

# **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