulation of IS/IT security policy(CEO Company F).

Policy areas covered in the organisation depended on the direction of IS/IT Security Vision,

“We have number of policies and procedures here, you may want to have a look the major headline of policies relating to IS/IT security- System information access control, Physical and environmental security, Network management, Back up and restoration, System back up and ownership, IT system change management, Problem management and IT system capacity management (CEO Company F)”.

Other examples of IS/IT security policies are presented. The CEO of Company A highlights the security issues areas of policy covered in his corporation:

“The security issues that are included here in the policy are related to network connectivity, account management, vulnerability management, secure system development, incident management, host protection and authentication”.

As reported by CIO of Company B:

“We have five basic security policies that cover backup, internet use, email use, desktop appearance and data classification.”

The CIO of Company D shows his security policy includes mobile:

“For security areas, it covers everything, email policy, information security, I mean in terms of what kind of information you can disseminate, in terms of you labelling the information, confidential, secret, internal use, and then desktop management inclusive, network, mobile. Mobile is formed under baseline, because security, inside a lot of items there, a lot of things, desktop baseline, quite several of baselines, very extensive in terms of (the area covers). We have also internet policy. In which it mentioned, all the internet facilities are meant for company purposes. In fact some of the non-business related sites are being blocked for staff to access”.

As noted by CEO of Company G:

“the security policy covers issues like access, return to operation (system down) and acceptable run time.”

8.5.2.1.2 Technical Component Themes

There are two important layers of the Technical component, Technological Areas and IS/IT Security Procedures. The Technological Areas layer identifies the IS/IT areas, which have potential risks to business; it has two inner layers, 1)IS/IT Infrastructure and business data, and 2)business

information systems. The IS/IT Infrastructure provides the foundation for all organisation's systems such as IT components and IT services including software and hardware. Specifically, business information systems support integration of parts between department and the entire organisation to achieve the business goal. The IS/IT Security Procedures layer provides security counter-measures and controls over the identified Technological Areas.

The Technical component is illustrated in the following case, Company D, a subsidiary of company, Company P. The first layer of Technological Areas identified that the IS/IT computer server of Company D was in the state of risk because the patches level for all servers between subsidiaries and parent were not standardised,

"What will happen, our server basically scattered in our offices in Malaysia, a lot of servers, the patches level are not standard (not the same) COMPANY P3 at this level, Company P2 at this level".

Thus, this may expose the computer server to various threats,

"so when the patches level is not the same, we expose the server from external/internal threat, this coming from ICT security point of view". (CIO D, Company D).

To mitigate the risks, security countermeasure has been implemented in the Company D to heighten the security of business data,

"We have project in ICT patches alignment to standardize patches for all servers. Because of that, we decided to embark on this".

Company D is connected to its internal employees through some group IT applications and related business information systems. Security issues start to arise when an employee leaves the corporation, where they still have access to some IT systems because the removal process of the IDs of the IT systems and business information systems was incomplete. ,

"when any staff resign or retire, let's say they have seven IDs, ID for SAP is different, MS Exchange is different.. Currently we really have to look at the registration, if they have 8 IDs, we have to remove 8 IDs".

Failure to remove all the IDs after resignation has exposed the corporation to external risks such as theft, data modification or alteration, malicious attacks or virus infection. To mitigate the security risks, IS/IT Security Procedure will be established. Company D has taken steps to develop a system,

"they called it IT Access Management whereby if let say a staff resigned instead of filling a lot of forms for ID, if the staff is confirmed resign by HR, we just use the system, all IDs automatically removed, regardless where. So we don't need, to do all the listings which you tend to miss out a few things".

Through the IS/IT Security Procedure, the system will automatically detect and remove all the IDs of a departing employee.

"With this initiative at the group wide level once the staff resigned the system will removed everything. That's being done by I-Pgroup and applicable to group wide. When staff resigned, the removal process

shouldn't be focusing on taking out Local Area Network ID only, also have to take out all the other IDs.. Instead of doing that".

The Technological Areas layer involves the continuous identification of security risk over the IS/IT infrastructure and business data. The risk identification is crucial for IS/IT security because it deals with human actions and reactions. According to the CIO of Company C, the freedom to use the external hard drive (e.g., Pen drive) may create problems.

"There are two problems with thumb drive, first information security and second how much information being copied from thumb drive".

The use of external hard drive by employees risks the network infrastructure and exposes critical business data if no security controls are applied. So, the IS/IT Security Procedures was established in Company C to provide security counter-measures over the end-users point security,

"To resolve thumb drive issue we use firewall, operating systems is firewalled. As we already have firewall and antivirus in place, the security need to be tightened more by moving our parameter from outside to inside the IT architecture."

The following case illustrates the Business Information Systems and the IS/IT Security Procedures of the Technical component. Business information systems are technological solutions to support the business operations and if not effectively controlled the critical business data would be leaked to irresponsible internal employees,

"Data that this transmitted to and for these systems - HRIS, Accounting, Plantation includes mail, engineering and all these are highly confidential".

After identifying and assessing the risk of the business information systems, the effective security counter-measures will be implemented to mitigate the associated risks.

"We take great care to safeguard our system adopting firewalls and security systems like "Tom Access" where at certain levels we use passwords to enter the systems because it is very important for us to make sure that people with relevant authorities are allowed to see and access information and also to input the right source documents (CEO, Company F)".

The Technical component is the realisation of the Formal components, where the implementation of Technical component depends on the direction provided in the IS/IT Security Vision, IS/IT Security Management Strategy and IS/IT Security Policy. In the IS/IT Security Governance Model, this relationship is identified as Relationship Type 2-Formal and Technical.

The following case signifies how the Formal component influenced the development of the Technical component. According to the CEO of Company A, the corporation utilised IT facilities for achieving successful business operations,

"Information Technology (IT) facilities are important to Company A Malaysia for the successful operations of its business". After recognising the risky IS/IT areas, security policy will be developed to provide the authorised users, defines roles and IS/IT resources, "The security issues that are included

here in the policy are related to network connectivity, account management, vulnerability management, secure system development, incident management, host protection and authentication”.

Next, the IS/IT Security Procedures will be established by employing effective IS/IT security counter-measures and controls to mitigate the risks.

“to protect the interests of Company A Malaysia by applying appropriate measures to the organisation’s IT assets and processes.

However, no specific IS/IT Security Procedures on security counter-measures or controls were mentioned.

The Formal component like IS/IT Security Policy was implemented effectively in the Technical component of Company B. For example, the IS/IT Security Policy of Company B covered the following security areas,

“backup, internet use, email use, desktop appearance and data classification”.

When the participant was asked about the implementation of IS/IT Security Policy, the security counter-measures were effectively implemented in the Technical component to mitigate the security risks,

“Our control system now identifies and deletes viruses automatically even on thumb drives. Virus is part of our security issues. Yes, it cleans the system immediately giving us protection. Our controls ensure unwanted intrusion is blocked automatically today”.

Furthermore, through effective management at the Technical component, the risk can be mitigated efficiently,

“I have two teams of IT people. One group looks after infrastructure (network, internet, desktop, security, data centre) and another group prepares a monthly report to me. The team is alerted hourly on potential breaches of security”.

Another example was taken from the case of Company B, how the Technical component is driven by the Formal component is presented. Good policy will not succeed without good implementation at the Technical component or IS/IT Security Procedures. For example, the IS/IT Security Procedures have been used to mitigate the risks associated with Internet use,

“We have also internet policy. In which it mentioned, all the internet facilities are meant for company purposes. In fact some of the non-business related sites are being blocked for staff to access”.

In addition, a scenario of the relationship between the Formal and Technical (RT2) components is presented. The implementation of IS/IT Security Procedures over the System Information Access Control policy is illustrated in the case of Company F. According to the CEO, each system has proper procedures including who can access, how to access, the security controls and counter-measures used for the system,

“even people that they assigned in the IT department only certain figure people will be accessible to the system, not every IT staff say 10, not all the 10 IT staff would have access to the Accounts File Directory, and all to Account, only certain staff doing the payroll system and IT manager sometimes IT manager don’t have the equipment. He has to go back to the Head of department, but the policies are there, we can have a look”.

8.5.2.1.3 Informal Component Themes

The Informal component deals with people and human aspects within the implementation of IS/IT security. The protection of IS/IT and business data involves not only maintaining the confidentiality, integrity and availability of the IS/IT but also engaging human aspects including responsibility of employees, integrity of people, trust and ethicality. The Informal component also involves with security culture, norms of employees, employee beliefs and personal values. Thus, the Informal component can be divided into two elements, Employee Values and Organisational Values. Employee Values and Organisational Values interrelate with the Formal component in respect to documents, processes and structures. According to the IS/IT Security Governance Model, the relationship between Formal and Informal components is recognised as Relationship Type 1(RT1).

Every participant has provided views relating to the importance of Informal component to their IS/IT Security processes including Employees Values and Organisational Values. Culture, Norms and Beliefs are also part of the Informal component which influence the Employee Values and Organisational Values.

a) Employee Values

Employee Values refer to people’s integrity, trust or ethicality, which deal with personnel values of employees. Integrity of people is part of the organisation. For example, as noted by the CEO of Company G,

“I think the core values, such as integrity are fundamental and everything”.

In addition, Employee Values should not be included in the policy statements because they are part of the requirements of membership of an organisation,

“Core values such as integrity, accountability and trust are not subject to policy statements. They underlie or are at the foundation of the business. For example, the way we interact with each other and the way we engage between internal users and customers (Company G)”.

A similar view by CEO of Company F, Employee Values are the basis for business and part of security culture and beliefs,

“Culture and company and all that, they know that our own ethics, knows our culture and company, and our expectation that must be, integrity must not be questionable, once we know we trust them, we must be able to empower them”.

According to the CEO of Company H, moral value plays an important role towards successful IS/IT security implementation,

“Informal factors will affect the human aspects like morale hence their support in the implementation of policies and security controls (CEO, Company H)”.

Lack of people’s integrity and lack of accountability may threaten the IS/IT system processes because security is not only a technical problem but also a social problem.

“Informal factors are important to support the implementation of IS/IT security because if people are not accountable and lack of integrity, the system processes would be compromised (CEO, Company G)”.

“CEO G: Imbue a culture that is aligned with the Board approved corporate strategy, mission, values, objectives, policies and procedures; and fosters risk awareness culture”

b) Organisational Values

Organisational Values are expectations from the board on the way in which employees should work and interact with each other in achieving IS/IT security governance. It influences the business process including the successful establishment of roles and duties. Organisational Values relate to structures of responsibility mainly derive from the Formal component likes policies. If the Formal component was adhered to consistently, these practices would become part of the security culture, norms and beliefs.

“Informal factors are very important to support the implementation of IT security policy and controls. Successful IT security policy and controls is not just the deployment of technology (firewalls and intrusion detection systems) but is a series of essential practices that is embedded into the culture of Company A Malaysia through training, education, awareness and others.

According to the CEO Company A, having clearer roles and responsibilities in what to accomplish will help employees to implement the IS/IT security procedures more effectively,

“Once the IS/IT security policy and controls are created, communicated and adopted, only then IT facilities can be effective to support and enable business requirements in a secure manner”.

8.5.2.2 Data Analysis and Research Question 2

To answer Research Question 2, the interactions of components were examined to determine if any data support the components interaction within a single case.

8.5.2.2.1 The relationship between Formal and Informal components, Relationship Type 1

The Formal component is important for the development of Employee Values and Organisational Values because it incorporates the risk strategies like education, training and policy awareness programme. Training was perceived to be crucial for the implementation of IS/IT security in the Informal component. Evidence was found in the comments of two CEOs of participant corporations. The CEO of Company F:

“I think very classic informal factors would be educational part, the training part” (CEO, Company F).

Another CEO comments about the important of training:

“Training is the most significant aspects but other informal factors such as culture, commitments, education, security awareness.. are also important (CEO, Company H)”.

Apart from training, security policy awareness was recognised as another risk management strategy for improving Employee Values and Organisational Values, as identified by the CEO Company F,

“If the employees lack training and awareness, they are not accountable”.

In addition, lack of training and security policy awareness would result in low Employee Values,

“This may lead to unmoral behaviour such as cheating and abusing of information (CEO, Company F)”

and also in low Organisational Values,

“If the employees are not trained, they are not aware and also not compliance with IT policies and procedures (CEO, Company F)”.

Corporations should consistently offer the IS/IT security programme to their staff for the development of the Informal component and creating a security culture.

“ In fact on I-Pgroup portion they do have some sort quarterly session like IT security awareness, in fact recently they have ICT security awareness 3 months ago and made for everybody to come, this is something I-Pgroup together with CORPORATE IT DEVELOPMENT UNIT, it is open to everybody (CIO, Company D)”.

The orientation program is an example of Formal component and is important for the development of the Informal component. For example, it exposes why IS/IT security is important in their organisation, the clear roles and responsibilities of IS/IT security and the implications of security practices. The CIO of Company B said,

“The orientation program is stated in the IT security policy (CIO, Company B)”.

The purpose of orientation or induction programme is to create awareness among employees in relating to IS/IT Security as highlighted by the CEO of Company F,

“We have orientation, we have induction programme and all that that would help us ensure the awareness is want to be”.

and

“CIO E: Informal aspects that incorporated in the implementation of policies and procedures relating to IT security are communication to all levels of the company, staff induction program, staff training, attending seminars, update or reviews of the Central Bank of Malaysia’s guidelines or compliance”.

Formal documents such as ICT baseline were identified as guidelines for the implementation of ICT. The ICT baseline is important for the development of Employee Values and Organisational Values,

“in short we have ICT baseline for informal aspects which cover the good ethics and educate the staff (CIO, Company D)”.

In the IS/IT Security Governance Model, IS/IT Security Standard is part of the Formal component. It outlines how processes need to be followed and be consistent with the security policy in the organisation. The standard is important to the Informal component in supporting the implementation of IS/IT security policy, as stated by a CIO,

“We have Code of practice to implement informal aspects. Employees need to follow code of practice to ensure employees aware with ICT security policy in this corporation. Code of practice provides the details on what to do when the lines come out”. (CIO, Company C).

8.5.2.2 The relationship between Formal and Technical components, Relationship Type 2

The Formal component sets the strategic direction for the Technical component implementation. This relationship is important because the Formal components such as IS/IT Security Policies provide a clear direction on which Technological Areas need to be secured and how the IS/IT Security Procedures need to be established. Importantly, the Technical component is the realisation of the Formal component.

With IS/IT security policies in place, the management has a clear direction which technological resources need to be secured and this leads to a proper IS/IT Security Procedures implementation in terms of accessibility,

“CEO F: Yes we have IT Policies and procedures, each of the systems, all structured procedures how to access, who to access and all that and IT department themselves have their own controls”, IS/IT security controls, “security features on each system”, and system privileges, “and even people that they assigned in the IT department only certain figure people will be accessible to the system, not every IT staff say 10, not all the 10 IT staff would have access to the Accounts File Directory, and all to Account, only certain staff doing the payroll system and IT manager”

The following is an example of how policy is important to the IS/IT Security procedures. Company B already had IS/IT Security Policies in place,

“We have five basic policies that cover backup, internet use, email use, desktop appearance and data classification. At implementation we roll out the policy to all staff. Policy is incorporated into our procedures. In what we do policy comes first, procedures follow and the things that must be done are done. We publish our policies to all staff in our IT repository. Roles are defined within the policy. Responsibility and data owners are identified. Data owners are referred to throughout our policy”.

The IS/IT Security Procedures such as IT security hardware appliance control was implemented to adhere to Internet policies,

“CIO B: we have security controls in place to identify breach of policy, let say the internet policy. We also have a hardware appliance that allows us to block access to websites we do not wish staff to access”.

8.5.2.2.3 The relationship between Informal and Technical components, Relationship Type 3

The Informal component has a relation with the Technical component with regard to IS/IT security procedures. Having adequate Employee Values and Organisational Values may improve perception over job roles and responsibilities in securing IS/IT assets and business data. For example, if the staff have inadequate Organisational Values and Employee Values, this would jeopardise the implementation process of IS/IT security procedures.

Individuals who do not have sufficient Organisational Values such as unaware of policy, unclear with job and responsibilities or lack of skills in the use of IS/IT systems, may lead to poor implementation of IS/IT security procedures.

“If the employees are not trained, they are not aware and also not compliant with IT policies and procedures (CEO, Company F)”.

Lack of awareness of IS/IT security procedures may cause unintended technical acts such as human errors. Policy awareness and security awareness are important aspects of the Organisational Values. In Company D, the CIO provided the staff with the security caution like the do's and don'ts relating to the correct use of IS/IT according to the policy requirements,

“not simply accepting email or forwarding it”.

The employee may open emails from someone unknown or click on links provided in the email and this action would expose the IT systems to security threats and vulnerabilities,

“CIO D: sometimes could be because of ignorance, they do not know that this could jeopardize the bigger picture, a lot of things”.

Lack of Employee Values such as people's integrity, distrust, not accountable, dishonest or unethical, may lead to social engineering attacks for achieving their own benefits or other intentional acts. According to Company F, not accountable was an example of lack in Employee Values,

“If the employees are lack of training and awareness, they are not accountable. This may lead to immoral behaviour such as cheating and abusing of information”.

The CEO of Company G emphasised the importance of Employee Values like accountable and people's integrity for achieving the goal of IS/IT systems.

“Of course. Informal factors are important to support the implementation of IS/IT security because if people are not accountable and lack of integrity, the system processes would be compromised”.

The Informal component including Organisational Values and Employee Values was an important human aspect to support the implementation of IS/IT security procedures. The Informal component was identified as the Critical Success Factor for IS/IT implementation,

“human aspects are always the critical success factors that determine the success or failure of any IT implementation (CEO, Company H)”.

In IS/IT Security Governance, the role of the board and senior management is important because the process of identifying, assessing and mitigating the security problems and dealing with the security issues is a continuous activity. One comment reflected the process,

“We all in management as a MD would be responsible to make sure people aware, we must provide training, we must update ourselves, we must send people for awareness courses or we provide information like through mail or whatever so that you can update yourself. Like FRS, the comments by auditors, of course to make sure we are, the culture we want to cultivate is aware especially new staff.”

8.5.3 Implementation and Monitoring Actions over the three components and interactions

There were two major responsibilities of corporate governance, directing action and monitoring action. Directing action refers to the role and responsibility of the board and senior management to achieve the intended goals and monitoring action is a reflective process in terms of measuring success or failure of the intended goals and the activities conducted at the directive stage. In the IS/IT Security Governance Model, the directing and monitoring actions refer to the involvement of the boards and senior management within the implementation of the Formal, Technical and Informal components of IS/IT Security Governance. The board and senior management need to ensure the balanced alignment between the three components to achieve the best security outcomes. To view the real world cases, interview data were analysed.

8.5.3.1 The Directing and Monitoring actions: The Formal component and its interaction

The board and senior management have responsibility to strategise and provide directives in terms of the IS/IT Security Vision, IS/IT Security Management Strategy, IS/IT Security Policy or IS/IT Security Standards to all employees in order to manage and control the IS/IT security risks. At the same time, the board and senior management need to ensure the alignment of the Formal component with the other two components. In spite of having directives in place, the board and senior management have responsibility to monitor the implementation of the Formal component and also its interactions.

The following draws evidence from interviews with regard to the directing action and the monitoring action; the most relevant cases are presented.

In the Formal component, the board and senior management are responsible to develop and implement the policies, strategies and decisions. The following activities were recognised as an example of the directing action of Company A,

“The CEO is part of the Senior Management that is charged with the responsibility of implementing the policies and decisions of the Board of Directors, overseeing the operations as well as developing, coordinating and implementing business and corporate strategies”.

The added value of this model is in order to achieve the Formal component of Company A, the Board and Senior Management should be able to identify the state and ground realities of the Technical and Informal components.

a) Case: Company A

The interaction between the Formal and Technical components is discussed. In achieving the policies and decisions of the Board, the management of Company A needs to ensure the appropriate IS/IT Security procedures such as security controls, hardware or software solutions are available and feasible, technically, economically and operationally.

In the case of Company A, the following statements show how the management were able to synchronise the implementation between the Formal and Technical components,

“Since the policy has been approved by the Board_of_Directors, the policy was already implemented under the direction of the Senior_Management. IT staff within the organisation subsequently ensured the appropriate measures for protection of the IT assets and processes were in place”.

The management also need to achieve the interaction between the Formal and Informal components, apart from achieving the Formal and Technical components interaction. The Formal component such as training and education strategies is important for the development of Informal component such as improving Employee Values and Organisational Values. With trained, skilled technical workers and high integrity people, the IS/IT Security Governance would be achieved. Company A has identified the use of education and training for mitigating the risks,

“organise training and education for employees on risk management and monitor the results of key performance indicators”.

In order to monitor the effectiveness of the Formal component and its interaction, the Board and Senior Management of Company A highlighted the methods used and identified the existing committees in place for monitoring activities.

The formal meeting with respective departments was the communication method for monitoring all types of activities including the Formal component and its interaction-Technical and Informal components.

“The Senior_Management has regular updates through meetings on all activities from respective department within the organisation and this enables the Senior_Management to review, identify, discuss and resolve strategic, operational, financial and key management issues”.

The other monitoring method used in the Corporation A was called as the Control Self Assessment process ,

“Central to the organisation’s internal control and risk management system is its Control Self Assessment process which it has developed and continues to improve over time. The Control Self Assessment process is a process that we put in place as part of the organisation’s internal control and risk management system”.

There were two active committees responsible in monitoring the corporation’s Control Self Assessment process, Risk Management and Internal Audit.

To monitor the Formal component and its interactions, the Risk Management Committee is responsible to monitor the IS/IT security matters through the quarterly reviews meetings.

“Like many other matters, IT related matters are also constantly reviewed as part of the organisation’s Enterprise Risk_Management programme. This includes the system recovery issues, information security issues and others. These issues are identified through the organisation’s Enterprise Risk_Management process whereby the Risk_Management Team headed by the Finance Director and comprising senior managers from all departments in the organisation including IT, will conduct quarterly reviews of the business risks as part of their responsibilities”.

Both committees of Company A worked together to address the IS/IT security risks effectively and efficiently. The Audit committee developed a key control checklist for monitoring the effectiveness of security internal controls.

“a key control checklist is developed and it sets out the various key controls and process requirements across all functions in the organisation and this includes any internal controls related to any IS/IT security matters. The key control checklist is reported regularly to the Audit Committee who assists the Board_of_Directors in reviewing the effectiveness of internal controls”.

The board and senior management also have responsibility in monitoring the internal controls applied in the context of IS/IT security. Through the review process, the management was able continuously to identify, assess, mitigate and control the risks which in line with policies.

“Through this process, the Board_of_Directors would be able to review the adequacy and integrity of the organisation’s internal_control systems and ensures that management undertakes such actions as maybe necessary in the implementation of the policies and procedures on risk and control approved by the Board_of_Directors whereby management identifies and assesses the risk faced and then designs, implements and monitors appropriate internal controls to mitigate and control those risks”.

To maintain the relationship between the Formal and Informal components, monitoring actions such as key performance indicators were used by Company A for measuring the effectiveness of the management strategies,

“organise training and education for employees on risk management and monitor the results of key performance indicators”.

8.5.3.2 The Directing and Monitoring actions: The Technical component and its interaction

a) Case: Company E

The interaction between the Technical component and Formal component is discussed. The implementation of the IS/IT Security Procedures of the Technical component derived from IS/IT security policy. After the implementation, the results of the Technical component are important to the Formal component in order to detect if the IS/IT Security Procedures are appropriate and effective for addressing the risks. The management needs to monitor this interaction to identify the inappropriateness or ineffectiveness of the strategies.

According to the CIO of Company E, IS/IT security related issues identified during the technical implementation normally will be reported to the IS/IT Steering Committee and the Audit Committee for reviewing the effectiveness of the IS/IT Security Procedures. However, if the risk mitigation is still not effective, the management may review the Formal component such as IS/IT security vision, IS/IT security management strategy or IS/IT security policy for coping with the risks and other factors.

“Any weaknesses identified will be table to the IS/IT steering committee and the Audit Committee (Board Level) and mitigating actions will be taken. The IS/IT security policies will be reviewed every year to take into account of the changing business, technology, operational, internal and external environment”.

The management of Company E adopted the project implementation methodology for tracking and monitoring the Technical component for the IS/IT systems projects.

“For the monitoring part of technical implementation, in any case, we do follow a proper project implementation methodology where a Project Plan will be developed and there will be ongoing tracking and monitoring. Prior to the implementation stage, the project’s objective would have been defined and the IS/IT Committee would have to approved it (CIO, Company E)”.

The Technical component such as IS/IT Security Procedures implementation is mainly derived from the IS/IT Security Policies. From the case of Company E, through the audit reports by auditors and bank (Central Bank of Malaysia), the board and senior management were able to detect non-compliance and inadequacy of policy.

“The IS/IT Security Policies are communicated to all levels of the staff in the company. Our Internal Auditors will audit the IS/IT Security Policies from time to time to ensure compliance and its adequacy. The same goes with our external auditors and also the Central Bank of Malaysia’s”.

The board and senior management can achieve the goal of Technical component such as IS/IT Security Procedure by improving or reviewing the Formal component such as the IS/IT security management strategy or the policies. If any deficiencies are found in the Technical component, the organisation may apply the IS/IT security management strategies such as Company E has incorporated for achieving Employee Values and Organisational Values,

“staff induction program, staff training, attending seminars, update or reviews”.

The interaction between Technical component and Informal component is also discussed. The Technical component such as IS/IT security procedures needs to be aligned with the Informal component development such as employee's needs, skilful person and high integrity employee. As identified by Company E, *communication to all levels* was a strategy used by the board and senior management for empowering Organisational Values (Informal component) in order to achieve the IS/IT security procedures.

The directives of the three components and the interactions should be monitored. The board and senior management are responsible to monitor the effectiveness of the components and interactions. For example, the following shows how the board and senior management monitor the Technical/Informal interaction.

“To monitor the implementation of informal aspects, we use KRAs and KPIs. KRAs and KPIs will be set and Action Required (AR) will be assigned. Daily or weekly or monthly or quarterly reviews or meeting with relevant managers or departments”.

In achieving the IS/IT security procedures of Company E, the KRAs and KPIs were used for monitoring the Formal components such as Staff Training, Seminars and Induction Program.

However, there was no evidence provided in Company C to show how the board and senior management monitor the Technical/Informal interaction.

8.5.3.3 The Directing and Monitoring actions: The Informal component and its interaction

In the IS/IT Security Governance Model, the board and senior management are responsible to provide directives and monitoring aspects to the Informal component. They have responsibility to identify, assess and mitigate all types of business risk including the risks associated with Employee Values and Organisational Values.

Security culture, norms and beliefs influence the development of Employee Values and Organisational Values because the security culture, norms and beliefs depend upon the involvement of the board and senior management in IS/IT security. In reality, the Informal component is very subjective to measure as it is about the culture and the Organisational Values and Employee Values held.

To achieve efficient and effective IS/IT security implementation, balanced interaction between the Informal component and the Formal and Technical components is needed.

The interaction between the Informal component and the Formal component is now viewed. To view the real world of components interaction, Company D was selected to be the case analysis.

a) Case: Company D

Active involvement can be seen through the inclusion of IS/IT security issues in the corporate risk plans and agendas. In Company D, the IS/IT security matters were included in the Risk Management Plan where the IS/IT risks are also part of business risks. Security culture may be observed through the IS/IT security processes in the organisation like the frequency of formal meetings

conducted at the board and management levels to identify and mitigate the business risks effectively. For example, at the board and senior management level the IS/IT security matters were discussed between 4 to 6 times a year depending on the urgency,

“The ISMC has quarterly (minimum) meeting. If there is a need to have it, we will do every two months, sometime we do every two months sometime we do quarterly, that will be discussing on any IT security issues, services, governance or whatsoever with regards to ICT matter of Company D”.

The security culture of an organisation is normally related to the norms of employees. It was found that the IS/IT security processes in Company D took place in the entire management levels and organisation. The meeting on the IS/IT security risk identification and mitigation is actively conducted at the operational level before reporting to the Board and Senior Management level,

“Yes every Thursday, we have meeting with ISMC. By right supposed to be done this evening. If we can't, we do on Friday; we try to make it every week. So any issues relating to IT security will be highlighted. With this operational meeting, we have a direct access to all I-Pgroup support and management. If the issue deemed to be highlighted at that level, we will use this operational meeting to highlight to their management”.

In the IS/IT Security Governance Model, the Informal/Technical interaction is also important. The active involvement of the board and senior management should be demonstrated through effective and efficient implementation of IS/IT security procedures. For example, Company D implemented an important IS/IT security project in order to minimise or prevent the threats becoming risks. The IS/IT project was involved with the standardisation of patches across servers between subsidiaries and parent.

“We have project in ICT patches alignment to standardize patches for all servers, our server basically scattered in our offices in Malaysia, a lot of servers, the patches level are not standard (not the same),.. so when the patches level is not the same, we expose the server from external/internal threat”.

Besides that, Company D planned to implement a new IS/IT security project which related to IT Access Management. Currently, the issue identified was the users have different IDs for different IS/IT systems,

“let's say they have seven IDs, ID for SAP is different, MS Exchange is different”.

So this becomes problematic when staff leave where the IT systems and business data may be threatened, fragile, exposed and risky to Company D,

“When staff resigned, the removal process shouldn't be focusing on taking out Local Area Network ID only, also have to take out all the other IDs. Currently we really have to look at the registration, if they have 8 IDs, we have to remove 8 IDs”.

With the new security project, the system will remove all the IDs at one time regardless the location of the databases,

“if the staff is confirmed resign by HR, we just use the system, all IDs automatically removed, regardless where. So we don't need, to do all the listings which you tend to miss out a few things. With this initiative at the group wide level once the staff resigned the system will removed everything”.

Chapter 9 Mail Survey Analysis

9.1 Response Rate

The number of questionnaires to be sent out began as half each of Group A companies (100) and Group B companies (425), i.e., 525/2 or 263, and was then rounded up to 270. A few group C companies were included to confirm the expectation that they would be unable to answer the questions.

270 sets of the mail survey were sent out to companies within the three sample groups, A(Top), B(Middle) and C(Bottom). A response rate of 7.8% (21) was obtained. The low response rate was disappointing as the response rates reported in the literature were often between 25-30 percent (Ticehurst et al, 2000). Interestingly, the mail survey responses were returned by appropriate roles in leading organisations in Malaysia, 71% of responses were from the board and senior management group and 91% were from the Top and Medium organisations. The survey had successfully collected responses from key people and high profit organisations. The survey had convincing and reliable data in terms of length of service and work experience in security risk areas, more than half of the respondents had more than 10 years work experience in security. The strong demographic backgrounds of respondents in roles, group size and work experience in security have given validity to the responses.

The literature suggests that many statistical tests require less than 20 instances in each cell, which suggests that the 21 responses of this survey could be used to generate various valid statistical results. Even though it would be possible to carry out several such tests, complex statistical analyses were not conducted; the analysis of the survey is limited to frequencies and percentages.

9.2 Demographic Information

This section describes the demographic details of respondents, shown in Table 9.1. A majority of sixty-seven percent of respondents was from Group A (Top). Group B (Medium) constitutes twenty-four percent of respondents while Group C (Bottom) had a minority with ten percent of respondents. A majority of respondents (71%) were from boards of directors and senior management. Fifty-eight percent had more than 10 years working in risk security type area. The majority of respondents held a first degree (68%), a master's degree (26%) PhD (5%). Forty-seven percent of respondent companies had above 3,000 employees and forty-three percent had less than 1,000 employees. Within the classification 'multi-national corporation', eighty-six percent had greater than 10,000 employees. The location of the respondents' parent company was predominantly (81%) Malaysia. There were three dominant sectors of respondents within the sample, Manufacturing (26%), Agriculture, Forestry and Fishing (21%) and Finance and Insurance (11%).

Survey question no	Category		Frequency	Percent (%)	
	Group Type	Group A	14	67%	
		Group B	5	24%	
		Group C	2	9%	
1	Role	The Board of Director	2	12%	
		Senior Management	11	69%	
		Junior Manager	3	19%	
3	Work Experience in Security Risk Type	Less than 1 year	3	16%	
		1-3 years	3	16%	
		4-6 years	1	5%	
		7-9 years	1	5%	
		More than 10 years	11	58%	
2	Education Level	First Degree/Equivalent	13	68.4%	
		Master’s Degree	5	26.3%	
		Doctor of Philosophy	1	5.3%	
5a	Number of Employees if National Level Corporation	Above 3000	9	47.4%	
		1000-2999	3	15.8%	
		100-999	7	36.8%	
5b	Number of Employees if Multinational Level	Greater 10000	6	85.7%	
		5000-9999	1	14.3%	
6	Location of Parent Company	Malaysia	13	81.25%	
		Other Country Specified	Sweden	1	6.25%
			US	1	6.25%
			France	1	6.25%
4	Industry of Company	Finance and Insurance		2	10.5%
		Manufacturing		5	26.3%
		Agriculture, Forestry and Fishing		4	21.1%
		Construction		1	5.26%
		Transport and Storage		1	5.26%
		Other Sector Type Specified	Utilities and Infrastructure	1	5.26%
			Construction and Plantation	1	5.26%
			Water Services	1	5.26%
			IT	1	5.26%
			Oil and Gas	1	5.26%
			Stock Exchange	1	5.26%

Table 9.1 Demographic characteristics of respondents

9.3.1 Additional Information on survey and Research Question 1

Research Question 1 was intended to examine if any related structures and responsibilities of IS/IT Security exist within corporations which reflect the Formal, Technical and Informal components.

9.3.1.1 Formal component

a) Importance of IS/IT Security

First, in order to know the level of IS/IT security within the corporation, the respondents were asked to indicate their agreement on the importance of IS/IT security in their corporation in survey question no.14. All respondents (21) agreed that IS/IT security is important to their corporation. See Table 9.2.

Question 14

		Frequency	Percent
No. 14	Agree	21	100.0
	Neutral	0	0
	Disagree	0	0
	Total	21	100

Table 9.2 Importance of IS/IT security

Further analysis of the involvement of the Board and Senior Management within their corporations reflects the level of agreement towards the importance of IS/IT Security. The further breakdown of the analysis included these matters; how the Boards (question 15.1) and Senior Managers (15.2) perceived the responsibility for IS/IT security risks, how important is IS/IT security risk against business risks(question 16.1) and how important is IS/IT security risk within the Corporate Risk Management Plan (question 16.2).

Question 15.1

In the survey question no.15.1, the analysis shows that 61.9% agreed that IS/IT security is the responsibility of the Board of Directors (Table 9.3).

		Frequency	Percent
15.1	Agree	13	61.9
	Neutral	6	28.6
	Disagree	2	9.5
	Total	21	100.00

Table 9.3 IS/IT Security Risks by the Board of Directors

Question 15.2

And 90.4% agreed that Senior Managers have a significant responsibility for IS/IT security risks. (Table 9.4)

		Frequency	Percent
15.2	Agree	19	90.4
	Neutral	1	4.8
	Disagree	1	4.8
	Total	21	100.0

Table 9.4 IS/IT Security Risks by Senior Management

The majority (95.2%) agreed that IS/IT security risk is part of business risks. (Table 9.5)

Question 16.1

		Frequency	Percent
16.1	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total		100

Table 9.5 IS/IT Security Risk a Business Risk

And most of respondents believed that IS/IT security risk is part of Corporate Risk Management Plan (90.5%) within their corporations. See Table 9.6

Question 16.2

		Frequency	Percent
16.2	Agree	19	90.5
	Neutral	2	9.5
	Disagree		
	Total	21	100.0

Table 9.6 IS/IT Security Risk, part of Corporate Risk Management Plan

b) IS/IT Security Policy

When respondents were asked whether their corporations had an IT/IS security policy in question 8, see Table 9.7, 85.7% indicated that they did have an IT/IS security policy in place. Looking at the respondents who indicated “no”, 10.6% were from manufacturing and 5.3 % from Agriculture, Forestry and Fishing.

Respondents who indicated “yes” were further asked two major questions, security areas covered in the IT/IS security policy-question 9, and security requirements stated in the IT/IS security policy- question 10.

The results of question 9 show that all respondents indicated that they did cover security areas in “user access management”, “prevention of viruses and worms”, “disclosure of information”, “violation and breaches of security” and “software development and maintenance”.

In the case of security requirements stated in the IT/IS security policy, question 10, all respondents pointed out that their corporation's policy included "objective of the IT/IS security policy", "roles and responsibilities" and "monitoring and review".

The majority (94.1%) of respondents indicated that their IT/IS security policy had requirements on "IT/IS security principles" and "violations and disciplinary action".

Survey Question N0			Categories	Frequency	Percent (%)
8	IT/IS security policy		Yes	18	85.7%
			No	3	14.3%
9	Security areas covered in IT/IS security policy	User access management	Yes	18	100%
			No	0	0%
		Prevention of viruses and worms	Yes	18	100%
			No	0	0%
		Disclosure of information	Yes	18	100%
			No	0	0%
		Violation and breaches of security	Yes	18	100%
			No	0	0%
		Software development and maintenance	Yes	18	100%
			No	0	0%
10	Security requirements stated in IT/IS security policy	Objectives of the IT/IS security policy	Yes	17	100%
			No	0	0%
		IT/IS security principles	Yes	16	94.1%
			No	1	5.9%
		Roles & responsibilities	Yes	18	100%
			No	0	0%
		Violations and disciplinary action	Yes	16	94.1%
			No	1	5.9%
		Monitoring & review	Yes	18	100%
			No	0	0%

Table 9.7 IT/IS security policy

In the Formal component, the Board and Senior Management have responsibility to provide direction in the policies relating to IS/IT security to ensure the IS/IT security risks are controllable. To reflect the involvement of the board and senior management in the Formal component, the following areas were examined which include the role of the board and senior management in the IS/IT Security Policy, the alignment between IS/IT security policy and business goals and the alignment between IS/IT security policy and security goals.

In terms of the specific roles held by the Board of Directors, only some respondents, 61.9%, agreed that the Board of Directors are responsible for the establishment of IS/IT security policies. This can be seen in Table 9.8.

Question 17.1

		Frequency	Percent
17.1	Agree	13	61.9
	Neutral	7	33.3
	Disagree	1	4.8
	Total		100

Table 9.8 The Board of Directors responsibility over IS/IT Security Policies

Many respondents (85.7%) agreed that the Senior Management had a significant accountability role in the implementation of the IS/IT security policy. (Table 9.9)

Question 17.2

		Frequency	Percent
17.2	Agree	18	85.7
	Neutral	3	14.3
	Disagree		
	Total	21	100.0

Table 9.9 Senior Management accountability over IS/IT Security Policies

The alignment between IS/IT security policy and business goals is important for IS/IT security governance because the greater the alignment between policy and business goals the higher the security protection being provided for IS/IT assets and business data of the corporation. The survey found that three-quarters (76.2%) of respondents agreed that the IS/IT security issues covered in the IS/IT security policy are dependent upon business goals. See Table 9.10.

Question 17.3

		Frequency	Percent
17.3	Agree	16	76.2
	Neutral	2	9.5
	Disagree	3	14.3
	Total	21	100.0

Table 9.10 Security issues IS/IT Security Policies Business Goals

The respondents were also asked about the alignment between the IS/IT security policy and security goals, the majority (90.5%) agreed that the security issues covered in the IS/IT security policy are dependent upon security objectives, as seen in Table 9.11.

Question 17.4

		Frequency	Percent
17.4	Agree	19	90.5
	Neutral	2	9.5
	Disagree		
	Total	21	100.0

Table 9.11 Security issues IS/IT Security Policies, Business Requirements

The quality of the implementation of security controls procedures does influence the success of IS/IT Security Policy. The quality of implementation can be achieved through effective and consistent directing and monitoring of the security controls procedures by the Board and Senior Management. The majority of respondents (95.2%) agreed that quality implementation processes over security controls are essential for the implementation of IS/IT security policy. When the respondents were asked about their role in the corporation, eighty-one percent claimed Board of Directors and Senior Management designations. (Table 9.12)

Question 17.5

		Frequency	Percent
17.5	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total	21	100.0

Table 9.12 Quality of processes over security controls

IS/IT security problems are mainly caused by people, not by technological factors, therefore, commitment from all levels of employees including the Board and Senior Management is vital. They are responsible for the cultivation of the security culture by consistently and effectively implementing and monitoring the IS/IT security policies and procedures. According to the survey, all respondents agreed that the implementation of IS/IT security policy requires the involvement of personnel at all levels of the business. (Table 9.13)

Question 17.6

		Frequency	Percent
17.6	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100.0

Table 9.13 IS/IT Security Policies involvement and personnel's at all levels

c) IS/IT security and internal controls

95.2% of respondents stated that they have applied internal controls within IT/IS security, see Table 9.14.

Question 12:

	Categories	Frequency	Percent (%)
IT/IS security internal controls in place	Yes	20	95.2%
	No	1	4.8%

Table 9.14 IT/IS security and internal controls

Further analysis reflects how the Board and Senior Management view the role of internal controls within the IS/IT security implementation. The internal controls were important in two areas, within the implementation of IS/IT security policies and IS/IT security risk management.

With regard to question 18.1, the majority (95.2%) of survey respondents agreed that the internal controls were essential in the implementation of IS/IT security policies.

Question 18.1

		Frequency	Percent
18.1	Agree	20	95.2
	Neutral		
	Disagree	1	4.8
	Total	21	100.0

Table 9.15 Internal controls and IS/IT Security Policies

In terms of the IS/IT security risk management, 57.2% believed that the Board of Directors has responsibility for the implementation of internal controls over IS/IT security risks, as set-out in question 18.2.

Question 18.2

		Frequency	Percent
18.2	Agree	12	57.2
	Neutral	7	33.3
	Disagree	2	9.5
	Total	21	100.0

Table 9.16 The Board of Directors responsibility and internal controls over security risks

More than half (66.7%) believed that the Board of Directors has accountability in the implementation of internal controls over IS/IT security risks.

Question 18.3

		Frequency	Percent
18.3	Agree	14	66.6
	Neutral	6	28.6
	Disagree	1	4.8
	Total	21	100.0

Table 9.17 The Board of Directors accountability and internal controls over security risks

The Senior Management has a significant role in IS/IT security governance, all agreed (question 18.4) that the Senior Management are accountable for the implementation of internal controls for IS/IT security risks.

Question 18.4

		Frequency	Percent
18.4	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100.0

Table 9.18 Senior Management accountability and internal controls over security risks

d) IT Steering Committee

The IS/IT Security Management Strategy, such as using an IT Steering Committee, provides ways to achieve the IS/IT Security Vision. Survey respondents were asked whether they had an IT Steering Committee at Board level. Only thirty-five percent indicated that their corporations had an IT Steering Committee at Board level. Sixty-two percent indicated that they had an IT Steering Committee at the Senior Management level.

Question 7

	Categories	Frequency	Percent (%)
IT Steering Committee at the board level	Yes	7	35%
	No	13	65%
IT Steering Committee at the senior management level	Yes	13	62%
	No	8	38%

Table 9.19 IT Steering Committee in place

Two further questions had been asked to examine the role of IT steering committee, questions 19.1 and 19.2.

Most respondents perceived, positively, the role of an IT Steering Committee at the Board and senior management level 85.7% agreed that the IT Steering Committee is an essential mechanism to support IS/IT security processes. The analysis result was referring to question 19.1.

Question 19.1

		Frequency	Percent
19.1	Agree	18	85.7
	Neutral	2	9.5
	Disagree	1	4.8
	Total	21	100

Table 9.20 IS/IT Steering Committee essential mechanism

Overall, the majority (85.7%) of the respondents agreed that the IT Steering Committee plays an important role in the establishment of IS/IT security policies.

Question 19.2

		Frequency	Percent
19.2	Agree	18	85.7
	Neutral	3	14.3
	Disagree		
	Total	21	100.0

Table 9.21 IS/IT Steering Committee plays role IS/IT security policies

e) IT/IS security and Risk Management

The majority (81%) of respondents indicated IT/IS security was part of their corporation's risk management plan. About two-thirds of the respondents were from Group A, the Top Companies in market capitalisation.

Question 11

	Categories	Frequency	Percent (%)
IT/IS security as part of risk management plan	Yes	17	81.0%
	No	4	19%

Table 9.22 IT/IS security and risk management

f) IS/IT Security Standard

Only a few (15.8%) of the respondents adopted an external IT/IS Security Standard which was "ISO 17799 / BS7799" within their corporations. Majority of respondents, eighty-four percent indicated they did not apply the IT/IS security standard of ISO 17799. When the respondents were asked if they had other related standards, two respondents agreed, the first company adopted "ISO 27001" and the second company used its own internal standard.

Question 13

	Categories	Frequency	Percent (%)
Adoption of ISO 17799 / BS 7799 Standards	Yes	3	15.8%
	No	16	84.2%

Table 9.23 IT/IS security standards

g) Technical role by board and senior management

About half of the respondents had a positive view that the board has accountability for technical roles as IS/IT security is part of the corporate risk management plan but only a small number (19%) had a negative perception about this topic.

Question 21.1

		Frequency	Percent
21.1	Agree	12	57.2
	Neutral	5	23.8
	Disagree	4	19
	Total	21	100.0

Table 9.24 The Board of Directors accountability, technical roles

Most (90.5%) respondents believed that the senior management has significant responsibility in implementing technical roles as IS/IT security is part of the corporate risk management plan.

Question 21.2

		Frequency	Percent
21.2	Agree	19	90.5
	Neutral	2	9.5
	Disagree		
	Total	21	100.0

Table 9.25 Senior Management responsibility, technical roles

The majority (61.9%) of respondents had an uncertain view of the board's responsibility to monitor the progress of technical implementation.

Question 22

		Frequency	Percent
22	Agree	6	28.6
	Neutral	13	61.9
	Disagree	2	9.5
	Total	21	100.0

Table 9.26 The Board of Directors, monitor technical roles

9.3.1.2 Informal component

The Informal component refers to the security culture and norms of employees of an organisation including Employee Values and Organisational Values. Employee Values relate to the personal and ethical values of individuals within the organisation and Organisational Values concern the responsibilities derived from the policies where the security culture will be cultivated through consistent practices.

The Informal component plays a significant role in IS/IT security. Ninety-five percent of respondents agreed that the Informal component is important for IS/IT security and they believed that the security issue was not only a technological or organisational issue but also a social issue.

Question 24

		Frequency	Percent
24	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total	21	100.0

Table 9.27 Human factor social issue

All of the survey respondents agreed that Employee Values such as trust, integrity and ethicality are needed for the implementation of IS/IT security.

Question 23.2

		Frequency	Percent
	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100.0

Table 9.28 Trust, integrity, ethicality

9.3.1.3 Summary

Fundamentally, the survey covered responses from two components, formal and informal. The survey did not provide questions relating to the technical component.

Formal component

In the IS/IT Security Model the formal component comprises six themes/topics relating to formal processes, IS/IT security vision, documents, and structures in place. These seven themes were ‘importance of IS/IT security’, ‘IS/IT security policy’, ‘IS/IT security and internal controls’, ‘IT steering committee’, ‘IS/IT security and risk management’, ‘IS/IT security standard’ and ‘technical roles by board and senior management’.

In the first theme of ‘importance of IS/IT security’, all companies agreed that IS/IT security was important to their organisations. More than half of the respondents agreed IS/IT security was the responsibility of the board of directors, while the majority of them stated that senior managers had significant responsibility for IS/IT security risks. Interestingly, a big majority claimed that IS/IT security risks were part of business risk and, consistent with this, almost all agreed that IS/IT security was part of the risk management plan.

The second theme, ‘IS/IT security policy’, the majority of respondents had IS/IT security policies in their organisations. All respondents had covered security issues in five areas which were “user access management”, “prevention of viruses and worms”, “disclosure of information”, “violation and breaches of security” and “software development and maintenance”. Apart from that, all respondents also included three security requirements in their corporations, these include “objective of the IT/IS security policy”, “roles and responsibilities” and “monitoring and review”. Almost all respondents agreed that their policies included two requirements, which were “IT/IS security principles” and “violations and disciplinary action”. In the context of policy formulation, almost two-thirds of the respondents agreed that the board had responsibility for the establishment of IS/IT security policy and a majority of respondents believed that senior management had significant accountability in the implementation of IS/IT security policy. About two-thirds of the respondents considered that the IS/IT security policy was driven by business goals but almost all respondents believed the IS/IT security policy was based on security requirements. A big majority had perceived the importance of

quality implementation processes over security controls for the implementation of IS/IT security policies. All respondents believed that the implementation of IS/IT security policy requires the involvement of personnel at all levels of the business.

The third theme of 'IS/IT security and internal controls' prescribes the importance of internal controls in IS/IT security and assesses the role of board and senior management in this area. Almost all respondents claimed that they had applied internal controls within their IS/IT security and believed in the important role of internal controls within the implementation of IS/IT security policies. About half of the respondents agreed that the board had responsibility for the implementation of internal controls in IS/IT security risks, but almost two thirds of them believed that the board had accountability in this area. Significantly, all respondents claimed that senior management were accountable for the implementation of IS/IT security internal controls.

With regard to the fourth theme of 'IT steering committee', questions were asked relating to committee structure in place and its role. Almost two-third of respondents claimed that they had an IT steering committee at the senior management level and a few at the board level. The IT steering committee was important for the implementation of IS/IT security processes and IS/IT security policy formulation.

In the fifth theme of 'IS/IT security and risk management', most respondents claimed that they had included IS/IT security as part their risk management plan.

With reference to the sixth them of 'IS/IT security standards', very few respondents adopted IS/IT security standards within their organisations and the most popular standard was ISO 17799/BS 7799.

In the final theme of 'technical role by board and senior management', the majority believed that the senior management had responsibility in the technical role but not many respondents thought the board had accountability in this technical role.

Informal component

Almost all respondents had claimed that the informal component was important for IS/IT security where they believed that the security issue was not only a technological or organisational issue but also a social issue. All respondents claimed that that Employee Values which were trust, integrity and ethicality are essential for the implementation of IS/IT security.

9.3.2 Additional Information on survey and Research Question 2

Research Question 2 is intended to examine if any interaction occurs between the three components and how does the Board and Senior Management implement and monitor these components interactions. The inter-relationship between these three components is important because lack of balance or deficiencies in any of these relationships may lead to narrow solutions such as Technical orientated or Management orientated only rather than a comprehensive view.

9.3.2.1 Formal/Informal Relationship Type 1 (RT1)

The Relationship Type 1 considers the relationship between the Formal and Informal components. The implementation of IS/IT Security Governance requires balance between the Informal component and Formal component. In terms of the relationship of Formal and Informal components, the Formal component has become an input towards the development of the Informal component.

All respondents agreed that the Formal component, like education, training and awareness relating to IS/IT security, is relevant to the implementation of IS/IT security governance. Education, training and awareness are needed to improve the Informal component.

Question 23.1

		Frequency	Percent
23.1	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100.0

Table 9.29 Education, training and awareness

All of the respondents believed that the Informal component such as human factors should be aligned with the Formal component such the Corporation's Code of Ethics.

Question 23.3

		Frequency	Percent
23.3	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100.0

Table 9.30 Conduct of human factors and Code of Ethics

With regard to the Formal and Informal components relationship, the Formal component such as policy requires the incorporation of the Informal component such as human factors but only 47.6% of respondents agreed that the Board of Directors is responsible for the establishment of policy relating to human factors.

Question 25

		Frequency	Percent
25	Agree	10	47.6
	Neutral	10	47.6
	Disagree	1	4.8
	Total	21	100.0

Table 9.31 The Board of Directors responsibility over human factors policy

Question 26.1

Only 42.8% of respondents believed that the Board and of Directors is ultimately accountable for the establishment of policy relating to human factors.

		Frequency	Percent
26.1	Agree	9	42.8
	Neutral	11	52.4
	Disagree	1	4.8
	Total	21	100.0

Table 9.32 The Board of Directors accountability over human factors policy

However, the important role of Senior Management in policy implementation is obvious, the majority (95.2%) of respondents agreed that the Senior Management has significant responsibility for the establishment of policy relating to the human factors of IT/IS security.

Question 26.2

		Frequency	Percent
26.2	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total	21	100

Table 9.33 Senior Management responsibility, human factors policy

When the respondents were asked whether the corporation's policy should include human factors, knowledge, culture, awareness and moral issues, all of them agreed, as set-out in question 27.

Question No 27

		Frequency	Percent
27	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100

Table 9.34 Corporation policy, human factor, knowledge, culture, awareness

Every security implementation requires monitoring activity. Question 28.1 was asked relating to whether the board of directors have accountability to monitor the implementation of human factors in achieving business policy, more than half (61.9%) of respondents agreed and 33.3% respondents were unsure.

Question 28.1

		Frequency	Percent
28.1	Agree	13	61.9
	Neutral	7	33.3
	Disagree	1	4.8
	Total	21	100.0

Table 9.35 The Board of Directors, monitor, human factor

Most (95.2%) respondents believed that the senior management had responsibility to monitor the implementation of human factors.

Question 28.2

		Frequency	Percent
28.2	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total	21	100.0

9.36 Senior Management responsibility, monitor human factor

9.3.2.2 Formal/Technical Relationship Type 2 (RT2)

In the IS/IT security governance model, reciprocal relationship is crucial. The Relationship Type 2 underlines the important link between the Formal and Technical components. As already prescribed in the IS/IT security governance model, formal refers to structure and formal processes and technical is concerned with technological resources and IS/IT security procedures.

The respondents were asked if policy, standards and procedures are important elements within IS/IT security, all respondents had positive perceptions towards it.

Question 20.1

		Frequency	Percent
20.1	Agree	21	100
	Neutral		
	Disagree		
	Total	21	100.0

Table 9.37 Policy, standards, procedures, elements IS/IT security

Half (52.4) of the respondents agreed that the board of directors is accountable to ensure an adequate monitoring of the IS/IT security policy, IS/IT security standards and IS/IT security procedures implementation. One-third of respondents (38.1%) were unsure whether the board has a role in this matter. See Table 9.38.

Question 20.2

		Frequency	Percent
20.2	Agree	11	52.4
	Neutral	8	38.1
	Disagree	2	9.5
	Total	21	100.0

Table 9.38 The Board of Directors accountability over policy, standards and procedures

Most (95.2%) respondents agreed that the senior management have responsibility for the implementation if IS/IT security policy, IS/IT security standards and IS/IT security procedures.

Question 20.3

		Frequency	Percent
20.3	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total	21	100.0

Table 9.39 Senior Management responsibility over policy, standards and procedures

When the respondents were asked whether reporting is an essential mechanism in IS/IT security governance, the majority (90.5%) had positive responses in this topic.

Question 20.4

		Frequency	Percent
20.4	Agree	19	90.5
	Neutral	2	9.5
	Disagree		
	Total	21	100.0

Table 9.40 Reporting mechanism and IS/IT security governance

9.3.2.3 Summary

Research question 2 was intended to discover the respondents' agreement on component interaction of the three relationships, Relationship Type 1-Formal/Informal, Relationship Type 2-Formal/Technical and Relationship Type 3-Technical/Formal. The survey had covered two types of relationships, Relationship Type 1 and 2, but no question related to Relationship Type 3.

In Relationship Type 1, all respondents claimed that the formal component including education, training and awareness was needed for the implementation of IS/IT security governance. The alignment between human factors and the corporation's code of ethics was crucial. Almost half of the respondents thought that the Board of Directors was responsible for the establishment of policy relating to human factors but the majority believed senior management had significant responsibility for the establishment of human factors in the IS/IT security policy. Human factors, knowledge, culture, awareness and moral issues were significant to be included in the corporation's policy. Almost two-thirds claimed that the board had accountability in monitoring the implementation of human factors but the majority believed that senior management had much responsibility in the monitoring activity.

RT2

The relationship type 2 was concerned with Formal/Technical. All respondents considered policy (formal), standards (formal) and procedures (technical) are important elements within IS/IT security. About half of the respondents agreed that the board was accountable in monitoring the IS/IT security policy, IS/IT security standards and IS/IT security procedures implementation but almost all believed that senior management should be much involved in this area. Reporting was considered to be an essential mechanism in IS/IT security governance.

Chapter 10: Conclusion, Limitations, Further Research and Recommendations

10.1 Introduction

The literature and prior research suggested that lack of understanding of IS/IT security problems at the ground level by the boards and senior management had impacted on IS/IT security practices across management levels within organisations. It was also suggested that the lack of understanding of IS/IT security problems was due to the ineffectiveness of supervision roles between the giver/supervisor of the security responsibility and the holder of the security responsibility. 'Directing' and 'monitoring' actions over IS/IT security policies and procedures were not implemented effectively and efficiently within the supervision role of IS/IT security, including the application of internal controls and risk management.

It had been shown that many security incidents and security deficiencies in organisations were mainly caused by human actions rather than by technical problems (Dhillon et al. 2000). There was also some evidence that apart from the technical and formal components the informal factor had played a significant role in IS/IT security practices (McIlwraith, 2006). Another gap shown was that a lack of interaction between the technical, formal and informal components had caused unbalanced requirements from each component, misaligned goals and strategies and low quality of security implementation in terms of supervision roles.

A model of IS/IT security governance was developed to address the research problems and the study covered these areas: 1) the concurrent implementation of three components, formal, technical and informal in IS/IT security and the interactions among them; 2) the application of internal controls and risk management to improve the understanding of security problems at the board and senior management level within the three components, through 'directing' and 'monitoring' actions.

The literature review (Chapter 2), conceptual framework (Chapter 3) and model of IS/IT security governance (Chapter 4) were developed from the research problems and research gaps identified in the early stages of the study. Along with research problems and research gaps, the research was primarily based on two research questions posed in Chapter 1:

Research Question 1: *In what way does the involvement of Boards and Senior Management impact on the implementation of IS/IT Security Governance in the Formal, Technical and Informal components?*

Research Question 2: *How can directing and monitoring actions in the technical, formal and informal components of IT/IS security governance in corporations be implemented efficiently and effectively?*

Overall, the findings reported in the data analysis chapters are consistent with the model of IS/IT security governance elements. Fundamentally, the study has answered the two research questions posed through findings reported in Chapters 6, 7, 8 and 9. There were three types of data used in the analysis: website data; interview data; and survey data. The website data, a secondary data type, were analysed and reported in Chapter 6. The primary data, the interviews, were analysed and reported in the

two subsequent chapters, Chapter 7, using software analysis and Chapter 8, using manual content analysis. While another primary data type, survey, was analysed and reported in Chapter 9.

The majority of findings supporting the model of IS/IT security governance was provided by big industry players among Malaysian Publicly Listed Companies.

The results of the analyses are reported in the following three sections of website analysis, interview data analysis and survey analysis.

10.1.1 Website Analysis

In the website analysis, about one-third of the annual reports of the main board of the Malaysian Publicly Listed Companies were reviewed and the majority of the data which supported the model came from the annual reports of Group A-top 100 companies and Group B-middle market capitalisation where the profits recorded were between MYR31 Billion and MYR 2 Million. The groups with higher market capitalisation played positive roles in the implementation of IS/IT security governance. The results support the Corporate Governance Survey (2008) conducted by the Minority Shareholder Watchdog Group in collaboration with its partner, the Nottingham University Business School, where the companies with higher market capitalisations had shown good principles of corporate governance practices in terms of the Malaysian Code of Corporate Governance, Listing Requirements and International Best Practices.

The results of the web analysis show that industry sector influences the disclosure of information in companies' annual reports relating to 'security'. The majority of disclosed information on 'security' was shown predominantly by two industries, Trading/Services and Finance. The results of this website analysis support the study by Yeh et al (2007), where industry type was among the factors that influenced organisations to adopt security counter-measures; over 109 Taiwanese organisations including large companies, the two industries, 'general manufacturing' and 'banking/financial' appeared heavily in the implementation of IS/IT security.

Research Question 1: The results of the website analysis show ideas similar to those in the model of IS/IT security governance, where the elements of the formal and technical components, but not the informal component, were presented in the annual reports from big players in Group A and Group B.

Research Question 2: The website analysis results supported the components interaction over three types of relationships of the model, 1) Formal/Informal relationship (RT1), 2) Formal/Technical relationship (RT2) and 3) Technical/Informal relationship (RT3). Understanding the relationships and reciprocal requirements among the components was critical in achieving good practice of IS/IT security governance.

10.1.2 Interview Analysis

The use of dual analysis improved the understanding of the interview data. The software analysis showed support for the themes used in the literature and the manual content analysis revealed themes similar to those identified in the model of IS/IT security governance. The validity of the

interview data of this study is high because interviews were drawn from the higher group, Group A and Group B and none from Group C. Different perspectives from different backgrounds of designations, years of experience and different industries, including CEOs, CIOs and other senior and junior managers, supported the model of IS/IT security governance in relation to IS/IT security practices.

Research Question 1: Fundamentally, the software analysis supported the elements of the three components of formal, technical and informal, as stated in the literature, including policy relating to IS/IT security, IS/IT security and internal controls, security issues and risk management, organisational structure, educational aspects and informal aspects. The results of software analysis have contributed to the literature.

The across-cases analysis conducted in the manual content analysis found evidence about the development of IS/IT security aspects with regard to the formal, technical and informal components; these findings have reinforced the themes developed in the model of IS/IT security governance. Fundamentally, all the issues identified in the interview data supported the three dimension themes, formal, technical and informal. Most of the results of interview data analysis supported the elements of formal themes, see Figure 10.1, which included IS/IT security vision, IS/IT security management strategy and IS/IT security policy. Some results of the interview data analysis supported the elements of the technical themes of the model, comprising technological resources and IS/IT security procedures, as can be seen in Figure 10.2. While the elements of the informal themes including employee values, organisational values and culture, norms and beliefs, were supported by some results of the interview data, see Figure 10.3.

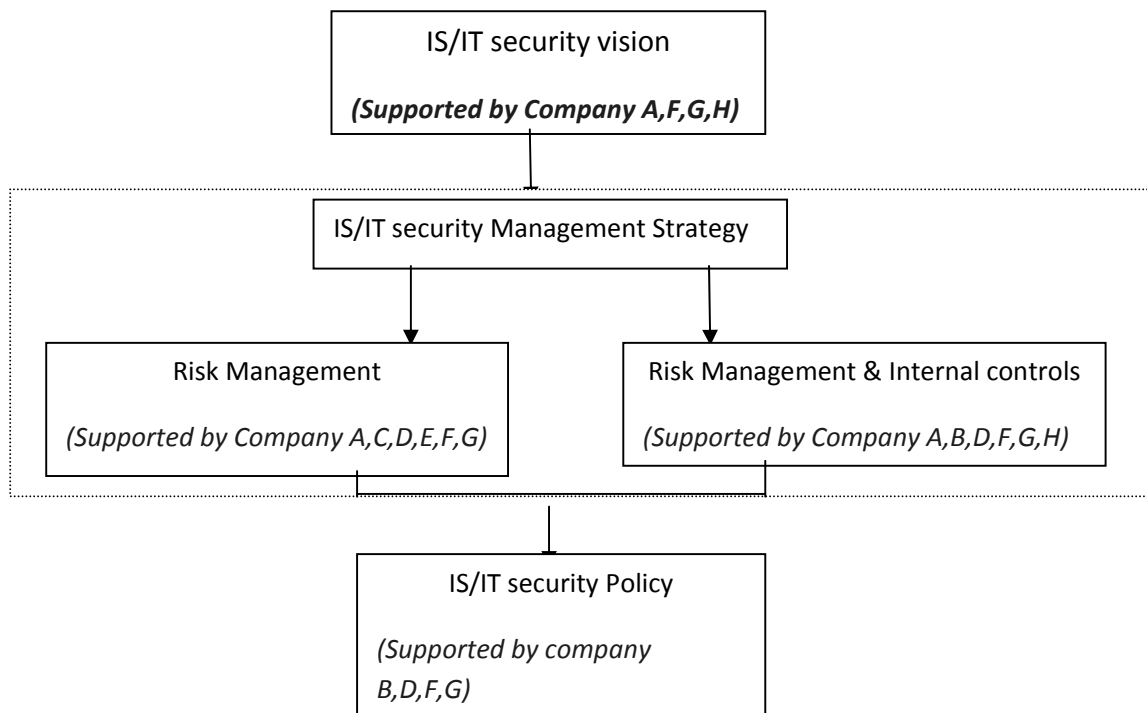


Figure 10.1 Formal component themes of model and supporting data, manual content analysis

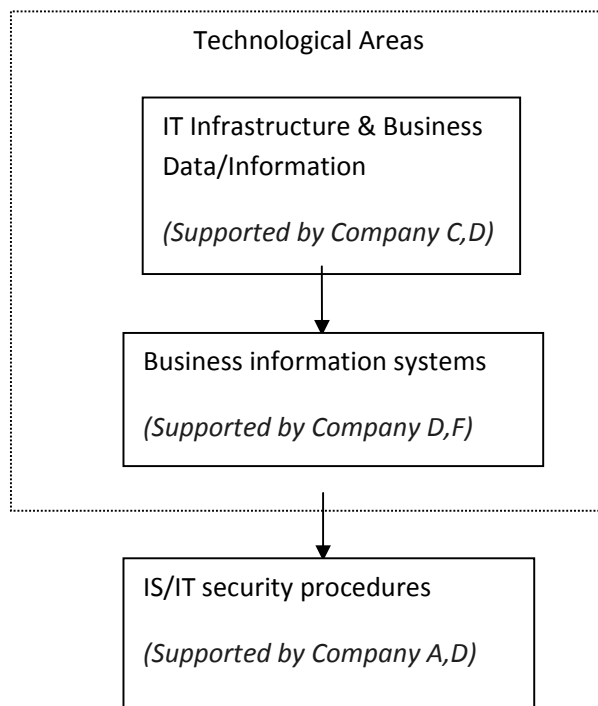


Figure 10.2 Technical component themes and supporting data, manual content analysis

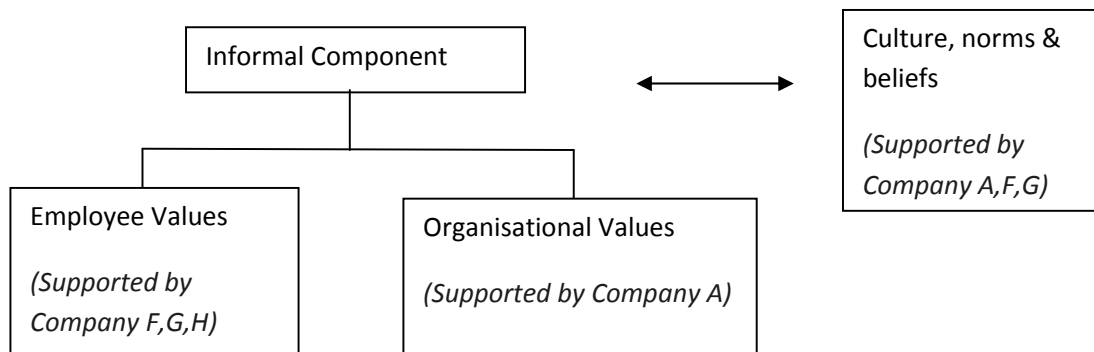


Figure 10.3 Informal component themes of model and supporting data, manual content analysis

Various primary issues, secondary issues and sub-issues that were identified in the data analysis presented rich materials from Group A and Group B, the themes of the model of IS/IT security governance were supported from different roles, views, perspectives, backgrounds, disciplines and different industries.

Research Question 2

Component interaction

The interview data analysis had shown similar ideas within a model of component interaction, the inter-relationship between the formal component, technical component and informal component. There are three types of component interactions that were supported by the interview data analysis, Relationship Type 1-Formal/Informal (RT1), Relationship Type 2-Formal/Technical (RT2) and Relationship Type 3-Technical/Informal (RT3).

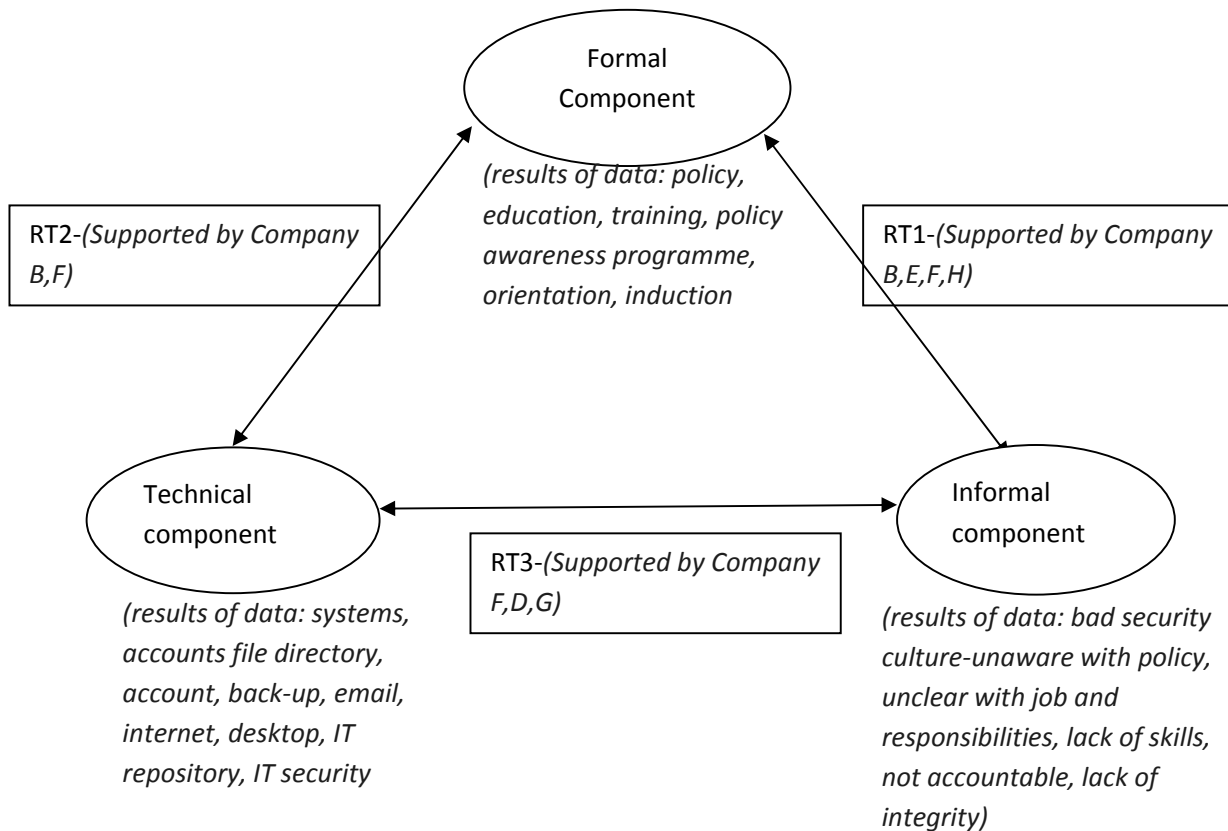


Figure 10.4 The component interaction across multiple companies (cases), the results of manual content analysis and supporting data

Directing and monitoring actions

The software analysis showed that the ‘directing’ and ‘monitoring’ actions were implemented over the three components across all management levels of strategic, tactical and operational levels, hence, supporting the model of IS/IT security governance. The supervision roles between the giver/supervisor of responsibility and the holder of responsibility had been explored, the results of this analysis supported the model of IS/IT security governance in terms of the elements of the formal component including IS/IT security policies, the role of committees and educational aspects (e.g., training, awareness programme) within the IS/IT security implementation. Having policies and organisational structures for IS/IT security in place may facilitate the supervision role between the giver/supervisor of responsibility and the holder of responsibility. Effective supervision roles could improve the ‘directing’ and ‘monitoring’ actions within IS/IT security implementation over the technical and informal components. The results supported the elements of the technical component including the progress of technical procedures implementation by entities/structures (IT department, IT committee, business division and technical group), project implementation methodology and artefacts (operational reports). In the technical component, the new findings of the analysis supported the literature, where IS/IT security implementation requires the integration of different specialists/experts in addressing security problems from different units/departments, ‘the generally applicable framework for an organisational structure of responsibilities’ by William (2007). The analysis supported the

elements of the informal component with regard to culture and employee values (integrity and being professional), where monitoring activities of the informal component are monitored by entities (departments, committees, third party service of technical group) through artefacts (reports from departments/committees, weekly/monthly statistic reports, KRAs).

In the manual content analysis, the single (company) case analysis supported the directing and monitoring action over the three components and component interactions. The content analysis supported the interaction of a component (formal or technical or informal) with another two components (formal or technical or informal) with regard to the directing and monitoring actions in three types of interaction: 1) the Formal component and its interaction (Figure 10.5), 2) the Technical component and its interaction (Figure 10.6) and 3) the Informal component and its interaction (Figure 10.7). The following presented the summary of the directing and monitoring actions over component interaction, identified in three cases, Company A, Company E and Company D.

The Directing and Monitoring actions: The Formal component and its interaction

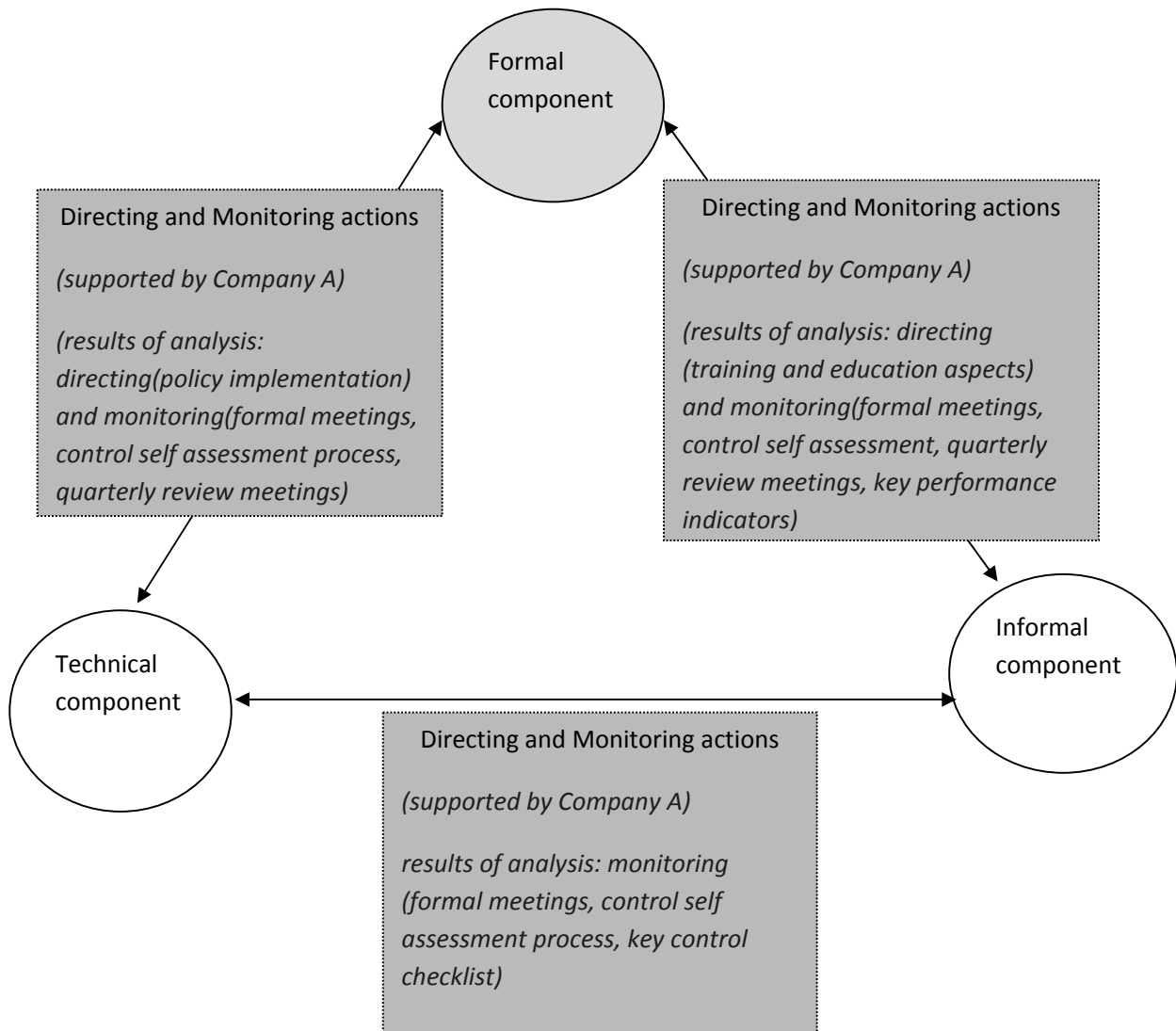


Figure 10.5 The directing and monitoring actions over the Formal component and its interaction and supporting data: by single case (company A)

The Directing and Monitoring actions: The Technical component and its interaction

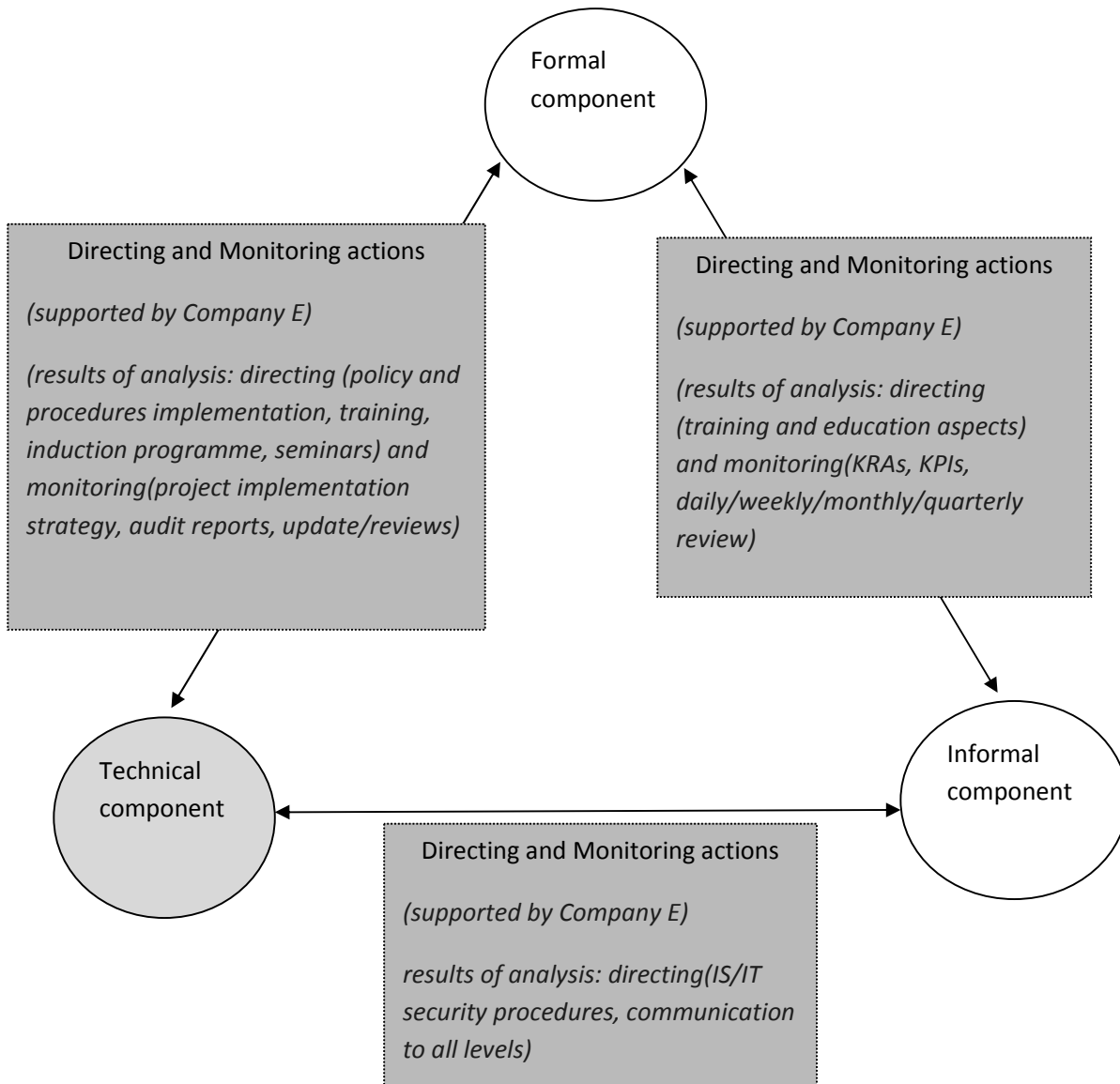


Figure 10.6 The directing and monitoring actions over the Technical component and its interaction and supporting data: by single case (company E)

The Directing and Monitoring actions: The Informal component and its interaction

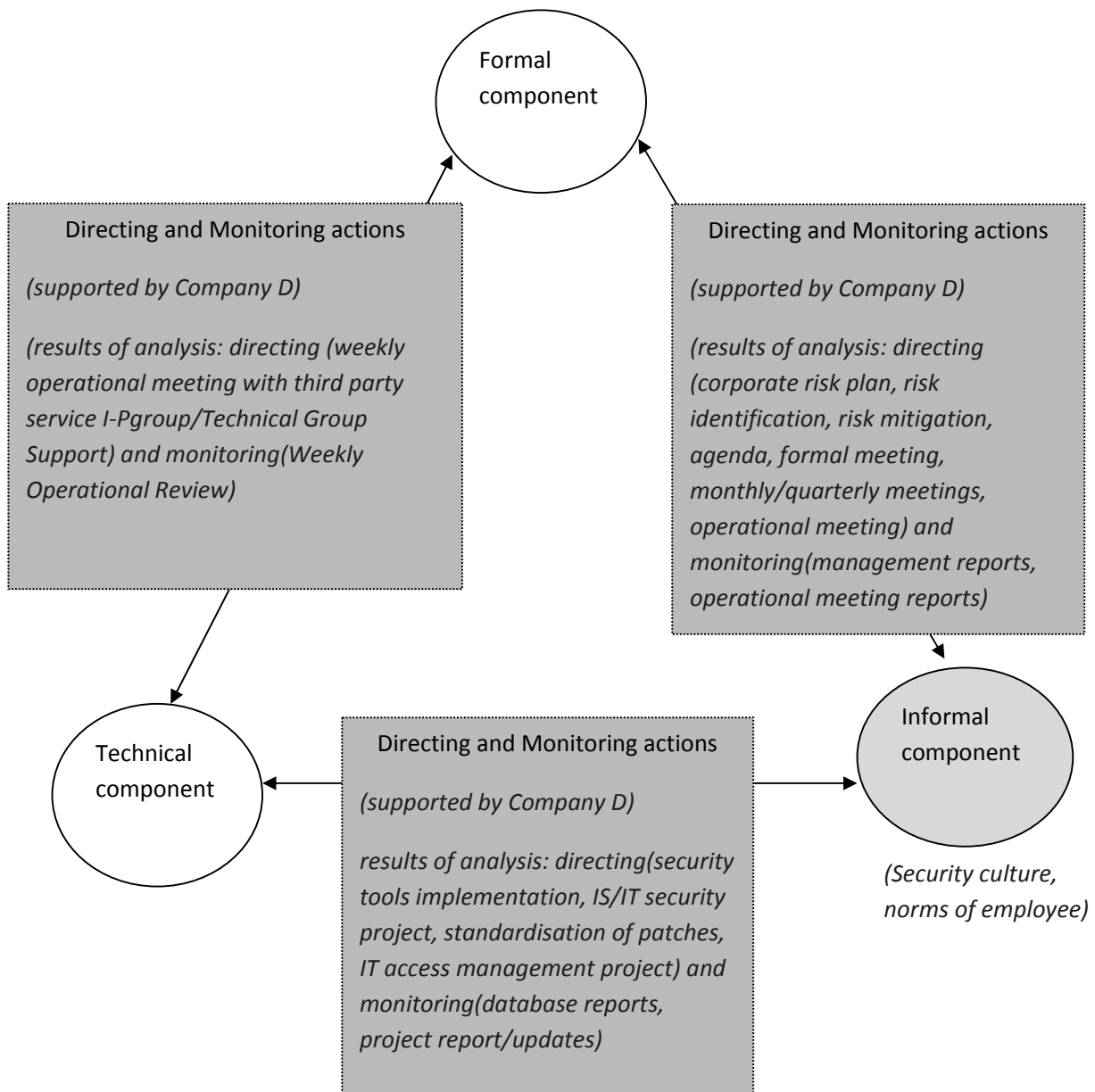


Figure 10.7 The directing and monitoring actions over the Informal component and its interaction and supporting data: by single case (company E)

10.1.3 Survey Analysis

Although the response was low, the survey had high validity as the majority of respondents came from Group A and were senior managers who had more than 10 years of work experience in Malaysian Publicly Listed Companies.

Research Question 1: The majority of the survey results supported the themes that were developed in the model of IS/IT security governance where, fundamentally, the survey supported the elements of two components, formal (Figure 10.8) and informal (Figure 10.9). However, there were no data available relating to the elements of the technical component.

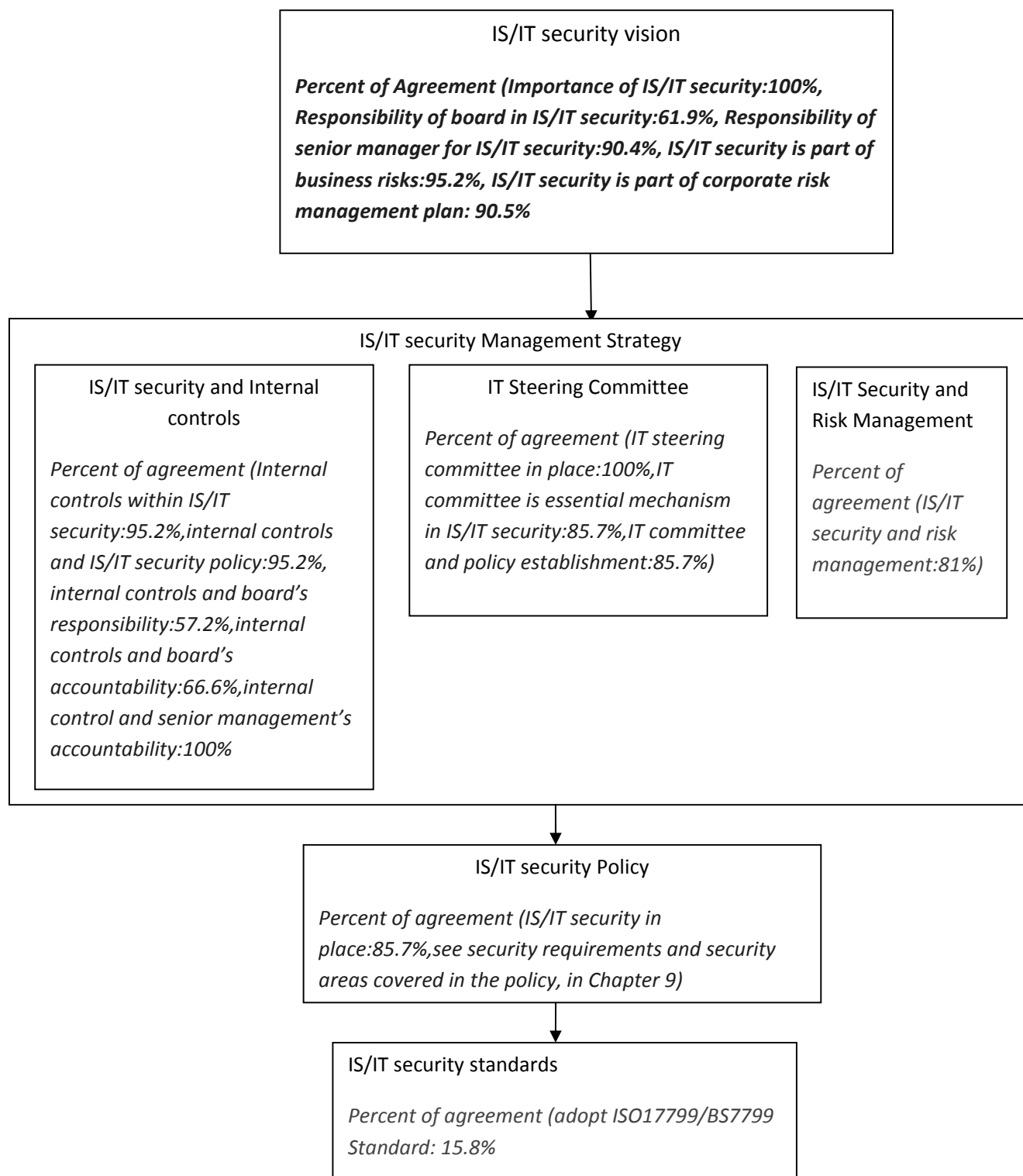


Figure 10.8 The results of survey of formal themes and supporting data

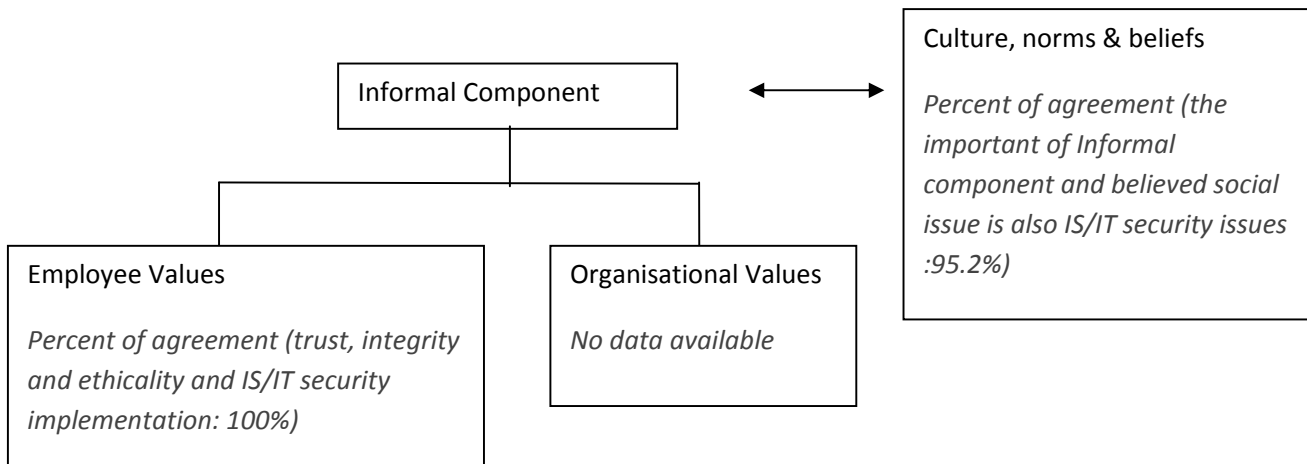


Figure 10.9 The results of Informal themes and supporting data

Research Question 2: The inter-relationship between the three components of formal, technical and informal had been explored and the findings support the component interaction suggested by the IS/IT governance model for two relationships; 1) Formal/Informal relationship Type 1 (RT1) and 2) Formal/Technical relationship Type 2 (RT2). There were no data available relating to the Technical/Informal relationship Type 3(RT3). See Figure 10.10 for the review of data that supported the RT1 and RT2.

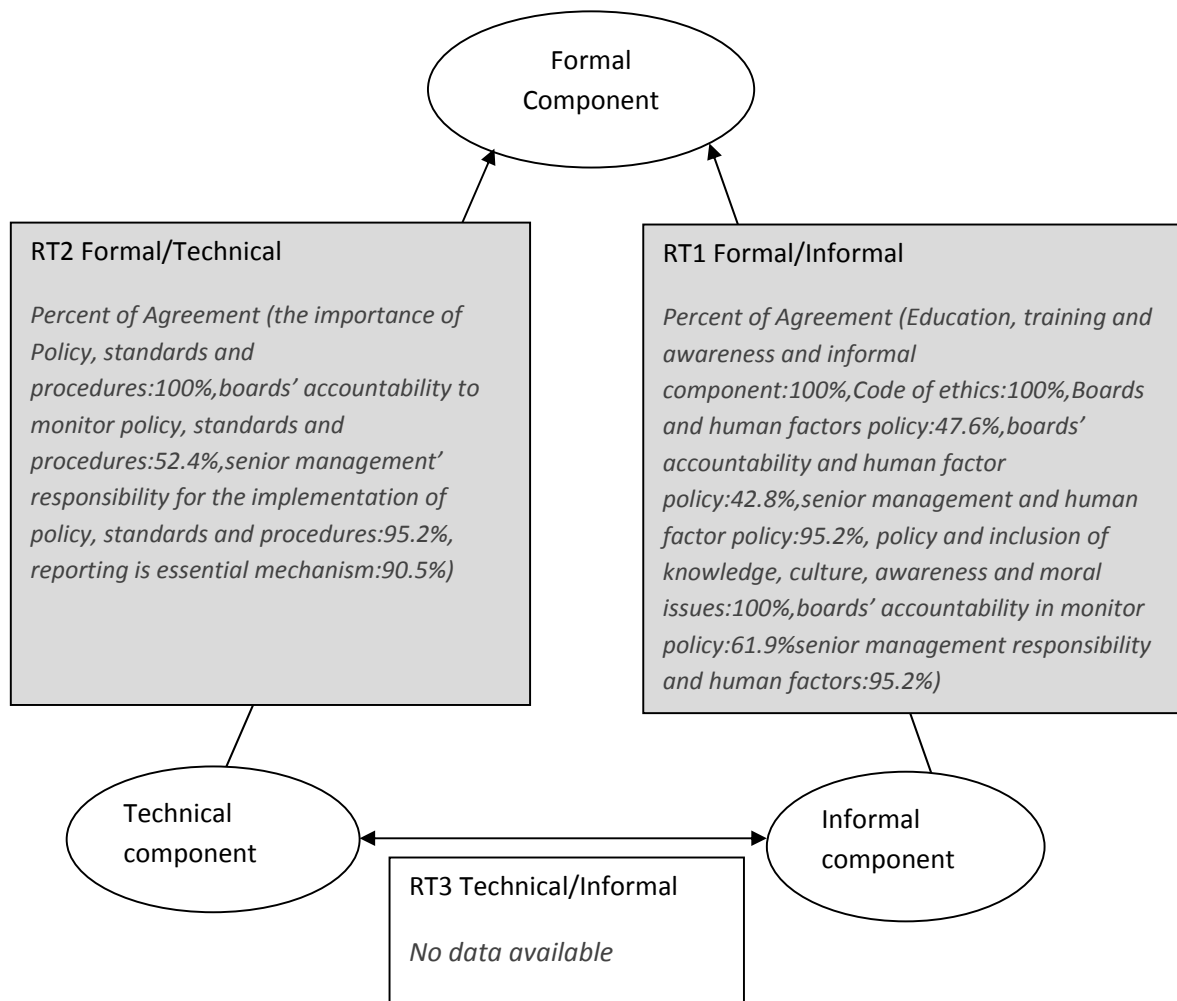


Figure 10.10 Results of survey analysis on component interaction

10.2 Limitations

10.2.1 Literature

The bulk of the literature review was carried out in 2007 when there were few published articles in this area and very little empirical data. Thus, the data collection instruments could not be informed by what other researchers had done. Perhaps the research instruments would have been different if other information had been available. A library search was carried out recently but nothing related specifically to this topic was discovered.

10.2.2 Research methods

10.2.2.1 Interview and Survey

Access to and getting responses from companies' private data were challenging tasks. The reason corporations did not participate in IS/IT security research as claimed by Kotulic et al (2004), as noted in Chapter 5: Research Design and Methodology, still exist.

10.2.2.2 Website data

The website analysis was the first data collection activity conducted, in middle 2008. The website data available during that time were annual report documents (in pdf format) between 2006 and 2008. Therefore, the study was limited to website data before 2008 only.

Unfortunately, researchers in other fields (Gibson, K et al (2007)) have shown that the material appearing in company reports is unlikely to be full disclosure of the knowledge about a particular topic held within the company.

Even so, the formal limitation is that only about one-third of the population was investigated.

10.3 Recommendations for Future Research

10.3.1 Extension, Model on supervision roles

The lack of a model for supervision roles between the giver/supervisor of responsibility and the holder of responsibility offers some potential for future research. A new/extended model could examine how the relationship between the two agents, 1) giver/supervisor and 2) holder of responsibility, could improve the ‘directing’ and ‘monitoring’ actions in corporate governance studies.

10.3.2 Extension, model of component interaction between formal, technical and informal components

Chapter 4 explained in detail how the interaction and reciprocal requirements among the components are crucial in achieving good IS/IT security governance. Future research could test the relationship using statistical methods and hypothesis testing. The mail survey questions could be replicated and adapted by other researchers.

10.3.3 Improving IS/IT security governance and involvement from all participants

Chapter 3 proposed a general organisational structure IS/IT security governance framework for any type of organisation, which increases the interaction between the supervisor and holder of responsibility across all levels, from ground (operational) levels, to middle management level up to top levels. To improve IS/IT security governance, future research could look into the data from various participants from board to low level employees, through interviews or other qualitative methods. The inputs from various participants are important to the IS/IT security governance model because the quality of processes/activities of IS/IT security are more important than the checklists provided by the standards.

10.3.4 Replication study of website analysis over annual reports

The study presumes that the contents of annual reports were similar after 2008 and a replication study could be conducted by other researchers especially if there were new listing requirements or regulations by Bursa Malaysia and the Security Commission relating to IS/IT security. Up to date, there have been few chapter up-dates on the Main Market Listing Requirements, Chapter 2 (General-as at 1 September 2010), Chapter 8 (Continuing Listing Obligations as at 1 September 2010) and Chapter 10

(Transaction-as at 28 January 2011) but there were no new requirements relating to IS/IT security (Bursa Malaysia, 2011).

10.3.5 Improving IS/IT security training among internal employees

Improving and reinforcing training are also important in IS/IT security governance apart from the enforcement of IS/IT security policies and procedures within organisations. Mostly, security incidents are the result of human actions rather than technical problems (McIlwraith et al, 2006). A future research study could develop a model to improve the gap/alignment between the training and technical procedures implementation. The training should be very specific and align with the needs and goals of policies (formal component) and procedures (technical component) requirements. Providing the correct training (if the goal of policies/procedures are matched with training elements) may improve the component interaction between formal (training) and technical (minimise security problems/incidents) and also between formal (training) and informal (minimise human actions, human errors).

A future model also needs to explore the role of supervision between the giver/supervisor of responsibility and the holder of responsibility, over the alignment issue between training and technical procedures implementation. The two elements of corporate governance, 'directing' and 'monitoring' actions should be implemented in a parallel way with the supervision role between the giver and the holder of responsibility, if given a specific security job. The giver/supervisor of a security job needs to ensure that the internal controls over technical training are achieved through effective monitoring and review process. The supervisor of a security job should be able to make correct and efficient decisions, such as in relation to IS/IT security training, what would happen if the training did not reflect the technical procedures, what actions should be taken by the supervisor of the job to improve the training. In this case, the supervisor may seek advice and feedback from IT experts such as IT programmer, whether the training elements were appropriate or less effective against the technical procedures. If less effective, the supervisor should improve the training elements and up-date their within the policies.

10.4 Recommendations for industry and practitioners

In the real world practices, the IS/IT security governance model is suitable for any type of organisation from medium to large corporations, from private to government and also to non-profit organisations within any industry or sector.

There are benefits from this model to industry and practitioners relating to IS/IT security particularly to the giver (supervisor) of the responsibility and the holder of responsibility from top level to bottom level management. Normally, the responsibility of IS/IT security are primarily from policies and procedures.

First, the IS/IT security governance model prescribes the role of supervision in the 'directing' and 'monitoring' actions over the elements of formal, technical and informal components and the component interaction. The elements of the three components and component interaction can be a checklist and indicators for organisations to ensure IS/IT security governance is achieved.

Second, the heart of this model is the inclusion of IS/IT security within risk management and the application internal controls with regard to IS/IT security, the governance structure such as Risk Management Committee, Audit Committee and IT Committee are important to drive organisations to achieve their goals and objectives. Again, the role of supervisor/giver and holder of responsibility should be delegated and discharged effectively in any domain of IS/IT security including within Risk Management and internal controls, to resolve the specific issues at optimum level by incorporating/re-emphasising the component interaction between the formal, technical and informal components. The 'directing' and 'monitoring' are two actions of corporate governance responsibility and should be handled effectively and efficiently by the supervisor and the holder of responsibility. The main purpose of these two actions is to improve IS/IT security governance practices through establishing and monitoring the manual internal controls and automatic IS/IT systems internal controls over the IS/IT security.

For example, the giver (Area Sales Supervisor) or the holder of responsibility (Sales Employee) does not understand their job properly due to lack of management controls in his/her organisation such as the Area Sales Supervisor of responsibility has had not applied internal controls (either manual or automatic IS/IT security internal controls) over the shop retailers. And given the worldwide access card for payment at any retailers, without automatic security controls in place may increase risks and unintended actions such as unauthorised/irresponsible people may swipe or sign the required purchase forms and the amount entered by Sales Employee would be inaccurate/ incorrect. Is it due to people or technical deficiencies? So, from this case the model suggests the Area Sales Supervisor may establish IS/IT security internal controls at multiple retailers, to ensure the correct person performed the transaction and the correct amount was debited from or credited to customer's bank account. As the model prescribes, the Area Sale Supervisor may reinforce the employee values and organisational values through appropriate and effective training to all Sales Employee. The training should cover how to detect unauthorised persons, how to prevent human errors from entering incorrect amount. Several more actions can be discharged by the Area Sale Supervisor until resolved. The role of Sales Supervisor is complex, but if the issues cannot be resolved at his/her level, he/she needs to report and seek consultation from upper level, Chief Marketing Officer, and present why the IS/IT security systems should be in place for security purposes. And now, the status of Sales Supervisor has changed from supervisor (giver) to holder of responsibility and the giver (supervisor) of responsibility has assigned to Chief Marketing Officer. This is a complex process. The Chief Marketing Officer needs to discharge his/her responsibility and make decisions whether to buy/install the IS/IT security internal controls or to look into other perspectives how to resolve the issues, until risks are at minimum level; if the issues cannot be resolved, the organisation has to accept the risks.

The IS/IT security governance process is a complex task which requires the supervisor/giver and the holder of responsibility to resolve the issues at minimum risk in effective and efficient ways, not merely the responsibility of board and senior management. Failure to understand his/her responsibility in discharging IS/IT security may bring potential risks to the organisation, such as money lost and bad reputation name of practicing IS/IT security (not credible company), loss of investors or potential investors for publicly listed corporations.

10.5 Contribution

It is contended that this thesis has made several contributions to this field of study.

First, although there are some limitations which reduce the generalisability of the results, it us a structured study leading to the collection of empirical data. Contact has been made with participants in industry at several levels of authority and responsibility.

Second, the IT/IS security governance model and some of the results have drawn attention to the fact that, in the past, authors have reached conclusions and made suggestions from often uninformed partisan positions.

Third, the suggestions for further research, many of which require empirical work, point out ways in which knowledge in this field can be improved.

Bibliography

- Ahlgren, M., M. Breidne, et al. (2005). "IT Security in the USA, Japan and China -A Study of Initiatives and Trends within Policy, R&D, Industry and Technology." Swedish Institute For Growth Policy Studies: 1-120.
- Armour, M. (2000). "Internal control: Governance framework and business risk assessment at Reed." Auditing, ABI/INFORM Global **19**: 75.
- Australian Stock Exchanges Group (2012). "Rules, Guidance Notes and waivers." Retrieved 18 March 2012, from <http://www.asx.com.au/>.
- Babiak, J., J. Butters, et al. (2005). "Defending the Digital Frontier: Practical Security for Management." John Wiley & Sons Inc, Hoboken, NJ.
- Backhouse, J. and G. Dhillon (1996). "Structures of responsibility and security of information systems." European Journal of Information Systems **5**: 2-9.
- Baker, W. H. and L. Wallace (2007). "Is Information Security Under Control?" IEEE Security & Privacy: 36-44.
- Baskerville, R. (1988). "Designing Information Systems Security." Information Systems Series, John Wiley.
- Bassett, J. (2006) Promoting IT Governance at the CEO Level. Internal Auditor-Global Perspectives on Risk, Control and Governance
- Bazaz, A. and J. D. Arthur (2007). "Towards a Taxonomy of Vulnerabilities." Proceedings of the 40th Annual Hawaii International Conference on System Sciences HICSS'2007.
- Bedell, D. (2006). "Security Complex." Global Finance **20**(6): 25.
- Berhad, B. M. (2008). "Trading Participant Information Technology Security Code (IT Security Code)." Retrieved 14 January 2009, from http://www.bursamalaysia.com/website/bm/rules_and_regulations/bursa_rules/bm_derivatives.html.
- Bhagwan, R., K. Tati, et al. (2004). "Total recall: system support for automated availability management." In NSDI'04: Proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation: 25-25.
- Bishop, M. and D. Bailey (1996). "A Critical Analysis of Vulnerability Taxonomies." Tech. Rep. CSE-96-11 Department of Computer Science at the University of California at Davis.
- Blakley, B., E. McDermott, et al. (2002). "Information Security is Information Risk Management." ACM.
- Boyle, G. and E. G.-. Webb (2007) Sarbanes-Oxley and its Aftermath: A Review of the Evidence, Working paper, University of Canterbury.

- Brian, D. V. (2001). "The Ultimate Defence of Depth: Security Awareness in Your Company." SANS reading room material.
- Burns, R. B. (2000). Introduction to Research Methods. London, Sage Publications.
- Campbell, D. R., M. Campbell, et al. (2006). "Adding Significant Value with Internal Controls." The CPA Journal **76**(6): 20.
- Conner, B., T. Noonan, et al. (2003). Information Security Governance: Toward a Framework for Action. M. International, Business Software Alliance.
- Cooper, A. and B. S. Cornett (2004). "Not Your Accountant's Oldsmobile: Internal Controls Today." Journal of Health Care Compliance.
- Cooper, D. R. and P. S. Schindler (2003). Business Research Methods Boston, McGraw Hill.
- Creswell, J. W. and V. Plano Clark (2007). Designing and Conducting Mixed Methods Research, Thousand Oaks, CA: Sage.
- Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM **43**(7): 125-128.
- Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." Information Systems Journal **11**(2): 127-153.
- Dhillon, G., G. Tejay, et al. (2007). "Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations." Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE.
- Doherty, N. F. and H. Fulford (2006). "Aligning the information security policy with the strategic information systems plan." Computers & Security **25**: 55-63.
- Dutta, A. and K. McCrohan (2002). "Management's Role in Information Security in a Cyber Economy." California Management Review **45**(1): 67-87.
- Englund, T. and F. Ojdemark (2000). Powerplay in industrial sales: A study of the potential of electronic marketplaces in manufacturing companies', University of Linköping.
- Entrust (2003-2004). "Implementing Information Security Governance (ISG): A case study: Entrust." 2007, from <http://download.entrust.com/resources/download.cfm/21636/>.
- Ezingear, J.-N. and D. Birchall (2005). "Information Security Standards: Adoption Drivers." The International Federation for Information Processing: 1-20.
- Farahmand, F., S. B. Navathe, et al. (2003). "Managing Vulnerabilities of Information Systems to Security Incidents." ACM: 348-354.

- Filatotchev, I. (2007). "Corporate Governance and the Firm's Dynamics: Contingencies and Complementarities." Journal of Management Studies **44**(6): 1041-1056.
- Fites, P., P. Johnston, et al. (1989). "The Computer Virus Crisis." Van Nostrand Reinhold, New York.
- National Cyber Security Summit Task Force (2004), "Information Security Governance: A Call To Action." Corporate Governance Report
- Gaunt, N. (2000). "Practical approaches to creating a security culture." International Journal of Medical Informatics **60**(2): 151-157.
- Germain, R. S.-. (2005). "Information Security Management Best Practice Based on ISO/ IEC 17799." Information Management Journal **39**(4): 60.
- Ghose, A. and U. Rajan (2006). "The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition and Social Welfare." Workshop on Economics of Information Security 2006.
- Gilbert, N. (1993). Researching Social Life. London, Sage Publications.
- Gill, J. and P. Johnson (1997). Research Methods for Managers. London, Paul Chapman Publishing.
- Gordon, L. A., M. P. Loeb, et al. (2006). "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities."
- Hafner, K. and J. Markoff (1991). Cyberpunk: Outlaws and Hackers on the Computer Frontier.
- Haniffa, R. and M. Hudaib (2006). "Corporate Governance Structure and Performance of Malaysian Listed Companies." Journal of Business Finance & Accounting **33**(7 & 8): 1034-1062.
- Hardy, G. (2006). "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges." Information Security Technical Report **11**(01): 55-61.
- Hellreigle, D., J. Slocum, et al. (1998). Organizational Behaviour (Eight Edition), OH: South-Western College.
- Herath, T. and H. R. Rao (2009). "Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness." Elsevier **47**: 154-165.
- Hone, K. and J. H. P. Eloff (2002a). "What makes an Effective Information Security Policy?" Network Security(6): 14-16.
- Hone, K. and J. H. P. Eloff (2002b). "Information security policy- what do international information security standards say?" Computers & Security **21**(5): 402-409.
- Huczynski, A. and D. Buchanan (2001). "Organisational Behaviour: An Introductory Text." Prentice Hall Europe.

- Hurst, N. W. (1998). "Risk Assessment: The Human Dimension." The Royal Society of Chemistry, Information Services.
- Icove, D., K. Seger, et al. (1999). Computer Crime- A Crime fighter's Handbook, O'Reilly & Associates, Inc.
- Institute, I. G. (2006). "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition."
- Kotulic, A. G. and J. G. Clark (2004). "Why there aren't more information security research studies." Information & Management **41**: 597-607.
- ISO/IEC. (2000). "ISO/IEC 17799: Information Technology-Code of Practice for Information Security Management."
- ITGI, I. G. I. (2003). "Board Briefing on IT Governance." 2007, from www.itgi.org.
- ITGI, I. G. I. (2005). "COBIT 4.0." 2006, from www.itgi.org.
- ixon, R., C. Marston, et al. (1992). "A report on the joint CIMA and IIA computer fraud survey." Comput Sec **11**(4): 307-313.
- Jensen, B. K., M. Cline, et al. (2007). "HIPPA, PRIVACY and Organisational Change: A Challenge for Management." SIGCAS Computers and Society **37**(1): 12-17.
- Johnson, P. and J. Duberly (2000). Understanding Management Research: An introduction to Epistemology, Sage Publications.
- Jr, W. R. K. (2000). "Research opportunities in internal control quality and quality assurance." Auditing, ABI/INFORM Global **19**: 83.
- Kizirian, T. and W. R. Leese (2004). "Security Controls and Management Tone." Internal Auditing, ABI/INFORM Global **19**(2): 42.
- Knapp, K. J., T. E. Marshall, et al. (2006). "Information security:management's effect on culture and policy." Information Management & Computer Security **14**(1): 24-36.
- Kritzinger, E., v. Solms, et al. (2003). "Information security: A Corporate Governance Issue." Integrity and Internal Control in Information Systems, International Federation for Information Processing (IFIP): 115.
- Labovitz, G. and V. Rosansky (1997). The Power of Alignment. New York, NY, USA, John Wiley & Sons, Inc.
- Lancaster, G. (2005). Research Methods in Management: A concise introduction to research in management and business consultancy, Elsevier.
- Landwehr, C. E. (1981). "Formal Methods for Computer Security." ACM Computing Surveys **13**(3): 247-278.

- Leximancer Manual (2009). "Leximancer Manual Version 3.07." 2010, from www.leximancer.com.
- Liew, P. K. (2006). "The (Perceived) Roles of Corporate Governance Reform in Malaysia: The Views of Corporate Practitioners." Working Paper 06-02 April 2006.
- Lin, P. P. (2006). "Systems security threats and controls." The CPA Journal, ABI/INFORM Global **76**(7): 58.
- Lindlof, T. R. and B. C. Taylor (2002). Qualitative Communication Research Methods. Thousand Oaks, CA, Sage Publications.
- Lineman, D. J. (2007). "Building and Deploying Effective Security Policies." Information Shield, Inc.
- Madnick, S. E. and J. K. Donovan (1973). "Application and analysis of the virtual machine approach to information system security and isolation." Proceedings of the workshop on virtual computer systems.
- Malaysian Listed Companies." Journal of Business Finance & Accounting **33**(7 & 8): 1034-1062.
- McCuaig, B. (2007). "Three Principles For Better Internal Control Over Financial Reporting." Internal Auditing, ABI/INFORM Global **22**(3): 19.
- McIlwraith, A. (2006). "Information Security and Employee Behaviour." Gower Publishing Company(Presses Universitaires de Namur): 465-472.
- Mishra, S. and G. Dhillon (2007). "Information Systems Security Governance Research: A Behavioral Perspective." Annual NYS Cyber Security Conference.
- Nachtigal, S. (2007). "eBPSM- A New Security Paradigm for E-Business Organisations." ACM.
- Naedele, M. (2007). "Addressing IT security for Critical Control Systems." Proceedings of the 40th Hawaii International Conference on System Sciences.
- Oakley, A. (1999). People's way of knowing: gender and methodology, in S.Hood, B. Mayall and S.Oliver, Critical Issues in Social Researcher: Power and Prejudice. Buckingham, Open University Press.
- OECD (1999). "OECD Principles of Corporate Governance." Retrieved 12 May 2007, from www.oecd.org/daf/corporateaffairs/principles/text.
- OECD (2002). "OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security." Retrieved 15 December 2010, from http://www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html.
- O'Leary, C., E. Iselin, et al. (2006). "The Relative Effects of Elements of Internal Control on Auditors' Evaluations of Internal Control." Pacific Accounting Review: Accounting & Tax Periodicals **18**(2): 69.

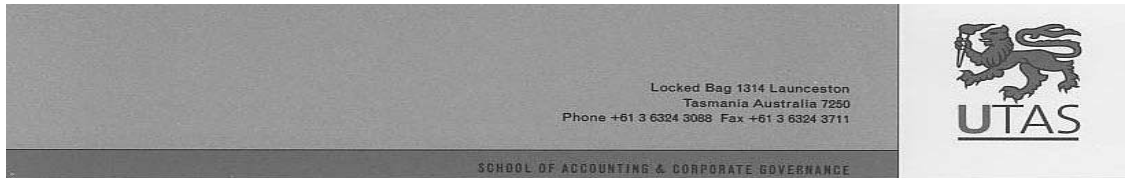
- O'Leary, D. E. (2000). Enterprise resource planning systems: Systems, Life Cycle, Electronic Commerce and Risk, Cambridge University Press.
- Osborne, M. (2006). "Information Security Standards and Audits." Elsevier, Science Direct(87-110).
- Porter, M. E. (1985). Competitive Advantage: Creating and Sustaining Superior Performance, Free Press.
- Posthumus, S. and R. v. Solms (2004). "A framework the governance of information security." Computers & Security **23**(8): 638-646.
- Radianti, J. and J. J. Gonzalez (2007). "Understanding Hidden Information Security Threats: The Vulnerability Black Market." 40th Annual Hawai International Conference on System Sciences: 156.
- Rainer, R. K. and C. G. Cegielski (2011). Introduction to Information Systems: Enabling and Transforming Business, John Wiley & Sons.
- Report, K. (2002). The King Report on Corporate Governance for South Africa. King Committee on Corporate Governance. Parktown, South Africa, Institute of Directors in Southern Africa.
- Robson, W. (1997). Strategic Management & Information Systems, Prentice Hall-Financial Times.
- Rogers, V. C., T. A. Marsh, et al. (2004). "Internal Controls: Winning the battle against risks." Internal Auditing, ABI/INFORM Global **19**(4): 28.
- Rudolph, K. (2000). "Security Awareness Metrics: Measure what matters." Retrieved 25 November 2008, from <http://nativeintelligence.com/index.aspx>.
- Securities Commission Malaysia (2000). "The Malaysian Code on Corporate Governance." Finance Committee on Corporate Governance, Perpustakaan Negara Malaysia. from www.sc.com.my.
- Services, U. S. D. o. H. H. (2003). "Summary of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) " Office for Civil Rights.
- Silverman, D. (2009). Doing Qualitative Research: A Practical Handbook. Thousand Oaks, CA, Sage Publications.
- Sinclitico, G. (2007). "Management Controls Have Finally Gone Away!" The Armed Frces Comptroller, Accounting & Tax Periodicals **52**(2): 21.
- Siponen, M. T. and H. Oinas-Kukkonen (2007). "A review of Information Security Issues and Respective Research Contributions." The DATA BASE for Advances in Information Systems **38**(1).
- Siponen, M. T. and H. Oinas-Kukkonen (2007). "A review of Information Security Issues and Respective Research Contributions." The DATA BASE for Advances in Information Systems **38**(1).
- Solms, B. v. (2001). "Corporate Governance and Information Security." Computers & Security **20**(3).

- Solms, B. v. (2001). "Information Security- A Multidimensional Discipline." Computers & Security **20**(6): 504-508.
- Solms, B. v. (2005). "Information Security governance: COBIT or ISO 17799 or both." Computers & Security **24**: 99-104.
- Solms, B. v. (2006). "Information Security- The Fourth Wave." Computers & Security **165-168**.
- Solms, R. v. and B. v. Solms (2004). "From policies to culture." Computers & Security **23**(4): 275-279.
- Solms, R. v. and S. h. B. v. Solms (2006). "Information security governance: A model based on the Direct-Control." Computers & Security **25**(6): 408-412.
- Stanton, J. M., K. R. Stam, et al. (2004). "Analysis of end user security behaviors." Computers & Security.
- Standards Australia and Standards New Zealand (2004), AS/NZS 4360: 2004, Risk Management Guidelines, NSW, ISBN 0 7337 59041
- Straub, D. W. and R. J. Welke (1998). "Coping with systems risk: Security planning models for management decision making." MIS Quarterly **22**(4): 441-469.
- Su, X., D. Bolzoni, et al. (2006). "A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements." 11th International Workshop on Exploring Modeling methods in Systems Analysis and Design (EMMSAD2006)
- Swanson, R. M. (1999). "Internal Controls: Tools, not hoops." Strategic Finance, ABI/INFORM Global **81**(3).
- Tashkkori, A. and C. Teddlie (2003). Handbook of Mixed Methods in Social and Behaviour Research, Sage Publications.
- Tharenou, P., R. Donohue, et al. (2007). Management Research Methods. Cambridge University Press.
- Ticehurst, G. W. and A. J. Veal (2000). Business research methods: A managerial approach. NSW, Australia, Pearson Education.
- Torres, J. M., J. M. Sarriegi, et al. (2006). "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness." ISC LNCS **417**: 530-545.
- V.Koskosas, I. and R. J.Paul (2004). "The Interrelationship and Effect of Culture and Risk Communication in Setting Internet Banking Security Goals." Sixth International Conference on Electronic Commerce(ICEC'04).
- Van Grembergen, W. (2002). "Introduction to the Minitrack: IT Governance and its mechanisms." Proceedings of the 35th Hawaii International Conference on System Sciences (HICCS).

- Varadharajan, V. (2007). "Researching Security in Organisations." EII Winter School, ARC Research Networks.
- Veal, J. (2005). Business Research Methods: A Managerial Approach, Pearson Addison Wesley.
- Waloff, I. (2002). "Speech by at "7799 Goes Global" conference." 2008, from <http://www.bsi-global/News/Releases/2002/September/n3f029de8c689a.xalter>.
- Ward, J. (2002). "Developing a culture of information security." Proceeding of the 19th World Conference on Computer Security Audit and Control: 193-200.
- Ward, J. (2005). "Operational Risk and Information Security need to co-exist if businesses want to effectively manage risks." Credit Control, ABI/INFORM Global **26**(7): p. 18.
- Whitman, M. E. (2003). "Enemy At The Gate: Threats To Information Security." Communications of the ACM **46**(8): 91-95.
- Wiant, T. L. (2005). "Information security policy's impact on reporting security incidents." Computers & Security **24**(6): 448-459.
- Williams, P. (2007). "Executive and board roles in information security." Network Security **8**: 11-14.
- Wood, C. (1990). "Principles of secure information systems design." Computer & Security **9**(1): 13-24.
- Wood, C. C. (2002). "Don't Let Role of Information Security Policies in the Arthur Andersen/Enron case go Without Mention to your Chief Executive Officer " Computer Fraud & Security **5**: 11-13.
- Yeh, Q.-J. and A. J.-T. Chang (2007). "Threats and countermeasures for information system security: A cross-industry study." Information & Management.
- Yngstrom, L. (2006). "Can We Tune Information Security Management Into Meeting Corporate Governance Needs?" Security Management, Integrity, and Internal Control in Information Systems: 237-245.
- Zakaria, O. (2005). "Employee Security Perception in Cultivating Information Security Culture." The International Federation for Information Processing.
- Zakaria, O. and A. Gani (2003). "A Conceptual Checklist of Information Security Culture." Proceeding of the 2nd European conference on Information Warfare and Security, MCIL, Reading, England: 365-371.

Appendices

Appendix 5A: Cover Letter with Information Sheet



Nadianatra Musa,
School of Accounting and Corporate Governance,
University of Tasmania, Hobart Campus,
Sandy Bay 7005,
Hobart, Tasmania,
Australia
Tel: +61-420387552

XX/XX/2009

CEO/CFO/CIO/Junior Managers,

Address

Invitation to Participate

Interviews “The Involvement of the Board of Directors and Senior Management in IT/IS Security Governance”

Dear [CEO/CFO/CIO/Junior Managers],

I am Nadianatra Musa, a doctoral student in the School of Accounting and Corporate Governance at the University of Tasmania. I am undertaking a research study that looks at “The Involvement of the Board of Directors and Senior Management in IT/IS Security Governance” within Malaysian publicly listed companies. To collect the necessary data I will be speaking with a number of people, at varying levels, within a number of organisations to gain the necessary insights to understand the involvement of the board of directors and senior managers in IT/IS Security Governance. I invite your participation and look forward to a positive response.

This study requires information from individuals including the Chief Executive Officer, Chief Accounting Officer, Chief Information Officer, two junior level Accounting Managers and the IT/IS Manager where possible. *[CEO letter only - I would be grateful if not only you would agree to participate but allow me to also speak with other members of your team holding the above positions.]* I have enclosed the Information Sheet to provide you with information addressing the purpose of the study, the reason why you have been selected, a description of interview procedures and the potential benefits/risks resulting from this study.

For your information, the study has been reviewed and approved by the University of Tasmania-Human Ethics Research Committee (HRECS) Tasmania Network. The HRECS has determined that this study meets the ethical

obligations by National Statement on Ethical Conduct in Human Research, Australian Government and University policies (HRECS No.). If you have any ethical issues with this project you should contact Executive Officer of the HRECS (Tasmania) Network on (03) 6226 7479 or email human.ethics@utas.edu.au. If you have questions or concerns regarding this study, please contact the investigator, Nadianatra Musa by telephone: (61- 4-20387552); by email: (nmusa@utas.edu.au) and supervisors, Associate Professor Dr Trevor Wilmshurst by telephone: (61-3-63243570); by email: (Trevor.Wilmshurst@utas.edu.au), Dr Gail Ridley by telephone: (61-362262313); by email: (Gail.Ridley@utas.edu.au) and Dr Vishv Malhotra by telephone: (61-362262944); by email: (Vishv.Malhotra@utas.edu.au).

I hope that you will be able to participate in this study.

Sincerely,

Nadianatra Musa

PARTICIPANT INFORMATION SHEET

SOCIAL SCIENCE/ HUMANITIES RESEARCH

THE INVOLVEMENT OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT IN IT/IS SECURITY GOVERNANCE.

Invitation to participate in the interview about IT/IS Security Governance

I am undertaking a research study for my doctorate that considers the involvement of the Board of Directors and Senior Management in IT/IS Security Governance. I have chosen this area of study as IT/IS security does not only deal with technological issues but also considers a corporate governance challenge. Therefore, this study looks at how the responsibilities of IT/IS security and the confidentiality, integrity and availability of information are shared between business and IT/IS at the board of directors and senior management level as the latter are responsible for the key success or failure of corporation.

My name is Nadianatra Musa. I am a PhD student within the School of Accounting and Corporate Governance at the University of Tasmania in Australia. This project is being supervised by Associate Professor Dr Trevor Wilmshurst, Dr Gail Ridley, (School of Accounting and Corporate Governance), and Dr Vishv Malhotra, (School of Computing and Information Systems).

1. 'What is the purpose of this study?'

The purpose of this study is to investigate how the board and senior management of Malaysian publicly listed companies are involved in directing and monitoring the formal, informal and technical dimensions of IT/IS security.

These dimensions are identified as:

Formal dimension - IT/IS security policies, standards, procedures, guidelines, administrative and practices relating to IT/IS security.

Informal dimension - Ethics, security training, education and awareness.

Technical dimension - IT/IS security controls and network or internet security.

The study will also examine whether IT/IS and its resources are directed and monitored effectively and efficiently to ensure security objectives are achieved as intended.

2. 'Why have you been invited to participate in this study?'

This study is about the views of persons employed within publicly listed companies in the Bursa Saham Malaysia. Your company is listed, and has been selected as the research study seeks information that is related

to IT/IS security governance variables. It is believed that you will be able to offer insights into this study which aims to investigate the role of corporate governance in the implementation of IT/IS security. It is expected that you will have an understanding of relevant issues including information about IT/IS security, associated internal controls and risk management plans that have been established to safeguard the firm.

3. 'What does this study involve?'

This part of the study involves a mail questionnaire survey. This questionnaire supplements interviews undertaken, and content analysis of relevant content reported in the annual report of your company. The questionnaire survey will take approximately 30 minutes to complete. The questionnaire survey focuses on the involvement of the board and senior management in directing and monitoring actions of IT/IS security governance within Malaysian Publicly Listed Companies.

There are two envelopes attached in here; the reply paid envelope and the request form. Please return your questionnaire in the reply paid envelope for questionnaire. If you would like a copy of research findings of this study, please fill up the request form and return to provided envelope. In the request form, you may indicate whether you willing to be interviewed or not.

It is anticipated that data will be analysed from November 2009.

Your involvement in this study is voluntary though we would be delighted if you participate. This survey is completely anonymous and no attempt will be made to link companies to participant names. However, each questionnaire will have B, M or T in the top right hand corner. This signifies that your company is listed in the bottom (B), middle (M) or top (T) 100 listed companies by market capitalization. All of the research will be stored securely in a locked cabinet within the School of Accounting and Corporate Governance, University of Tasmania, Hobart Campus. Access to this cabinet is available only to authorised persons. After the 5 year date from publication, all written data and paper documents which have been stored in a locked cabinet within the School of Accounting and Corporate Governance will be shredded and CDs on which questionnaire survey data was backed up will be destroyed. The researcher's computer which is located at Room 104, Annexe Building will be reformatted by IT staff to erase questionnaire survey data once the doctorate program has been completed and researcher has returned to Malaysia.

4. Are there any possible benefits from participation in this study?

This study may contribute to improvements in best practice for IT/IS security implementation by board of directors and senior management in Malaysian Publicly Listed Companies. It may also result in a better understanding that IT/IS security is not a technological issue but also as a governance issue.

5. Are there any possible risks from participation in this study?

There are no known health and safety risk from participating in this study. The data gathered through the interview will be secured and will not be directly attributable to the interview or their organisation.

6. What if I have questions about this research?

If you would like to discuss any aspect of this study please feel free to contact:

Nadianatra Musa by telephone: (61-3-62267224); by email: (nmusa@utas.edu.au)

Associate Professor Dr Trevor Wilmshurst by telephone: (61-3-63243570); by email: (Trevor.Wilmshurst@utas.edu.au)

Dr Gail Ridley by telephone: (61-362262313); by email: (Gail.Ridley@utas.edu.au)

Dr Vishv Malhotra by telephone: (61-362262944); by email: (Vishv.Malhotra@utas.edu.au).

Any of us would be happy to discuss any aspect of the research with you. Once we have analysed the information we will mail /email you a summary of our findings, if you would like one. You are welcome to contact us after the interview has taken place to ask for a copy of summary, or to discuss any issue relating to the research study.

This study has been approved by the Tasmanian Social Science Human Research Ethics Committee. The HRECS number is H10664. If you have concerns or complaints about the conduct of this study should contact the Executive Officer of the HREC (Tasmania) Network on (61-3-6226 7479) or email human.ethics@utas.edu.au. The Executive Officer is the person nominated to receive complaints from research participants.

Thank you for taking the time to consider this study.

Your completion and return of this questionnaire will signify your consent to participate in this study.

This information sheet is for you to keep.

Appendix 5B: Cover Letter and Questionnaire

Nadianatra Musa
Hobart Campus, Faculty of Business
Commerce Building, Room 509
Private Bag 86 Hobart
Tasmania 7001 Australia
Phone +61(03) 6226 7224 Fax +61(03) 6226 7845
Email nmusa@utas.edu.au
Website Address <http://www.utas.edu.au/accg>



School of Accounting and Corporate Governance

«FirstName» «LastName»
«JobTitle»
«Company»
«Address1»
«Address2» «City»
«State» «PostalCode»

<DD/MM/YY>

Dear «FirstName»

I am Nadianatra Musa, a doctoral student in the School of Accounting and Corporate Governance at the University of Tasmania. I am undertaking a research study that looks at “The Involvement of the Board of Directors and Senior Management in IT/IS Security Governance” within Malaysian publicly listed companies. Basically, the study aims to investigate and explore both the awareness and the current status of involvement of the Board of Directors and Senior Management in IT/IS security governance.

A part of this project involves a mail survey. I would be delighted if your corporation could be part of the process. The views and opinions from your corporation will make an invaluable contribution to this research. Would you be able to respond to the attached questionnaire. It is envisaged that this mail survey would take approximately 30 minutes to complete. I invite your participation and look forward to a positive response.

As a research student at the University of Tasmania, I am bound by the University's strict rules of confidentiality. There will be no attempt made to identify your corporation in any published material and all raw data collected from this study will be stored at the School of Accounting and Corporate Governance for a period of five years from publication. At the expiry of this five year period, the data will be destroyed in line with established University procedures. Subject to the University's copyright, I would be most happy to give you access to my findings relating to your firm and a copy of my thesis after it has been examined.

For your information, the study has been reviewed and approved by the University of Tasmania-Human Research Ethics Committee (HRECS) Tasmania Network. The HRECS has determined that this study meets the ethical obligations by National Statement on Ethical Conduct in Human Research, Australian Government and University policies (HRECS No: H10664). If you have any ethical issues with this project you should contact Executive Officer of the HRECS (Tasmania) Network on (61-3-62267479) or email human.ethics@utas.edu.au. If you have questions or concerns regarding this study, please contact the investigator, Nadianatra Musa by telephone: (61-3-62267224); by email: (nmusa@utas.edu.au) and supervisors, Associate Professor Dr Trevor Wilmshurst by telephone: (61-3-63243570); by email: (Trevor.Wilmshurst@utas.edu.au), Dr Gail Ridley by telephone: (61-3-62262313); by email:

(Gail.Ridley@utas.edu.au) and Dr Vishv Malhotra by telephone: (61-3-62262944); by email: (Vishv.Malhotra@utas.edu.au).

Your participation would be appreciated and I look forward to receiving your completed questionnaire by the end of November. Your reply can be returned to my collection base at Faculty of Computer Science and IT, Universiti Malaysia Sarawak (UNIMAS), 94300 Kota Samarahan, Sarawak, Malaysia in the prepaid envelope supplied.

I hope that you will be able to participate in this study.

Sincerely,

A handwritten signature in black ink, appearing to be 'Nadianatra Musa', with a stylized, somewhat abstract shape.

Nadianatra Musa

QUESTIONNAIRE

The involvement of the Board of Directors and Senior Management in IT/IS Security Governance within Malaysian Publicly Listed Companies

This survey will produce information about the status of IT/IS Security Governance implementation by the Board of Directors and Senior Management within Publicly Listed Companies in Malaysia. This information will be of benefit to your organisation since it could help the Board of Directors and Senior Management in three ways:

- 1. You will obtain a better understanding of the involvement of Boards of Directors and Senior Management in IT/IS security risk which impacts on the implementation of IT/IS security governance;**
- 2. Assist in understanding how the application of internal controls in directing and monitoring actions within IT/IS security governance can be implemented efficiently and effectively; and**
- 3. This information could assist in providing a foundation for the more effective and efficient implementation of IT/IS security governance in your corporation.**

Directions: This questionnaire is presented in two sections; the first section seeks basic information about your corporation while the second investigates your firm's awareness of and level of importance attached to IT/IS security governance.

Your assistance is greatly appreciated. Please respond to ALL of the items. All responses will be treated as strictly confidential. If you would like a copy of the results, please complete the attached request form and return in the smaller envelope supplied. The request for information will be separated from your completed questionnaire when received.

To assist you in responding to this questionnaire a number of terms used are defined to ensure you understand how I am using these terms in this study.

IT/IS: IT is an abbreviation for 'Information Technology' while IS is an abbreviation for 'Information Systems'. Information Technology is broadly defined as technology, solutions and services of digital infrastructures and different nodes connected to the networks such as computer systems, power grid control systems, a car, a wireless phone, information databases, or other devices (Ahlgren, 2005). Information systems are defined specifically as hardware, software, people, information, people and processes (Theoharidou, 2005).

IT/IS Security: IT/IS security is the process of ensuring information integrity, availability and confidentiality of business information (Baskerville, 1988; Parker, 1998}. Integrity is the process of ensuring information should not be altered and modified by those who are not responsible and only in a way that preserves its correctness and viability. Availability is the process of ensuring information should be available to an authorised person when required in a form useful for its use. Confidentiality is the process of ensuring improper disclosure of information should be prevented.

IT/IS Security can be viewed in three perspectives:

- **Formal Aspects** : The formal aspects of IT/IS security are concerned with organisational issues such as policy related to IT/IS security, the IT Steering Committee and IT/IS security standards.
- **Informal Aspects** : The informal dimension of IT/IS security covers personnel and human aspects such as education, training and security awareness, trust, integrity and ethics.
- **Technical Roles** : The technical aspects of IT/IS security deal with the security of IT/IS areas, techniques and controls such as assets classification and control, communication and operation management, access control security (eg encryption, cryptography, filters, back up and disaster recovery) and system development and maintenance.

IT/IS Security Governance: IT/IS security governance is a subset of corporate governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses corporation resources responsibly, and monitors the success or failure of the corporation security program (IT Governance Institute 2006:17). This refers to the responsibility of the Board of Directors and Senior Management to ensure the confidentiality, integrity and availability of business information are protected from unauthorised access to modification/alteration of the recorded data/information, including the recording process.

IT/IS Security Risk: A type of risk relates to confidentiality, integrity and availability of business information through the usage of IT/IS to support operations, assets and personnel (Wilshusen, 2007). This risk can be compromised in some ways such as through unauthorised access and modification or alteration of the recorded data/information, including the recording process.

Internal Control : Internal control is defined as a process of ensuring IT/IS and its resources are directed and monitored effectively and efficiently so that potential security risks can be identified, assessed and mitigated simultaneously (Sinclitico, 2007).

Section 1: Demographic Details

Direction: Please tick (✓) your answer in the respective boxes.

[1] Role: _____

[2] Education Level

- ☐ Diploma
- ☐ First degree/equivalent
- ☐ Master's degree
- ☐ Doctor of Philosophy
- ☐ Other: _____

[3] Work experience in risk security type area

- ☐ Less than 1 year
- ☐ 1-3 years
- ☐ 4 -6 years
- ☐ 7-9 years
- ☐ More than 10 years

[4] Industry of Company

- ☐ Finance and Insurance

- ☐ Manufacturing
- ☐ Wholesale Trade
- ☐ Retail Trade
- ☐ Agriculture, Forestry and Fishing
- ☐ Property and Business Services
- ☐ Communication Services
- ☐ Construction
- ☐ Mining
- ☐ Transport & Storage
- ☐ Accommodation, Cafes and Restaurants
- ☐ Other: _____

[5] How many employees are there in your whole company?

- ☐ If national level,
 - ☐ Above 3000
 - ☐ 1000-2999

- ☐ 100-999

☐ If multinational level corporation,
Total number of employees in a world

- ☐ Greater 10,000
- ☐ 5000- 9999
- ☐ 3000-4999
- ☐ 1000-2999
- ☐ 100-999

[6]Where is your parent company located?

- ☐ Malaysia
- ☐ Other country,
please specify:

Section 2: IT/IS Security Governance

[7] Does your business have an IT/IS Steering committee?

At Board of Directors Level

☐1 Yes ☐2 No

At Senior Management Level

☐1 Yes ☐2 No

[8] Does your corporation have IT/IS security policy? If not, go to question 11.

☐1 Yes ☐2 No

[9] In IT/IS security policy, security areas that covered in this corporation:

User access management ☐1 Yes ☐2 No

Prevention of viruses & worms ☐1 Yes ☐2 No

Disclosure of information ☐1 Yes ☐2 No

Violation & breaches of security ☐1 Yes ☐2 No

Software development & maintenance ☐1 Yes ☐2 No

[10] The IT/IS security policy in this corporation having the following requirements:

Objectives of the IT/IS security policy ☐1 Yes ☐2 No

IT/IS security principles ☐1 Yes ☐2 No

Roles & responsibilities ☐1 Yes ☐2 No

Violations and disciplinary action ☐1 Yes ☐2 No

Monitoring & review ☐1 Yes ☐2 No

[11] Is IT/IS security a part of your business risk management plan?

☐1 Yes

☐2 No

[12] Are IT/IS security internal controls in place?

☐1 Yes

☐2 No

[13] Has your corporation adopted the following IT/IS security standards?

ISO 17799 / BS 7799

☐1 Yes

☐2 No

Other related standards, please specify: _____

Involvement of the Board of Directors and Senior Management in IT/IS security governance in your corporation.

Please tick (✓) the appropriate ranking

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
14. IT/IS security is important.	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
15.1. IT/IS security risks is the responsibility of the Board of Directors	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

	Strongly Disagree Disagree Neutral Agree Strongly Agree
15.2. Senior Management have significant responsibility for IT/IS security risks.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
16.1. IT/IS security risk is a business risk.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
16.2. IT/IS security risk is part of the Corporate Risk Management Plan.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
17.1. The Board of Directors is responsible for the establishment of IT/IS Security policies.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
17.2. Senior Management have significant accountability in the implementation of IT/IS Security Policy	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
17.3. Security issues covered in the IT/IS security policy are dependent upon business goals	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
17.4 Security issues covered in the IT/IS security policy are dependent upon security objectives	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
17.5. Quality of processes over security controls are essential for the implementation of IT/IS security policy	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
17.6. The implementation of IT/IS security policy requires the involvement of personnel at all levels of the business.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5

18.1. Internal controls are a essential part in the implementation of IT/IS security policies	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
18.2. The Board of Directors is responsible for the implementation of internal controls over IT/IS security risks.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
18.3. The Board of Directors is ultimately accountable for the implementation of internal controls over IT/IS security risks.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
18.4. Senior Management is accountable for the implementation of internal controls for IT/IS security risks.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
19.1. The IT Steering Committee is an essential mechanism to support IT/IS security processes and structures	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
19.2. The IT Steering Committee plays an important role in the establishment of IT/IS security policies.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
20.1. Policy, standards and procedures are the most important elements within IT/IS security.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
20.2. The Board of Directors is accountable to ensure adequate monitoring of the implementation of IT/IS security policy, IT/IS security standards and IT/IS security procedures.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
20.3. Senior Management have responsibility for the implementation of IT/IS security policy, IT/IS security standards and IT/IS security procedures.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5

	Strongly Disagree Disagree Neutral Agree Strongly Agree
20.4. Reporting is an essential mechanism in IT/IS security governance	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
21.1. The Board of Directors has accountability for technical roles as IT/IS security is part of the Corporate Risk Management Plan.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
21.2. The Senior Management has significant responsibility in implementing technical roles as IT/IS security is part of Corporate Risk Management Plan.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
22. For technical roles , the Board of Directors monitors the progress of technical implementation to ensure the resources are used and managed effectively according to business and corporation policy	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
23.1. Education, training and awareness (relating to IT/IS security) are essential aspects relevant to the implementation of IT/IS security governance.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
23.2. Human aspects such as trust, integrity and ethicality are essential aspects that are needed for the implementation of IT/IS security.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
23.3. It is important that the conduct of human factors that relate to IT/IS security be placed in the Corporation's Code of Ethics.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5

24. Human factors are important for IT/IS security as security is not only a technological or organisational issue but also a social issue.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
25. The Board of Directors is responsible for the establishment of policy relating to human factors of IT/IS security.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
26.1. The Board of Directors is ultimately accountable for the establishment of policy relating to human factors of IT/IS security.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
26.2. Senior Management has significant responsibility for the establishment of policy relating to human factors of IT/IS security.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
27. The corporation's policy should include aspects related to IT/IS security such as human factors, knowledge, culture, awareness and moral issues when seeking to achieve IT/IS security governance.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
28.1. The Board of Directors is ultimately accountable to monitor the implementation of human factors related to IT/IS security to ensure these aspects are incorporated effectively according to business and corporation's policy.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5
28.2. Senior Management has a responsibility to monitor the implementation of human factors related to IT/IS security to ensure these aspects are incorporated effectively according to business and corporation's policy.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5

Appendix 5C: The link between survey and research questions

No	Questions of Mail Survey	Research Questions 1 or 2	Conceptual framework
			Section 1,2,3,4,5,6,7 in Chapter 3
1.0	Role	1,2	1.0
2.0	Education Level		
3.0	Work Experience		
4.0	Industry		
5.0	No of Employees if National Level		
5.0	No of Employees if Multi National Level		
6.0	Location Parent Company		
7.0	IT Steering Committee at Board Level	1	1
7.0	IT Steering Committee at Senior Mgmt Level	1	1
8.0	IT/IS security policy in place	1	4
9.0	IT/IS Security Policy Coverage: User Access Mgmt	1	4
9.0	IT/IS Security Policy Coverage: Prevention of viruses & worms	1	4
9.0	IT/IS Security Policy Coverage: Disclosure of information	1	4
9.0	IT/IS security Policy Coverage: Violation & breaches	1	4
9.0	IT/IS security policy coverage: software development & maintenance	1	4
10.0	IT/IS Security Policy Requirements: Objectives of the IT/IS security Policy	1	4
10.0	IT/IS Security Policy Requirements: IT/IS security principles	1	4
10.0	IT/IS Security Policy Requirements: Roles & Responsibilities	1	4

No	Questions of Mail Survey	Research Questions 1 or 2	Conceptual framework
			Section 1,2,3,4,5,6,7 in Chapter 3
10.0	IT/IS Security Policy Requirements: Violations & Disciplinary Action	1	4
10.0	IT/IS Security Policy Requirements: Monitoring & Review	1	4
11.0	IT security and the Risk Management Plan	1	3
12.0	IT security and the internal controls	1	3
13.0	IT security and IT/IS security standards	1	4, 5
14.0	IT/IS security is important.	1	1,2,3
15.1	IT/IS security risks is the responsibility of the Board of Directors	1	2,3
15.2	senior management have significant responsibility for IT/IS security risks.	1	2,3
16.1	IT/IS security risk is a business risk.	1	2,3
16.2	IT/IS security risk is part of the Corporate Risk Management Plan.	1	2,3
17.1	The Board of Directors is responsible for the establishment of IT/IS Security policies.	1	5
17.2	senior management have significant accountability in the implementation of IT/IS Security Policy	1	5
17.3	Security issues covered in the IT/IS security policy are dependent upon business goals	1	4
17.4	Security issues covered in the IT/IS security policy are dependent upon security objectives	1	4
17.5	Quality of processes over security controls are essential for the implementation of IT/IS security policy	1	5
17.6	The implementation of IT/IS security policy requires the involvement of personnel at all levels of the business.	1	4
18.1	Internal controls are a essential part in the implementation of IT/IS security policies	1	5

No	Questions of Mail Survey	Research Questions 1 or 2	Conceptual framework
			Section 1,2,3,4,5,6,7 in Chapter 3
18.2	The Board of Directors is responsible for the implementation of internal controls over IT/IS security risks.	2	5
18.3	The Board of Directors is ultimately accountable for the implementation of internal controls over IT/IS security risks.	2	5
18.4	Senior Management is accountable for the implementation of internal controls for IT/IS security risks.	2	5
19.1	The IT Steering Committee is an essential mechanism to support IT/IS security processes and structures	1	
19.2	The IT Steering Committee plays an important role in the establishment of IT/IS security policies.	1	
20.1	Policy, standards and procedures are the most important elements within IT/IS security.	1	3
20.2	The Board of Directors is accountable to ensure adequate monitoring of the implementation of IT/IS security policy, IT/IS security standards and IT/IS security procedures.	2	3
20.3	Senior Management have responsibility for the implementation of IT/IS security policy, IT/IS security standards and IT/IS security procedures.	2	3
20.4	Reporting is an essential mechanism in IT/IS security governance	1	5
21.1	The Board of Directors has accountability for technical roles as IT/IS security is part of the Corporate Risk Management Plan.	2	5
21.2	The Senior Management has significant responsibility in implementing technical roles as IT/IS security is part of Corporate Risk Management Plan.	2	5
22.0	For technical roles, the Board of Directors monitors the progress of technical implementation to ensure the resources are used and managed effectively according to business and corporation policy	2	5
23.1	Education, training and awareness (relating to IS/IT security) are essential aspects relevant to the implementation of IS/IT security governance	1	5

23.2	Human aspects such as trust, integrity and ethicality are essential aspects that are needed for the implementation of IT/IS security.	1	5
23.3	It is important that the conduct of human factors that relate to IT/IS security be placed in the Corporation's Code of Ethics.	1	5
24.0	Human factors are important for IT/IS security as security is not only a technological or organisational issue but also a social issue.	1	5
25.0	The Board of Directors is responsible for the establishment of policy relating to human factors of IT/IS security.	2	5
26.1	The Board of Directors is ultimately accountable for the establishment of policy relating to human factors of IT/IS security.	2	5
26.2	Senior Management has significant responsibility for the establishment of policy relating to human factors of IT/IS security.	2	5
27.0	The corporation's policy should include aspects related to IT/IS security such as human factors, knowledge, culture, awareness and moral issues when seeking to achieve IT/IS security governance.	1	5
28.1	The Board of Directors is ultimately accountable to monitor the implementation of human factors related to IT/IS security to ensure these aspects are incorporated effectively according to business and corporation's policy.	2	5
28.2	Senior Management has a responsibility to monitor the implementation of human factors related to IT/IS security to ensure these aspects are incorporated effectively according to business and corporation's policy.	2	5

Appendix 5D: Sample of Malaysian Publicly Listed Companies with Market Capitalisation Figures (In Malaysian Ringgit-MYR)

SName	Name	Board	Sector	MarketCap @ 31/12/2008
MISC	MISC BERHAD	MAIN BOARD	TRADING/SERVICES	31,637,134
SIME	SIME DARBY BERHAD	MAIN BOARD	TRADING/SERVICES	31,249,212
PBBANK	PUBLIC BANK BERHAD	MAIN BOARD	FINANCE	31,151,586
TENAGA	TENAGA NASIONAL BHD	MAIN BOARD	TRADING/SERVICES	27,091,546
MAYBANK	MALAYAN BANKING BERHAD	MAIN BOARD	FINANCE	24,893,850
IOICORP	IOI CORPORATION BERHAD	MAIN BOARD	PLANTATION	21,896,125
COMMERZ	BUMIPUTRA-COMMERCE HOLDINGS BERHAD	MAIN BOARD	FINANCE	20,931,755
PETGAS	PETRONAS GAS BERHAD	MAIN BOARD	INDUSTRIAL PRODUCTS	19,391,573
DIGI	DIGI.COM BERHAD	MAIN BOARD	INFRASTRUCTURE PROJECT COS.	16,949,500
PLUS	PLUS EXPRESSWAYS BERHAD	MAIN BOARD	TRADING/SERVICES	14,900,000
GENTING	GENTING BERHAD	MAIN BOARD	TRADING/SERVICES	13,704,081
TMI	TM INTERNATIONAL BERHAD	MAIN BOARD	TRADING/SERVICES	13,587,315
RESORTS	RESORTS WORLD BHD	MAIN BOARD	TRADING/SERVICES	13,338,063
BAT	BRITISH AMERICAN TOBACCO (MALAYSIA) BERHAD	MAIN BOARD	CONSUMER PRODUCTS	12,706,085
YTL	YTL CORPORATION BERHAD	MAIN BOARD	CONSTRUCTION	11,692,071
YTLPOWR	YTL POWER INTERNATIONAL BHD	MAIN BOARD	INFRASTRUCTURE PROJECT COS.	11,106,033
PPB	PPB GROUP BERHAD	MAIN BOARD	CONSUMER PRODUCTS	11,025,149
TM	TELEKOM MALAYSIA BERHAD	MAIN BOARD	TRADING/SERVICES	11,018,398
KLK	KUALA LUMPUR KEPONG BERHAD	MAIN BOARD	PLANTATION	9,500,792
RHBCAP	RHB CAPITAL BERHAD	MAIN BOARD	FINANCE	8,398,551
HLBANK	HONG LEONG BANK BERHAD	MAIN BOARD	FINANCE	8,058,546
PETDAG	PETRONAS DAGANGAN BHD	MAIN BOARD	TRADING/SERVICES	7,152,869
AMMB	AMMB HOLDINGS BERHAD	MAIN BOARD	FINANCE	6,725,735
BJTOTO	BERJAYA SPORTS TOTO BERHAD	MAIN BOARD	TRADING/SERVICES	6,457,924
NESTLE	NESTLE (MALAYSIA) BERHAD	MAIN BOARD	CONSUMER PRODUCTS	6,331,500
UMW	UMW HOLDINGS BERHAD	MAIN BOARD	CONSUMER PRODUCTS	5,624,539
TANJONG	TANJONG PUBLIC LIMITED COMPANY	MAIN BOARD	TRADING/SERVICES	5,363,307
MAS	MALAYSIAN AIRLINE SYSTEM BERHAD	MAIN BOARD	TRADING/SERVICES	5,113,266
ASTRO	ASTRO ALL ASIA NETWORKS PLC	MAIN BOARD	TRADING/SERVICES	4,274,219
HLFG	HONG LEONG FINANCIAL GROUP BERHAD	MAIN BOARD	FINANCE	4,190,016
PARKSON	PARKSON HOLDINGS BERHAD	MAIN BOARD	TRADING/SERVICES	4,124,913
BJLAND	BERJAYA LAND BERHAD	MAIN BOARD	TRADING/SERVICES	3,846,869
GAMUDA	GAMUDA BERHAD	MAIN BOARD	CONSTRUCTION	3,791,686
SARAWAK	SARAWAK ENERGY BERHAD	MAIN BOARD	TRADING/SERVICES	3,543,630
BKAWAN	BATU KAWAN BERHAD	MAIN BOARD	PLANTATION	3,444,013
LMCEMNT	LAFARGE MALAYAN CEMENT BHD	MAIN BOARD	INDUSTRIAL PRODUCTS	3,347,800
MMCCORP	MMC CORPORATION BERHAD	MAIN BOARD	TRADING/SERVICES	3,166,861
F&N	FRASER & NEAVE HOLDINGS BHD	MAIN BOARD	CONSUMER PRODUCTS	3,154,964
SPSETIA	S P SETIA BERHAD	MAIN BOARD	PROPERTY	3,151,765

AFG	ALLIANCE FINANCIAL GROUP BERHAD	MAIN BOARD	FINANCE	2,817,553
BURSA	BURSA MALAYSIA BERHAD	MAIN BOARD	FINANCE	2,708,186
ASIATIC	ASIATIC DEVELOPMENT BERHAD	MAIN BOARD	PLANTATION	2,678,913
IJM	IJM CORPORATION BERHAD	MAIN BOARD	CONSTRUCTION	2,623,495
KLCCP	KLCC PROPERTY HOLDINGS BERHAD	MAIN BOARD	PROPERTY	2,615,408
ORIENT	ORIENTAL HOLDINGS BERHAD	MAIN BOARD	CONSUMER PRODUCTS	2,553,980
AIRPORT	MALAYSIA AIRPORTS HOLDINGS BERHAD	MAIN BOARD	TRADING/SERVICES	2,431,000
SHELL	SHELL REFINING COMPANY (FEDERATION OF MALAYA) BERHAD	MAIN BOARD	INDUSTRIAL PRODUCTS	2,430,000
STAR	STAR PUBLICATIONS (MALAYSIA) BERHAD	MAIN BOARD	TRADING/SERVICES	2,392,946
MAYBULK	MALAYSIAN BULK CARRIERS BERHAD	MAIN BOARD	TRADING/SERVICES	2,390,000
BIPORT	BINTULU PORT HOLDINGS BERHAD	MAIN BOARD	TRADING/SERVICES	2,280,000
AFFIN	AFFIN HOLDINGS BERHAD	MAIN BOARD	FINANCE	2,271,437
BSTEAD	BOUSTEAD HOLDINGS BERHAD	MAIN BOARD	PLANTATION	2,226,529
EONCAP	EON CAPITAL BERHAD	MAIN BOARD	FINANCE	2,218,268
UTDPLT	UNITED PLANTATIONS BERHAD	MAIN BOARD	PLANTATION	2,143,783
IGB	IGB CORPORATION BERHAD	MAIN BOARD	PROPERTY	2,056,608
AIRASIA	AIRASIA BERHAD	MAIN BOARD	TRADING/SERVICES	2,053,691
BJCORP	BERJAYA CORPORATION BERHAD	MAIN BOARD	TRADING/SERVICES	1,845,030
IOIPROP	IOI PROPERTIES BERHAD	MAIN BOARD	PROPERTY	1,660,512
KNM	KNM GROUP BERHAD	MAIN BOARD	INDUSTRIAL PRODUCTS	1,603,168
GUINNESS	GUINNESS ANCHOR BERHAD	MAIN BOARD	CONSUMER PRODUCTS	1,525,595
KFC	KFC HOLDINGS (MALAYSIA) BERHAD	MAIN BOARD	TRADING/SERVICES	1,477,146
AEON	AEON CO. (M) BHD	MAIN BOARD	TRADING/SERVICES	1,474,200
KULIM	KULIM (MALAYSIA) BERHAD	MAIN BOARD	PLANTATION	1,412,714
DRBHCOM	DRB-HICOM BERHAD	MAIN BOARD	INDUSTRIAL PRODUCTS	1,401,597
UBG	UBG BERHAD	MAIN BOARD	FINANCE	1,386,099
TITAN	TITAN CHEMICALS CORP. BHD.	MAIN BOARD	INDUSTRIAL PRODUCTS	1,314,525
LPI	LPI CAPITAL BHD	MAIN BOARD	FINANCE	1,310,932
UEMLAND	UEM LAND HOLDINGS BERHAD	MAIN BOARD	PROPERTY	1,299,075
HSPLANT	HAP SENG PLANTATIONS HOLDINGS BERHAD	MAIN BOARD	PLANTATION	1,272,000
HAPSENG	HAP SENG CONSOLIDATED BERHAD	MAIN BOARD	TRADING/SERVICES	1,264,000
IJMLNT	IJM PLANTATIONS BERHAD	MAIN BOARD	PLANTATION	1,243,684
MPI	MALAYSIAN PACIFIC INDUSTRIES BERHAD	MAIN BOARD	TECHNOLOGY	1,227,824
KENCANA	KENCANA PETROLEUM BERHAD	MAIN BOARD	TRADING/SERVICES	1,181,620
WCT	WCT BERHAD	MAIN BOARD	CONSTRUCTION	1,172,678
JTINTER	JT INTERNATIONAL BERHAD	MAIN BOARD	CONSUMER PRODUCTS	1,161,213
YTL CMT	YTL CEMENT BERHAD	MAIN BOARD	INDUSTRIAL PRODUCTS	1,152,631
AMWAY	AMWAY (MALAYSIA) HOLDINGS BERHAD	MAIN BOARD	TRADING/SERVICES	1,134,261
DIALOG	DIALOG GROUP BERHAD	MAIN BOARD	TRADING/SERVICES	1,123,502
CARLSBG	CARLSBERG BREWERY MALAYSIA BERHAD	MAIN BOARD	CONSUMER PRODUCTS	1,109,081
NCB	NCB HOLDINGS BERHAD	MAIN BOARD	TRADING/SERVICES	1,095,689

Appendix 6A: Foxit Reader

Foxit Reader is a free PDF document viewer. This application supports opening and displaying multiple documents (instances) of Foxit reader in the reading area and allowing for viewing side by side. For example, the Foxit reader can display about 50 PDF documents at one time. The Foxit reader provides an effective and efficient 'search' feature, when specific word(s) is entered in the search box, the contents that related to the words will be highlighted and shown the number of occurrences of searched word(s). These two information; the highlighted texts and number of occurrences are useful outputs of Foxit reader application and become important input for Chapter 6.

Appendix 7A: Leximancer and concept map

The *concept map* presents *conceptual structures*. *Conceptual structures* of the information on a *concept map* are instances and inter-relations of *concepts*. The examples of instances are *concept* and *theme*, and the examples of inter-relations are ‘likelihood percentage (%)’, ‘brightness of label (font)/ray (lines)’ and ‘larger size of nodes (dots)’. The *concept map* was used to explore a *concept* and its relationship with other *concepts* of the interview data relating to IT/IS security governance study.

In Leximancer, *concepts* are collections of words that generally travel together throughout the text analysed. In tables, frequency of the concept is represented by the *likelihood percentage (%)*, and in figures, a frequency of concept is represented by the brightness of the *label* (font), the brightness of the *ray* (lines) and the larger size of *nodes* (dots) in figures. The *concepts* that appear together frequently in the text will be indicated by their closeness on the map.

Themes are the highest level summary of the data output generated by Leximancer. *Themes* set up in Leximancer are different to the manual *themes* that are widely used in the manual practices. *Themes* are generated automatically when popular (frequent) *concepts* are co-located (connectedness) within the clusters of *concepts*. Each theme (represented as a circle) surrounds a cluster of *concepts* (which appear as *labels*). *Themes* are similar to thematic clusters. The relevance score can be used to represent the degree of the connectedness between *concepts* in each *theme* and others on a map. The interpretation of *themes* output also can be seen through the colour of the theme circles where the more connected *themes* are presented in the *red* spectrum. The colour of the theme also indicates the connectedness of its parent *concepts*.

In the Concept Map, there are two important sliders for generating the output visualisation- *Visible Concept Slider* (A) and *Theme Size Slider* (B). Both are presented in percentage (A %, B %). The default setting for the output visualisation is (50%, 33%). The researcher can reveal the most important *concepts* by increasing the percentage of *Visible Concept Slider*.

Co-occurrence is the frequency of *concepts* that occur together within the text. The *Likelihood Score* provides the conditional probability of co-occurrence for the *concepts*. The strength of association between these two *concepts* is determined by the *Likelihood Score*. The strong association between *concepts* can also be seen through the brightness of the *ray line*, the brighter the colour such as light red the closer the relationship.

The researcher may investigate the co-occurrence of any two *concepts* in the text. This can be done by querying the co-occurrences between *concepts* from the *Query Results* feature. Exploring instances (within full text) where *concepts* co-occur can be undertaken to understand the meaning of *concepts* and explore how they are related. To investigate more than two *concepts*, the researcher can use the *Knowledge Pathway* feature on the *concept map*. *Knowledge Pathway* allows investigation of the most likely path from a start *concept* to an end *concept* and defines the relationship that may define a direction for cause.

Appendix 8A (Sample-The details of secondary issues)

Issue	MAIN ISSUES	SECONDARY ISSUES (Within Cluster of concepts)		Source	Themes													
					Policy	Procedures To implement policy												
					Formal Aspects (Organisational Aspects)				Technical Aspects IT/IS security					Informal Aspects				
					Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Technical Theme 1	Technical Theme 2	Technical Theme 3	Informal Theme 1	Informal Theme 2	Informal Theme 3	Informal Theme 4
					Policy (#2)	Strategic vision & security importance (#1)	Security internal controls (#4)	Compliance/ Legal Requirements/ Regulation	Organisational Structure (#7)	Committee	Security Risk & its Management (#3)	Techniques & Controls (#8)	System Development (#8)	Internet/ Network Security (#8)	Staff integrity/ trust/ ethicality /accountability (#6)	Culture, commitment (#6)	Human issues- lack of awareness, stupidity (#6)	Education, training, seminar, orientation (#6)
1	Business needs	Protection/Safeguard	Integrity	A, F		√ √												
			Availability	A, F	√	√ √												
			Confidentiality	A, F, D, H	√ √	√ √					√	√						
			Protection of business information	A,D	√√	√												
			Safeguard the systems	F		√												
			Password management	F		√												
			Recovery	A							√							
		Risk	Risk managing	F		√												
			Risk management	A,F,B,C,D,E							√√√√√							
			Risk profile	F							√							
			Risk Business Plan	H							√							

			Risk Register of Company/Risk Profile	H,D						√√							
			IT security risks	H,C,D, G,A,F B E,					√√	√√√√√√							
		Business/strategic goals	Requires Governance focus	C D	√		√										
			Sustain growth & shareholder value	A						√							
			Competitive edge over competitors	G						√							
			Creates values to customer	G						√							
			Balance between profit and risk	G						√							
			Corporation reputation	B			√										
		Compliance	Complying Legal requirement	E F	√		√ √		√								
			Compliance with policies relating to confidential of information	F,			√			√							
			Compliance with security policy & procedures	F,G			√√										
			Lack of trained leads to incompliance with IT security policies & procedures	F	√								√		√	√	
		Internal controls procedures & processes	Auditing	F		√											
			IT related matters review	A						√							
			Control environment	A			√										
			Correct resources available	A			√										
			Achieving goal of IT/IS security policy	F,G			√√										

			Exception reports	H			√										
			Avoiding security breaches	B			√										
			IT/IS security procedures	E			√										
			Governance focus	D			√										
			Good practices in password management	D													√
			Achieving standards of password policy	D													√
			Using intranet website to publish security policy & good practices	D													√

Appendix 8B: A sample of the transcripts

Interview with CEO Company G

23 November 2009

Interviewer: Does IT/IS security important to your corporation?

CEO: In our business, some processes like transactions are automatic in parts. If certain parts are IT based, security is very important to this corporation. If the online based systems compromised, the business will resume and risk management plan like disaster recovery process and business continuity strategy will take place to restore necessary data.

Interviewer: May I know your responsibility and accountability in IT/IS security risks?

CEO: I as a CEO, I am supposed to be responsible with IT/IS security risks.

The CEO of Company F primarily focusing the strategic level of group IT infrastructure development, provide leadership and supports to the effectiveness of IT governance structure. Making the transformation IT development to continuously improve the competitive edge over its competitors and creates values to the customers, agents and policyholders at large.

A central role of the CEO of Company F is to ensure that decision making stays grounded in the facts where we play a critical role in ensuring an appropriate balance between near-term profit initiatives and risk (i.e., compliance with statutory guidelines and requirements, competition, customer satisfactions and operational efficiency).

Interviewer: So your corporation have IT steering committee in place?

CEO: Yes.

Interviewer: Does IT steering committee influence to the implementation of policy?

CEO: We have IT steering committee to oversee IT applications development. The function of IT steering committee is to develop solution which is consistent with outsource risk. IT steering committee is not responsible to the implementation of policy relating to IT security.

Interviewer: Are IT/IS issues included as part of your business risk management plan?

CEO: Yes. IT/IS issues are part of business risk management plan. I need to ensure effective risk management process and System Development Lifecycle are in place of identifying, evaluating and mitigating critical IT risks covering both software and hardware aspects so as to maintain database confidentiality and system integrity.

And also I need to ensure the IT securities policies are in place and to be reviewed for effective disaster recovery process and business continuity management. The business operation to be resumed without major disruption and inconvenience caused to the customers, agents and policyholders.

Interviewer: Can you give me some examples of the issues or problems in the risk management plan?

CEO: Through Group Risk Management Department and Company's CEO to implement a strategic, comprehensive and systematic risk management process throughout the Company covering: -

- System security;
- System & Database;
- Network and PC support;
- Host Base Development; and
- Business Intelligent

Interviewer: Does your corporation have policy relating to IT/IS security, for example email, internet, back up policy?

CEO: Yes.

Interviewer: Does the board take responsibility for the establishment of policies relating to IT/IS security issues?

CEO: Yes, they take responsible.

Interviewer: May I know what issues are covered by this policy?

CEO: Could be access, return to operation (system down), acceptable run time.

Interviewer: You mean availability?

CEO: Yes, what I understood, availability is, should be there once acceptable.

Interviewer: May I know how are the issues of concern identified?

CEO: The issues are identified through users, IT Team (IT services and functions are outsourced to Maagnet) and Risk Managers. At the board level, we have Risk Committee and Audit Committee to ensure policies and internal controls are in place.

Interviewer: What and whom is involved in the formulation of IT/IS security policy?

CEO: The same groups again, users, risk managers and IT team (Maagnet), and also Executive Directors and all the boards. To find the boards, that may be either Committee of the boards, Risk Committee and Audit Committee.

Interviewer: Who is responsible for implementation of aspects of the policy?

CEO: Depending on the nature, the work portion, users always responsible, the owner of the system who always responsible for the system, usually the owner is the user group.

Interviewer: Does your corporation have internal controls to ensure the goal of IT/IS security policies are achieved as intended?

CEO: Yes, we do have internal controls to ensure the goal of IT security policies are implemented as intended. Internal Risk Team, Internal Audit Team and IT Team are working together for achieving compliance for the user group.

Interviewer: So IT/IS security is part of internal controls in your corporation.

CEO: Yes, has to be.

Interviewer: How do internal controls assist the board and senior management to monitor whether the goal of IT/IS security policies have been implemented?

CEO: Because internal controls are based on and reflect what you expect to happen. Deviations are exceptions, where exceptions occur you may either accept the risk or change the process. You think through what is likely to occur, what impacts are likely to occur, mitigating circumstances and are there any mitigating controls.

To ensure the internal controls are in place, steering committee are asked to report the results of the programs with the original plan, identify the root causes of any deviations, hold leaders accountable for keeping the transformation on track, both in activities and impact.

The role modelling desired mind-sets and behaviour are important aspects to achieve internal controls in the implementation of IT/IS security policies and procedures.

Interviewer: What security standards or regulations exist that you need to comply?

CEO: We have to comply IT security requirements (such as software applications) by Bank Negara (Malaysia Central bank) and Listing Requirements by Bursa Malaysia.

Interviewer: Are you required to report compliance? To whom?

CEO: To the board of director and Bursa Malaysia.

Interviewer: What is your responsibility and accountability in technical roles to ensure the business goals and security controls are achieved according to the corporation's policy?

CEO: I am the Head of IT Steering Committee, basically it also comes to me anyway, I am responsible.

Interviewer: Do you face a difficulty in sharing technical roles among other employees?

CEO: No. I don't have difficulty in sharing technical roles.

Interviewer: How do you monitor the progress of technical implementation (such as IT/IS security controls, design and development of IT/IS and internet/network security) to ensure the resources are used and managed effectively according to the business and corporation's policy?

CEO: By using the Gant Chart, what we have done and what sources we need.

Interviewer: That's the way how you monitor, in what way are informal factors (eg culture, commitments, education, training, awareness, people's integrity, trust and ethicality) important to support the implementation of policies and security controls?

CEO: What is informal?

Interviewer: For example, culture, commitment, education on security, awareness.

CEO: I think accountability, when you get back to system, processes, it's about culture and corporation both accountability anyway, need to be trust, accountability, integrity

Interviewer: Those that you have mentioned just know very important

CEO: Yes.

Interviewer: Do you believe informal factors are important to support the implementation of IT/IS security?

CEO: Of course. Informal factors are important to support the implementation of IT/IS security because if people are not accountable and lack of integrity, the system processes would be compromised.

Interviewer: What is your responsibility and accountability to engage with these informal factors as policy is put into practice?

CEO: Imbue a culture that is aligned with the Board approved corporate strategy, mission, values, objectives, policies and procedures; and fosters risk awareness culture.

Interviewer: Does the corporation's policy embrace informal factors in seeking to achieve the security controls? What do you believe are the important informal factors to your corporation?

CEO: I think the core values, such as integrity are fundamental and everything.

Interviewer: How do you monitor whether the goals of policy relating to informal factors are achieved as intended? Do you have policies relating to informal aspects?

CEO: Core values such as integrity, accountability and trust are not subject to policy statements. They underlie or are at the foundation of the business. For example, the way we interact with each other and the way we engage between internal users and customers.

If you start move away from, I mean, the old days, 20 years back, the rules, if there is a rules and not get caught, I think, what should be done and how it works, so it comes like more rules based, outcome driven, think about industry, it should be prescriptive, which you find yourself in ever increasing the less the thing you shouldn't do, you get longer and longer, actually if the outcome is one, you should have a system to find integrity, we define high security, high integrity data, and everything that happen around that,

We would like to achieve the outcome, so the boards suspended if we want this, if we want this, that every other policies we have to make it outcome, so rather than talking in terms of we don't have the situation what you have said, what we do is consistent the outcome that we designed, so no longer prescriptive rules but becomes outcomes of it, if you would like four of juices, honours to accept the responsibility, and the human outcome

Interviewer: I would like to know in your corporation, do internal employees become threat to your organization?

CEO: Yes, internal employees are threat to this organization if they are lack of education, training and awareness. For example, using one single user name at multiple systems. User name get shared among employees. Clearly the accountability is immediately lost, why employees get shared, well they don't understand what is important, people thinking about that stealing or that form of integrity, they don't see that is a big issue, this need to be done because my friend asked me to help me, so that is lack of education, now that being said lack of understanding, we not educate the person, whatever the user group, lack of integrity. Always problems for industries, billion policies are not through that way.

Interviewer: Lack of awareness?

CEO: Yes, lack of awareness, educate, once you educate but people still do it, that's means accountability, and make people understand, if you don't do your job properly, there is action every reaction, if I behave inappropriately and there is no reaction, that's mean you condone my inappropriate action, so goes back to accountability, so whatever high benchmark becomes a new target with acceptable minimum.

Interviewer: I think we have covered all the questions. Thanks a lot for the interview and I really thankful for that.

CEO: Ok