



## **University of Bradford eThesis**

This thesis is hosted in [Bradford Scholars](#) – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team



© University of Bradford. This work is licenced for reuse under a [Creative Commons Licence](#).

**ANALYSIS OF INFORMATION SECURITY RISKS AND  
PROTECTION MANAGEMENT REQUIREMENTS FOR  
ENTERPRISE NETWORKS**

**Mohamed Saad Morsy SALEH**

**Submitted for the degree  
of Doctor of Philosophy**

**Department of Computing  
School of Computing, Informatics and Media**

**University of Bradford**

**2011**

## ABSTRACT

- Name** : Mohamed Saad Morsy Saleh
- Thesis Title** : Analysis of Information Security Risks and Protection Management Requirements for Enterprise Networks.
- Keywords** : Information Security, Risk Management, Analytical Models, Protection Measures, ISO/IEC 27002 Standard, Cost-Benefit Analysis, Six-Sigma, Compliance

With widespread of harmful attacks against enterprises' electronic services, information security readiness of these enterprises is becoming of increasing importance for establishing the required safe environment for such services. Various approaches are proposed to manage enterprise information security risks and to assess its information security readiness. These approaches are, however, not adequate to manage information security risks, as all required information security components of its structural and procedural dimensions have not considered. In addition, current assessment approaches lack numerical indicators in assessing enterprise information security readiness. Furthermore, there is no standard approach for analysing cost versus benefit in selecting recommended protection measures.

This thesis aims at contributing to the knowledge by developing comprehensive Enterprise Information Security Risk Management (EISRM) framework that integrates typical approaches for information security risk management, and incorporates main components of key risk management methodologies. In addition, for supporting phases of the proposed EISRM framework, analytical models for enterprise information security readiness assessment and cost-benefit analysis are developed.

The practical evaluation, using the proposed enterprise information security readiness assessment model has been performed depending on a developed investigation form that used to investigate nine enterprises inside Saudi Arabia. The results demonstrate the effectiveness of the model in assessing and comparing enterprises information security readiness at all levels of the model, using numerical indicators and graphical representations. The EISRM framework and the analytical models presented in this research can be used by enterprises as single point of reference for assessing and cost effectively improving their information security readiness.

## **ACKNOWLEDGEMENTS**

Foremost, praise and thanks to ALLAH, blessing, and peace to the Prophet. I would like to express my greatest gratitude to the Almighty ALLAH, the only who has given me the opportunity, strength, courage and blessing to pursue this work. Conducting this research work and writing the thesis required the patience, persistence and motivation of many people whom I would like to personally acknowledge. I would like to express my heartfelt gratitude, deepest thanks and appreciation to my supervisors for their continuous encouragement, assistance and valuable advice throughout this work. I would like to thank Dr. Mumtaz Kamala, Dr. Andrea Cullen and Mr. John Mellor for their kind advising and cooperation. Special thanks and appreciations go to professor Saad Haj Bakry for his patience, help and guidance in completing this research. My sincere gratitude and special thanks to my family: To my mother, for her support and her unconditional love; to my wife, for her love and tremendous amount of support; to my lovely children, Dina, Ziad and Nada, for their patience, understanding and support. Without them all, my PhD could have been an extremely lonely trip.

DEDICATED TO

*My Father (may Allah Bless him)*

*Who has taught me that dedication and hard work are the  
essentials for the successful life*

*My Mother*

*Who always inspires me with her love and prays*

*My Wife*

*Without her love and encouragement, this thesis would not  
have been possible*

*And My Sweet Children*

*(Dina, Ziad and Nada)*

*For what they give to me, their love and patience*

# TABLE OF CONTENTS

<b>ABSTRACT</b> .....	ii
<b>ACKNOWLEDGMENTS</b> .....	iii
<b>DEDICATED TO</b> .....	iv
<b>TABLE OF CONTENTS</b> .....	v
<b>LIST OF TABLES</b> .....	ix
<b>LIST OF FIGURES</b> .....	xi
<b>LIST OF ACRONYMS</b> .....	xiii
<b>PART I: INTRODUCTION</b> .....	1
<b>Chapter 1:- INTRODUCTION</b> .....	2
1.1 Introduction.....	2
1.2 Background.....	2
1.3 Statement of Problem.....	5
1.4 Research Questions.....	7
1.5 Objectives of the Study.....	8
1.6 Significance of the Study.....	10
1.7 Research Process.....	12
1.7.1 <i>Problem Analysis</i> .....	13
1.7.2 <i>Innovation</i> .....	14
1.7.3 <i>Evaluation</i> .....	15
1.8 Thesis Contributions.....	16
1.9 Applicability and Usability.....	18
1.10 Thesis Organisation.....	19
1.11 Summary.....	22
<b>PART II: BACKGROUND</b> .....	23
<b>Chapter 2: ENTERPRISE INFORMATION SECURITY RISK MANAGEMENT</b> .....	24
2.1 Introduction .....	24
2.1.1 <i>Enterprise Information Security</i> .....	24
2.1.2 <i>Risks to Information Security</i> .....	25
2.1.3 <i>Importance of Risk Management</i> .....	26
2.2 Existing Risk Management Approaches.....	28
2.2.1 <i>The Risk-Analysis Approach</i> .....	29
2.2.2 <i>The Best-Practice Approach</i> .....	44
2.3 Risk Management Main Requirements.....	51
2.3.1 <i>Risk Management Basic Elements</i> .....	52
2.3.2 <i>Risk Management Scope</i> .....	53
2.3.3 <i>Risk Management Process</i> .....	55
2.3.4 <i>Assessment of Information Security Situation</i> .....	57
2.3.5 <i>Economical Analysis of Security Investments</i> .....	59
2.3.6 <i>Other Requirements</i> .....	59

2.4 Summary.....	60
<b>PART III: THEORETICAL ANALYSIS.....</b>	<b>61</b>
<b>Chapter 3: AN ENTERPRISE INFORMATION SECURITY RISK MANAGEMENT</b>	
<b>FRAMEWORK.....</b>	<b>62</b>
3.1 Introduction.....	62
3.2 Proposed EISRM Framework.....	62
3.2.1 EISRM Structural Issues.....	64
3.2.2 EISRM Procedural Issues.....	70
3.2.3 Using EISRM Framework.....	80
3.3 The Information Security Policy.....	82
3.3.1 Information Security Policy Process.....	82
3.3.2 The Policy Document Structure.....	84
3.4 EISRM Work Team.....	85
3.5 Summary.....	86
<b>Chapter 4: ENTERPRISE INFORMATION SECURITY ASSESSMENT</b>	
<b>MEASURES.....</b>	<b>88</b>
4.1 Introduction.....	88
4.2 Development of ISO Based Assessment Measures.....	88
4.2.1 Knowledge Acquisition.....	90
4.3 ISO/IEC 27002 Assessment Measures.....	97
4.3.1 Technology Issues.....	98
4.3.2 Organisation Issues.....	101
4.3.3 People Issues.....	104
4.3.4 Environment Issues.....	104
4.4 Incremental Assessment Approach.....	106
4.4.1 Level1: Essential and Common Security Measures.....	108
4.4.2 Level2: ISO/IEC 27002 Security Measures.....	109
4.4.3 Level3: ISO Other Security Standards.....	110
4.5 Summary.....	111
<b>Chapter 5: A MODEL FOR ENTERPRISE INFORMATION SECURITY READINESS</b>	
<b>ASSESSMENT.....</b>	<b>112</b>
5.1 Introduction.....	112
5.2 Assessing Enterprise Information Security.....	112
5.3 Information Security Assessment Approach.....	114
5.3.1 The TOPE View of the ISO/IEC 27002 Standard.....	115
5.3.2 The Assessment Model.....	115
5.4 The Proposed Assessment Process.....	121
5.5 Practical Application of the Model.....	124
5.5.1 The Investigation Form.....	126
5.6 An Illustrative Example.....	132
5.7 Impact of the Assessment.....	133

5.8 Summary.....	135
<b>Chapter 6: AN ENTERPRISE INFORMATION SECURITY COST-BENEFIT MODEL...</b>	<b>136</b>
6.1 Introduction.....	136
6.2 Background.....	136
6.2.1 <i>Standard Organisations Economic Directions</i> .....	138
6.2.2 <i>Information Security Financial Metrics</i> .....	141
6.2.3 <i>Cost-Benefit Analysis</i> .....	145
6.3 Information Security Economical Analysis.....	147
6.3.1 <i>Protection of Information</i> .....	147
6.3.2 <i>Required Protection</i> .....	148
6.3.3 <i>Evaluation of Information Security Benefits</i> .....	149
6.3.4 <i>Summary</i> .....	150
6.4 The Proposed Cost-Benefit Model.....	150
6.4.1 <i>Security Challenges</i> .....	152
6.4.2 <i>Protection Measures</i> .....	153
6.4.3 <i>Resulting Protection</i> .....	154
6.4.4 <i>Cost Saving</i> .....	154
6.4.5 <i>Residual Cost</i> .....	155
6.4.6 <i>Cost Function</i> .....	155
6.5 Summary.....	156
<b>PART IV: APPLICATIONS.....</b>	<b>157</b>
<b>Chapter 7: EVALUATION CASE STUDIES.....</b>	<b>158</b>
7.1 Introduction.....	158
7.2 The Collected Data.....	158
7.2.1 <i>The Concerned Enterprises</i> .....	160
7.2.2 <i>Data Collection</i> .....	160
7.3 General Enterprises Information .....	162
7.3.1 <i>The Investigated Enterprises</i> .....	162
7.3.2 <i>The Business Profile</i> .....	166
7.3.3 <i>The Personal Profile</i> .....	167
7.4 Data Analysis and Findings.....	169
7.4.1 <i>Level-1 Assessment Results</i> .....	169
7.4.2 <i>Level-2 Assessment Results</i> .....	172
7.4.3 <i>The Information Security Assessment Report</i> .....	180
7.4.4 <i>Assessment Results for All Case Studies</i> .....	181
7.5 Application of the Cost-Benefit Model.....	185
7.5.1 <i>Security Challenges</i> .....	185
7.5.2 <i>Protection Measures</i> .....	185
7.5.3 <i>Achieved Protection</i> .....	188
7.5.4 <i>Cost Function</i> .....	188
7.6 Summary.....	189



<b>PART V: CONCLUSION.....</b>	191
<b>Chapter 8: CONCLUSION AND FUTURE WORK.....</b>	192
8.1 Introduction.....	192
8.2 Conclusion.....	193
8.2.1 <i>Study Main Objectives</i> .....	193
8.2.2 <i>Study Main Contributions</i> .....	195
8.2.3 <i>Study Limitations</i> .....	199
8.2.4 <i>Validation of the Results</i> .....	201
8.3 Recommendations for Saudi Enterprises.....	202
8.4 Future Work.....	204
<b>PART VI: REFERENCES.....</b>	208
<b>REFERENCES.....</b>	209
<b>PART VII: APPENDIXES.....</b>	220
<b>Appendix A: THE INVESTIGATION FORM.....</b>	221
<b>Appendix B: SAMPLE CASE STUDY.....</b>	231
<b>Appendix C: DETAILED ASSESSMENT RESULTS.....</b>	247
<b>Appendix D: EISRM COMPUTER TOOL.....</b>	257
<b>Appendix E: PUBLICATIONS.....</b>	272

## LIST OF TABLES

Table 2-1	The generic risk management steps & process of AS/NZS 4360.....	31
Table 2-2	IT risk management steps & process of NIST SP 800-30.....	32
Table 2-3	IT risk management steps & process of ISO/IEC TR 13335-3.....	34
Table 2-4	Relation of standard risk management methods and the proposed EISRM framework.....	35
Table 2-5	Relation of professional risk management methods and the proposed EISRM framework.....	41
Table 2-6	Comparison of the risk-analysis based methods.....	42
Table 2-7	Key researchers risk management methods and techniques.....	43
Table 2-8	The standard of good practice for information security aspects, areas and sections.....	45
Table 2-9	The ISO/IEC 27002 clauses, objectives and controls.....	47
Table 2-10	Mapping the basic elements & concepts of key risk management methods to the identified basic elements of the proposed EISRM framework.....	54
Table 2-11	Mapping the contents of key information security management methods to the TOPE scope.....	56
Table 2-12	The ISO information security risk management process.....	57
Table 2-13	Mapping the processes of key risk management methods to the DMAIC phases of the six-sigma model.....	58
Table 3-1	Enterprise assets considered by different references mapped on the TOPE domains (ISO/IEC TR 13335 1998; CRAMM 2001; BSI 2004).....	67
Table 3-2	Threats and vulnerabilities considered by different references mapped on the TOPE domains (ISO/IEC TR 13335 1998; CRAMM 2001; BSI 2004).....	68
Table 3-3	ISO information security clauses, objectives and controls mapped on the TOPE domains (ISO/IEC 27002 2005) .....	69
Table 3-4	DMAIC process (Pyzdek 2003).....	74
Table 3-5	The use of six-sigma five phase cyclic process DMAIC for EISRM.....	78
Table 3-6	Six-sigma based cyclic process for the use of ISO/IEC 27002:2005 .....	83
Table 3-7	Information security policy document: structure and progress.....	85
Table 3-8	Six sigma team for the application of the ISO/IEC 27002 standard.....	86
Table 4-1	TOPE view of ISO/IEC 27002 main clauses.....	92
Table 4-2	Assessment measures considering the ISO/IEC 27002 security objective of “information security policy document” with two controls. ....	94
Table 4-3	Reference table for the importance values of the measures.....	96
Table 4-4	TOPE view of ISO/IEC 27002 main security clauses, objectives, controls and assessment measures.....	97
Table 4-5	Technology: protection measures for “communications and operations management”.....	98
Table 4-6	Technology: protection measures for “access control”.....	100
Table 4-7	Technology: protection measures for “information systems acquisition, development and maintenance”.....	101
Table 4-8	Organisation: protection measures for “security policy”.....	101
Table 4-9	Organisation: protection measures for “organisation of information security”.....	102
Table 4-10	Organisation: protection measures for “asset management”.....	102
Table 4-11	Organisation: protection measures for “information security incident management”.....	103
Table 4-12	Organisation: protection measures for “business continuity management”.....	103
Table 4-13	People: protection measures for “human resources security”.....	104
Table 4-14	Environment: protection measures for “physical and environmental security”.....	105
Table 4-15	Environment: protection measures for “compliance”.....	106
Table 4-16	TOPE view of ISO/IEC 27002 essential security objectives, controls, together with the number of measures associated with each control....	108

Table 4-17	TOPE view of ISO/IEC 27002 related ISO standards.....	110
Table 5-1	Reference table for performance values of the assessment measures...	119
Table 5-2	The TOPE model issues, equations and steps concerned with the investigation of enterprises with the ISO/IEC 27002 standard.....	120
Table 5-3	Evaluation grades, weights and examples of measures, relative weights and indicators.....	125
Table 5-4	Technology domain: Related ISO/IEC 27002 clauses, objectives, protection controls and evaluation measures.....	129
Table 5-5	Organisation domain: Related ISO/IEC 27002 clauses, objectives, protection controls and evaluation measures.....	130
Table 5-6	People domain: Related ISO/IEC 27002 clause, objectives, protection controls and evaluation measures.....	130
Table 5-7	Environment domain: Related ISO/IEC 27002 clauses, objectives, protection controls and evaluation measures.....	130
Table 5-8	An example of the results concerned with the measures of the use of the protection controls of ISO/IEC 27002 “security policy”.....	132
Table 5-9	An example of the results concerned with the achievement of ISO/IEC 27002 security policy objective, considering the results of Table 5-8....	133
Table 6-1	Microsoft detailed new or enhanced control costs.....	140
Table 6-2	Information security financial metrics.....	141
Table 6-3	Protection tools and their use according to the annual computer crime and security survey (CSI 2007).....	148
Table 6-4	Security challenges and their cost.....	153
Table 6-5	Protection measures and their cost.....	153
Table 6-6	Protection from challenges.....	154
Table 6-7	Saving of challenges cost.....	154
Table 6-8	Residual cost of challenges.....	155
Table 6-9	Cost functions: challenges with protection.....	156
Table 7-1	“Business profile” results of the participated enterprises.....	167
Table 7-2	“Personal profile” of the respondents to the investigation form.....	168
Table 7-3	Level-1 assessment results of ISO/IEC 27002 essential controls.....	170
Table 7-4	Level-1 assessment results of ISO/IEC 27002 common controls.....	171
Table 7-5	E9, E7 and E5 scores on the ISO/IEC 27002 eleven clauses.....	178
Table 7-6	TOPE weighted indicators.....	179
Table 7-7	A list of the missing controls for each of the investigated enterprises...	180
Table 7-8	The average scores of each of the TOPE domains and the TOPE indicator.....	181
Table 7-9	The average score of the ISO/IEC 27002 clauses based on the collected data from the nine investigated enterprises.....	182
Table 7-10	The ten lowest-ranked ISO/IEC 27002 objectives based on the analysed data from the nine investigated enterprises.....	183
Table 7-11	The ten lowest-ranked ISO/IEC 27002 security controls based on the analysed data from the nine investigated enterprises.....	184
Table 7-12	The ten lowest-ranked ISO/IEC 27002 assigned security measures based on the analysed data from the nine investigated enterprises.....	184
Table 7-13	Challenges considered and their cost.....	185
Table 7-14	ISO/IEC 27002 controls associated with application of the antivirus .....	187
Table 7-15	Cost-benefit analysis for twelve protection levels.....	188
Table C-1	All case studies assessment results concerned with the achievement of the ISO/IEC 27002 security controls.....	248
Table C-2	All case studies assessment results concerned with the achievement of the ISO/IEC 27002 security objectives.....	251
Table C-3	All case studies assessment results concerned with the achievement of the ISO/IEC 27002 security clauses.....	252
Table C-4	All case studies assessment results concerned with the achievement of the EISRM TOPE domains.....	252

## LIST OF FIGURES

Figure 1-1	Stages of the research.....	13
Figure 1-2	Thesis outline.....	21
Figure 2-1	CRAMM risk management process (CRAMM 2001).....	36
Figure 2-2	OCTAVE risk management process (Alberts 2003).....	37
Figure 2-3	CORAS risk management process (Fredriksen et al. 2002).....	38
Figure 2-4	EBIOS risk management process (EBIOS 2004).....	40
Figure 3-1	The structure of the proposed EISRM framework.....	64
Figure 3-2	An illustrative view of ISO risk management components.....	72
Figure 3-3	The proposed process for the EISRM framework .....	75
Figure 4-1	A TOPE scope for information security requirements.....	107
Figure 5-1	The structure of the TOPE model concerned with the investigation of enterprises with the ISO/IEC 27002 standard.....	117
Figure 5-2	The steps of the proposed information security readiness assessment process.....	122
Figure 6-1	Protection measures versus security challenges: Cost-benefit analysis	151
Figure 6-2	Cost-benefit analysis procedure.....	152
Figure 7-1	The assessment results of E9, E7 and E5 enterprises concerned with the “Technology” domain.....	174
Figure 7-2	The assessment results of E9, E7 and E5 enterprises concerned with the “Organisation” domain.....	175
Figure 7-3	The assessment results of E9, E7 and E5 enterprises concerned with the “People” domain.....	176
Figure 7-4	The assessment results of E9, E7 and E5 enterprises concerned with the “Environment” domain.....	177
Figure 7-5	Radar graph of the E2, E5 and E7 performance scores on the ISO/IEC 27002 – clause level .....	178
Figure 7-6	Illustration of E9, E7 and E5 assessment results concerned with the TOPE domains.....	179
Figure 7-7	The changes of enterprise E2 of: residual cost of challenges (r), cost of protection (k), and total cost (c).....	189
Figure B-1a	Sample Case study results concerned with the achievement of the ISO/IEC 27002 technical security objectives of the “communications and operations management” clause.....	233
Figure B-1b	Sample Case study results concerned with the achievement of the ISO/IEC 27002 technical objectives of the “access control” clause.....	235
Figure B-1c	Sample Case study results concerned with the achievement of the ISO/IEC 27002 technical objectives of the “information systems acquisition, development and maintenance” clause.....	236
Figure B-1d	Sample Case study results concerned with the achievement of the ISO/IEC 27002 technology clauses, considering the results of Figures B-1a, B-1b and B-1c.....	237
Figure B-1e	Sample Case study results concerned with conformance with the technology domain considering the results of Figure B-1d.....	237
Figure B-2a	Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objective of the “security policy” clause.....	238
Figure B-2b	Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “organisation of Information Security” clause.....	238
Figure B-2c	Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “assets management” clause.....	239
Figure B-2d	Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “information security incident management” clause.....	240
Figure B-2e	Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “business continuity management” clause.....	240
Figure B-2f	Sample Case study results concerned with the achievement of the	

	ISO/IEC 27002 organisation clauses, considering the results of Figures B-2a, B-2b, B-2c, B-2d and B-2e.....	241
Figure B-2g	Sample Case study results concerned with the achievement of organisation domain, considering the results of Figure B-2f.....	241
Figure B-3a	Sample Case study results concerned with the achievement of the ISO/IEC 27002 people security objectives of the “human resources security” clause.....	242
Figure B-3b	Sample Case study results concerned with the achievement of ISO/IEC 27002 human resources clause, considering the results of Figure B-3a.	242
Figure B-3c	Sample Case study results concerned with the achievement of people domain, considering the results of Figure B-3b.....	242
Figure B-4a	Sample Case study results concerned with the achievement of the ISO/IEC 27002 environmental security objectives of the “physical and environmental security” clause.....	243
Figure B-4b	Sample Case study results concerned with the achievement of the ISO/IEC 27002 environmental security objectives of the “compliance” clause.....	244
Figure B-4c	Sample Case study results concerned with the achievement of the ISO/IEC 27002 environmental security clauses considering the results of Figures B-4a, and B-4b.....	245
Figure B-4d	Sample Case study results concerned with the achievement of the ISO/IEC 27002 environment domain considering the results of Figure B-4c.....	245
Figure B-5	Sample case study results concerned with conformance with TOPE domains.....	246
Figure C-1	All case studies results concerned with the achievement of the ISO/IEC 27002 technical security objectives ( <i>Technology Domain</i> ).....	253
Figure C-2	All case studies results concerned with the achievement of the ISO/IEC 27002 organisation security objectives ( <i>Organisation Domain</i> ).	254
Figure C-3	All case studies results concerned with the achievement of the ISO/IEC 27002 human security objective ( <i>People Domain</i> ).....	255
Figure C-4	All case studies results concerned with the achievement of the ISO/IEC 27002 environment security objectives ( <i>Environment Domain</i> ).	256
Figure D-1	EISRM tool - Input screen for the “Personal Profile”.....	270
Figure D-2	EISRM tool - Input screen for the “Business Profile”.....	270
Figure D-3	EISRM tool - Input screen for the TOPE domains.....	271
Figure D-4	EISRM tool – Example of reports for the TOPE domains.....	271

## LIST OF ACRONYMS

<b>Acronym</b>	<b>Meaning</b>
ACCSS	Australian Computer Crime and Security Survey
AS/NZS	Australian – New Zealand Standard
ALE	Annual Loss Expected
BBN	Bayesian Belief Network
BERR	Business Enterprises and Regulatory Reform
BSI	British Standard Institute
BPIRM	Business Process Information Risk Management
BSI -Germany	Bundesamt für Sicherheit in der Informationstechnik
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and related Technology
CRAMM	CCTA Risk Analysis and Management Method
CERT	Computer Emergency Response Team
CERT/CC	CERT/ Coordination Centre
CIO	Chief Information Officer
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
CCITT	International Telegraph and Telephone Consultative Committee
CCTA	Central Computer Telecommunications Agency
CORAS	Consultative Objective Risk Analysis System
CBA	Cost Benefit Analysis
CSI	Computer Security Institute
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DMAIC	Define-Measure-Analyse-Improve-Control
DTI	Department for Trade and Industry
e-	Electronic
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EISRM	Enterprise Information Security Risk Management
EC	European Commission
EU	European Union
FTC	Federal Trade Commission
FedCIRC	Federal Computer Incident Response Centre
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission – technical Commission
IPR	Intellectual Property Rights
ISMS	Information Security Management Systems
ISO	International Standards Organisation
IT	Information Technology
IS	Information Security
ISF	Information Security Forum
ISMS	Information Security Management System

IDS	Intrusion Detection System
IRR	Internal Rate of Return
ISBS	Information Security Breach Survey
IPF	Information Processing Facilities
I-CAMP	Incident Cost-Analysis Modelling Project
ID	Identifier
JTC	Join Technical Committee
KPIs	Key Performance Indicators
KSA	Kingdom of Saudi Arabia
MDG	Millennium Development Goals
MICTS	Management of Information and Communications Technology Security
MEHARI	MEthod Harmonisee d' Analyse du Risques Informatique
NIPC	National Infrastructure Protection Centre
NIST	National Institute for Standard and Technology
NPV	Net Present Value
OCTAVE	Operationally Critical Threat Asset & Vulnerability Evaluation
OIG	Office of Inspector General
PDCA	Plan – Do – Check – Act
PROTECT	Policies – Risks – Objectives – Technology – Execute – Compliance - Team
RiMaHCoF	Risk Management in Health care using Cognitive Fuzzy techniques
RAMeX	Risk Analysis and Management eXpert system
ROI	Return on Investment
ROSI	Return on Security Investment
SAEM	Security Attribute Evaluation Method
SOGP	Standard of Good Practice
SP	Special Publication
SQ	Special Qualification
SCM	Supply Chain Management
S_	Security
TOPE	Technology – Organisation – People - Environment
SWOT	Strengths – Weakness – Opportunities - Threats
SQUARE	System Quality Requirements Engineering
TR	Technical Report
TP	Third Party
UN	United Nation
USA	United State of America
UK	United Kingdom
UPML	Unified Problem – solving Method Development Language
VP	Vice President
VPN	Virtual Private Network

**PART I**  
**INTRODUCTION**

**Chapter 1 INTRODUCTION**



# **Chapter 1**

## **INTRODUCTION**

### **1.1 Introduction**

This research study investigates the current applied approaches within enterprises for information security risk management so as to integrate these approaches in a comprehensive reference framework that contributes to the protection of information resources. The main objective is to provide analytical models for information security readiness assessment and cost-benefit analysis within an enterprise wide reference information security risk management framework, aimed at assessing numerically the state of information security inside enterprises with different levels of detail and cost effectively helping in the selection of the recommended security protection measures. The results obtained from such an assessment can be used for economically directing enterprises' resources to proactively respond to the information security challenges and therefore minimise the risks to the protection of information resources.

### **1.2 Background**

The use of Information and Communication Technology (ICT) is widely recognised as an important mean for national and international development. This has been emphasised by various important international sources including: the United Nations (UN) summit meeting of September 2000, which

issued the widely known UN Millennium Development Goals (MDG) (UN 2000); the Lisbon European summit held in March 2000 (European Summit 2000); the European community drive toward the knowledge society (European Community 2001); the Okinawa G8 summit of July 2000 (G8 Summit 2000); and the Sea Island G8 summit of June 2004 (G8 Summit 2004). The strength of the previous emphasis on the use of ICT is not surprising. This use enables people and enterprises to perform their tasks faster, cheaper and with better quality. It also supports transformation to the knowledge society, creating new opportunities, supporting innovation and leading to sustainable development.

Consequently, current enterprises base their operations on the Information Technology (IT) infrastructure and most business processes are completely dependent on information systems. As most enterprises become increasingly dependent on information and its related technology, they become highly susceptible to risks of IT systems' security flaws. Therefore, IT systems' security has become such an integral part in successfully conducting business, and it also plays a crucial role in giving an enterprise the competitive edge over another (Gerber and Solms 2001).

Solms (2006) explains that enterprise information systems security historically passed through three successive waves during the last two decades, which are technical, management and institutional. The technical wave was characterised by information security being a technical issue, best left to the technical experts. It includes using computer security systems, such as authentication devices, encryption programmes and access control services. The management wave begins when enterprises' top management started to

involve in implementing and managing information security systems and security policies. It was driven by the realisation that information security has a strong management dimension, and aspects like procedures, policies and management are considered very important. The institutional wave includes considering information security as enterprise culture, covering standardisation, certification, measurement and concern of human factors in information security culture where information security activities become a daily concern of all employees of the enterprise. According to Solms (2006), the current fourth wave of enterprise information systems security is defined as the process of explicit inclusion of information security as a pivotal part of corporate governance. It is characterised by integration of the information security management processes and effective implementation of information security risk management programmes.

Recognising the importance of information security risk management, various organisations concerned with standards and business have published or republished different risk management methods and updated these methods regularly (ISO/IEC TR 13335-3 1998; CRAMM 2001; NIST SP800-30 2002; AS/NZS4360 2004; OCTAVE 2005). In the past, these methods were used successfully by enterprises using IT and working in different fields for identifying, analysing and minimising risks for their IT activities. Nowadays, the results of these methods, in addition to time consuming and high cost, show unrealistic expectations (Warren and Hutchinson 2003; Karabacak and Sogukpinar 2005; Braber et al. 2007; Ekelhart et al. 2008).

Recent studies of computer crime and security management, despite the increasing number of information technology and information security risk

management methodologies, still continually report that there is a poor implementation of security measures and a low level of awareness in general about security issues (CSI 2007; DTI 2008). The results of the 2008 Information Security Breaches Survey (ISBS) running by the Department of Business Enterprises & Regulatory Reform (BERR) of the United Kingdom (UK) indicated that only 11% of the surveyed enterprises have implemented BS 7799/ISO/IEC 27001. The same survey reported that 79% of the surveyed enterprises are not aware of the contents of BS 7799/ISO/IEC 27001. In addition, the survey showed that 52% of the surveyed enterprises do not carry out any formal security risk assessment programme (ISBS 2006, pp.8-9).

It is widely known that the structure and type of enterprise information technology systems have changed over time. In contrary, the risk management methodologies used to identify the most appropriate security protection measures still depend on the same traditional theory of the past. This theory is focused mainly on the technological assets and the most effective technical security solution to protect these assets. Knowing that the emphasis has changed from protecting computer assets to protecting information assets and to secure information, a different and more modern approach is needed that considers human, organisational, environmental aspects in addition to the technical aspects in dealing with the information security management issues (Vraalsen et al. 2005; Braber et al. 2007; Mayer et al. 2008; Kraemer et al. 2009).

### **1.3 Statement of the Problem**

After thorough literature review, it is found that, two main approaches are prevailing in dealing with enterprise information security risk management,

namely the risk-analysis approach and the best-practice approach (ISO/IEC 13335-1 2004; Boehmer 2008). In spite of the importance of these two approaches in managing enterprise information security risks; these approaches are however seldom considering the numerical assessment of the current situation enterprise information security readiness (Johansson and Johnson 2005). It is well known that one can't manage what he can't measure. It is necessary to be able to numerically assess the current state enterprise information security to be able to prioritise the required changes and monitor the achieved security improvement (Hoo 2000). Therefore, the development of an effective information security assessment models is considered as one of the main challenges facing enterprises for having better view of their information security situation, and for identifying and evaluating ineffective and non-compliant controls with the information security management standards.

Most of the risk-analysis based methodologies start the risk management process by trying to discover the important assets and their associated risks then suggesting mitigation plans without introducing a convincing measure or numeric value to the top management regarding the weakness in information security controls that needs improvement. Similarly, the best-practice methodologies audit only the existence of the security controls according to a given standard without investigating the effective use of these controls by the users of the system or even having an overall indicator of the enterprise information security level that needs improvement (ISO/IEC 13335-1 2004).

The main goal of this PhD thesis is to develop a comprehensive framework for enterprise information security risk management, which combines the typical approaches for information security risk management from one hand, and

accommodates the essential components of the key risk management methodologies from the other hand. The proposed framework is expected to assess numerically and improve cost effectively the protection level of enterprises' information security considering not only technological factors, but also organisational, human and environmental factors as well. The assessment is performed using a developed analytical multi-level assessment model that depends on the security controls of the ISO/IEC 27002, code of practice for information security management standard. This research also seeks to raise the level of awareness inside Saudi enterprises about the importance of the effective management of the information security protection measures.

## **1.4 Research Questions**

The main research concern is to find answers to the following five main questions aiming at filling the gaps in the information security risk management literature.

- **Research question 1:** What should a comprehensive enterprise information security risk management framework comprise of in order to integrate current available enterprise information security risk management approaches?
- **Research question 2:** How to assess enterprise information security readiness using an efficient numerical valid and reliable modelling technique?
- **Research question 3:** What is the possibility of using suitable economic metrics in the selection of the recommended information security protection measures?

- **Research question 4:** What is the current situation information security readiness inside Saudi enterprises?
- **Research question 5:** What steps Saudi enterprises must take to improve their current information security risk management practices?

## **1.5 Objectives of the Study**

This study aims to provide a comprehensive Enterprise Information Security Risk Management (EISRM) framework. The proposed EISRM framework is designed to incorporate the essential components of the key risk management methods on one hand, and depends on the TOPE (Technology, Organisation, People and Environment) scope for its structural dimension and on the six-sigma DMAIC (Define, Measure, Analyse, Improve and Control) process for its procedural dimension on the other hand. The research also presents information security readiness indicators based on a developed analytical model that can assess numerically enterprise information security readiness. These indicators represent protection levels against possible risks, and provide an information security performance measure for future improvements. In addition, a practical cost-benefit analytical model is developed for applying the recommended protection measures cost effectively. Furthermore, for practical application of the proposed information security assessment model, the research suggests a gradual approach for the implementation of the ISO information security standards. Finally, for evaluating the EISRM framework and investigating the effective use of its associated models, practical case studies are presented and the data was analysed using a developed computer tool. In summary, the work presented in this thesis has six main objectives as follows:

- **The first objective** is related to the development of a comprehensive enterprise information security risk management framework.
- **The second objective** focuses on the identification of the ISO/IEC 27002 based enterprise information security assessment measures.
- **The third objective** is concerned with the development of an analytical model that provides integrated multi-level information security readiness indicators considering the risk controls of the ISO/IEC 27002 code of practice for information security management standard.
- **The fourth objective** is devoted for the development of a practical model that provides cost-benefit trade-off between the estimated cost from applying the recommended information security protection measures and the expected benefits as a result from the protection of the information resources.
- **The fifth objective** is associated with using the information security assessment model for investigating information security readiness of nine Saudi enterprises working in different fields and presenting the assessment results numerically and graphically using a developed computer tool.
- **The sixth objective** is concentrated on raising the level of awareness about the importance of managing information security risks within Saudi enterprises and providing recommendations for improving the current situation information security management practices inside these enterprises.



The ultimate objective of this research study is to present to the theory of information security management by unique analytical models via a comprehensive enterprise information security risk management framework.

## **1.6 Significance of the Study**

This study is important in general for both practitioners and researchers in the field of information security risk management. There is still little work regarding agreed comprehensive reference framework for enterprise information security risk management (Robert and Rolf 2003; ISO/IEC 27005 2008). In addition, the information security assessment approaches lack the numerical indicators in assessing enterprises information security readiness (Werlinger et al. 2009). Furthermore, there is no agreed practical economical model for analysing the cost of applying the recommended protection measures against the expected benefits that could convince the top management about the importance of applying these security measures (Mercuri 2003; Gordon and Loeb 2006; Anderson and Choobineh 2008).

The developed EISRM framework in this research study is distinguished from previous related work in the subject by four main features. It has a comprehensive view in that it incorporates the main components of the key risk management methodologies; it integrates the current approaches for information security risk management in a reference framework; it depends on the international information security management standards; it uses the TOPE scope for its structural dimension and depends on the six-sigma DMAIC cyclical process for its procedural dimension. The use of the TOPE scope enables the EISRM framework to accommodate wide range of issues associated with risk management in a well structured and comprehensive

manner. While the use of the DMAIC process enables the EISRM framework to incorporate the essential components of the key enterprise information security risk management methods.

The developed analytical model, for enterprise information security readiness assessment, provides a set of integrated indicators for the TOPE domains at various levels of the ISO/IEC 27002 code of practice for information security management standard. The levels of the model start in measuring the effective use of each of the 283 assigned basic ISO security measures leading to 133 ISO security controls, and move up measuring the achievement of 39 ISO security objectives, measuring the implementation of 11 ISO/IEC 27002 main clauses, assessing the security state of each of the 4 TOPE domains and finally reaching up to an indicator that assesses enterprise information security readiness. The overall high-level enterprise information security readiness indicator aggregates the lower-level indicators, with the value of each indicator not only based on its performance in protection against certain risks, but also on the weight of importance with its related issues.

The developed practical cost-benefit model is based on economical metrics and presents an approach that depends on the ISO/IEC 27002 recommended security protection measures. This model seeks to weight the investment in information security protection measures against the expected benefit from implementing these measures and tries to explore the optimal solution.

To support the developed enterprise information security assessment model, a prototype computer tool is developed and used in applications concerned with nine Saudi enterprises to examine its strengths and weaknesses and to check its effectiveness. Finally, this study is important in specific for Saudi enterprises

in that its results are compiled in a number of important recommendations for improving the current applied information security risk management practices.

## **1.7 Research Process**

The choice of research strategy depends mainly on the type of questions and to what extent one has control over the event (Yin 1996). It is also clear that the choice of the right methodology to achieve the research objectives is crucial for the success of any research study. March and Smith (1995) explains the unique characteristics of the technology research paradigm and its methodologies. They explained that in the context of computer and information science there are two main research strategies, the behavioural-science and the design-science. The behavioural-science originates from research methods within natural science where it is used to develop and refine principles and laws. The aim of the behavioural-science research in the natural and social science is to achieve more knowledge about some existing part of the world. From the other hand, the design-science drives from engineering and the artificial since. The aim of the design-science research is to solve a problem by creating new or improved artefacts (constructs, models, methods or instantiations) in the IT systems (Simon 1997; Hevner et al. 2004).

This thesis used the design-science research methodology to achieve its stated objectives. This method encompasses three steps: (1) problem analysis, (2) innovation and (3) evaluation (Glass 1995; Stolen 2006; Peffers et al. 2008). The design-science research methodology is used for thorough understanding of the main requirements for developing comprehensive enterprise information security risk management framework and its associated analytical models. In this respect, the research process has involved six basic

stages: 1) identification of research problem/objectives; 2) research design/methodology; 3) development of comprehensive EISRM framework; 4) development of analytical models for information security readiness assessment and for cost-benefit analysis of the recommended protection measures ; 5) practical evaluation of research assessment model & data analysis; and 6) discussion and conclusion. Figure 1-1 shows a schematic representation of the research stages and the phases considered at each of these stages toward the achievement of the target objectives of this research study.

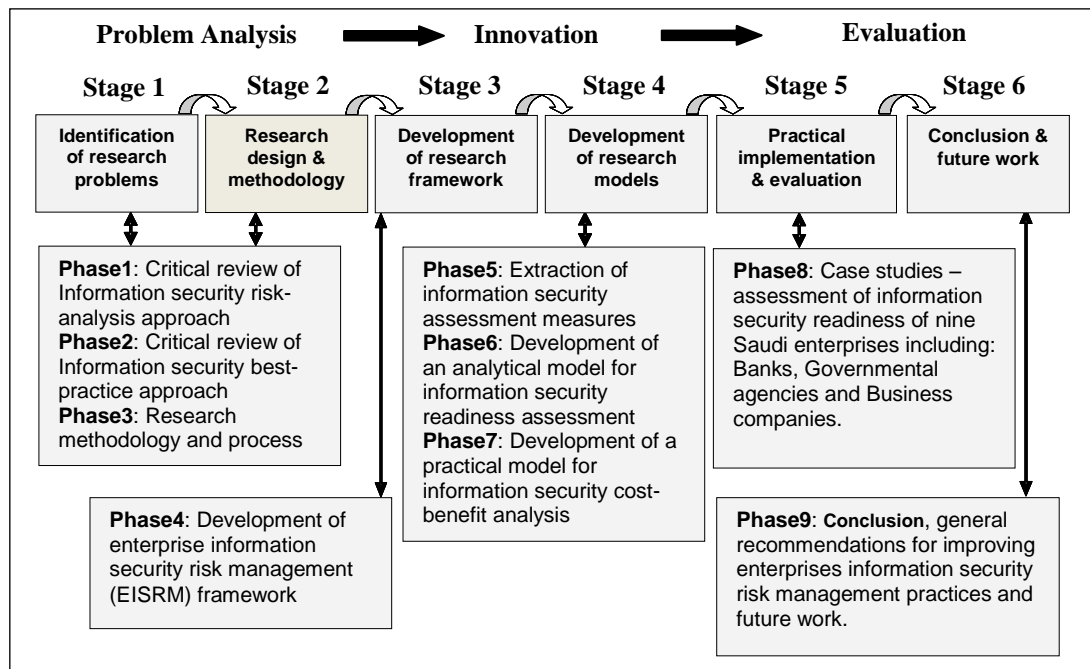


Figure 1-1 Stages of the research

### 1.7.1 Problem Analysis

The problem analysis step of the research methodology includes two stages, stage 1: identification of research problems and objectives; and stage 2: research design and methodology. The first stage involved literature review for the identification of research problems and objectives. The extensive literature survey in Chapter 2 allowed the concepts and issues in information security

risk management to formalise. Section 2.2.1 presents a critical review of the relevant literature related to enterprise information security risk-analysis approach. It discusses standard, professional and research methods for enterprise information security risk management in order to explore basic elements, essential components and main steps of these methods to be included in the proposed framework. The best-practice approach for information security risk management and the key information security management methods are discussed in detail in Section 2.2.2. Section 2.3 serves to discuss the main requirements for developing a comprehensive enterprise information security risk management framework.

The second stage of the research methodology serves to investigate the available research methods and to discuss the research design. The technological research methodology is adopted in this research in developing new analytical tools for enterprise information security risk management.

### **1.7.2 Innovation**

The innovation step of the research methodology includes two stages, stage 3: development of EISRM framework; and stage 4: development of analytical models for enterprise information security readiness assessment and for cost-benefit analysis. In the third stage, the research developed an EISRM framework and identified its four main dimensions. The EISRM framework was developed in this stage of the research based on the literature review of Chapter 2 and on the extensive review of various risk management standards to formulate the framework and its main dimensions, basic elements, essential components and main steps. Chapter 3 provides the proposed framework and its structural and procedural dimensions.

The fourth stage adds to the theory and extends the existing techniques for enterprise information security readiness assessment. An analytical model for enterprise information security readiness assessment was developed based on the literature review of Chapter 2 and on the identified enterprise information security assessment measures extracted in Chapter 4. In addition an incremental approach for gradual implementation of the protection controls of the ISO international information security management standards is presented in Chapter 4. A standardised investigation form was developed based on the proposed model to collect the required assessment data from different enterprises. The formulation of the model appeared in Chapter 5. A practical model for cost-benefit analysis appeared in Chapter 6. This model is concerned with the analysis of cost of challenges facing information security in enterprises versus the benefits of applying the recommended security protection measures that can be used to reduce the effect of these challenges. This model seeks to help enterprises in selecting the optimum economical solution.

### **1.7.3 Evaluation**

The evaluation step of the research methodology includes also two stages, stage 5: model evaluation; and stage 6: discussion and conclusion. In stage five, in order to evaluate the developed enterprise information security readiness assessment model, testing was conducted using a developed investigation form and case study technique. The developed investigation form was used to collect data from public and private Saudi enterprises. Because of the sensitivity of research subject and the collected data, it requires to use a small sample of nine Saudi enterprises instead of having a larger one as was

planned at the early stages of this study. The collected data was analysed using a developed computer tool and graphs were developed to represent the information security situation of the investigated enterprises with different levels of detail. In addition, for the comparison between the investigated enterprises specialised in the same field, the nine Saudi enterprises were categorised under three groups. The collected data from the investigated enterprises is analysed in Chapter 7.

Finally, stage six is dedicated for discussing the key findings presented in Chapter 8. It also provides a comprehensive interpretation of findings. The conclusion and implications achievement of the research in terms of theoretical and practical contributions are reported and the direction for future research is presented as well. In addition, a number of recommendations for enhancing the information security practices inside Saudi enterprises are also presented.

## **1.8 Thesis Contributions**

The work presented in this thesis introduces a comprehensive enterprise information security risk management framework to fulfil the gap, which exists in the literature regarding the need to combine the two main approaches for enterprise information security risk management and incorporate the basic elements, main components and essential steps of the key risk management methodologies in a comprehensive reference information security risk management framework. The proposed framework consists of four dimensions and introduces analytical models for enterprise information security readiness assessment and for cost-benefit analysis. The research suggested these models to provide more effective assessment tools that capture the perceptions of the users of the information security systems in the assessment

programmes, and also to introduce a practical model for analysing the cost versus the benefit of applying the recommended security protection measures.

In this respect, the work provides the following main achievements:

- It provides a comprehensive enterprise information security risk management framework that integrates the prevailing two approaches for information security risk management and incorporates the main components of the key risk management methodologies.
- It provides information security readiness indicators, based on a mathematical model that integrates the risk control issues of the ISO/IEC 27002, according to the TOPE domains. The final assessment results presented as a single value for the decision maker to ease its understanding.
- It provides a cost-benefit approach for basing the selection of the recommended protection measures on an economical analysis. The proposed approach is based on a mathematical model that provides the best trade-off between the cost of adopting the recommended protection measures and the expected benefits as a result from reducing the security challenges.
- It presents practical case studies of nine Saudi enterprises using a developed computer tool in order to investigate the effectiveness of the proposed approach in evaluating enterprises information security readiness with different levels of details and in cost effectively evaluating the recommended best-practice protection measures. This will provide examples for future practical use of the proposed models developed in this research work.



## 1.9 Applicability and Usability

The importance of quantifying enterprises' IT systems security strength and risk continue to grow as private and public enterprises become totally dependent on these systems. Nowadays, the security of enterprises IT infrastructure has suffered because IT security protection measures are developed and implemented without any meaningful measures of their overall security strengths. This leaves the decision makers unable to assess the state of information security inside their enterprises. Even if the decision makers realised the urgent need for implementing more protection measures, the lack of efficient information security assessment models has hindered their ability to forecast the value to be gained by purchasing and implementing these protection measures. Without analytical models and tools for numerically assessing enterprises information security readiness, and economically assessing the gains from applying these measures, those tasked with making security decisions have been forced to depend mainly on expert's opinion only as a base for their decisions.

The work of this research would be useful to all enterprises concerned with improving their security readiness and providing e-services, compatible with international information security standards. This study will provide practical tools for the internal and the external assessors of enterprises information security readiness that has the following main features:

- The developed enterprise information security assessment model, presented in Chapter 5 of the thesis will provide an early assurance measure for the effectiveness of the implemented information security

protection measures which considers as an essential input to the developed EISRM framework presented in Chapter 3 of the thesis;

- the assessment results will determine numerically and graphically the overall enterprise information security effectiveness at five levels of detail;
- the results will determine the validity and effectiveness of the security controls contained in the security plans that are based on the perception of the users of the systems; and
- the results of the proposed cost-benefit analytical model, presented in Chapter 6 of this thesis, will facilitate the process of correcting weaknesses in the information security protection measures in an orderly and economical manner consistent with each enterprise mission and business goals.

## **1.10 Thesis Organisation**

This thesis is structured in five main parts, with each part, in turn, consisting of a number of chapters. Figure 1-2, holds the outline of the thesis and the arrows indicate the relationship between the various chapters.

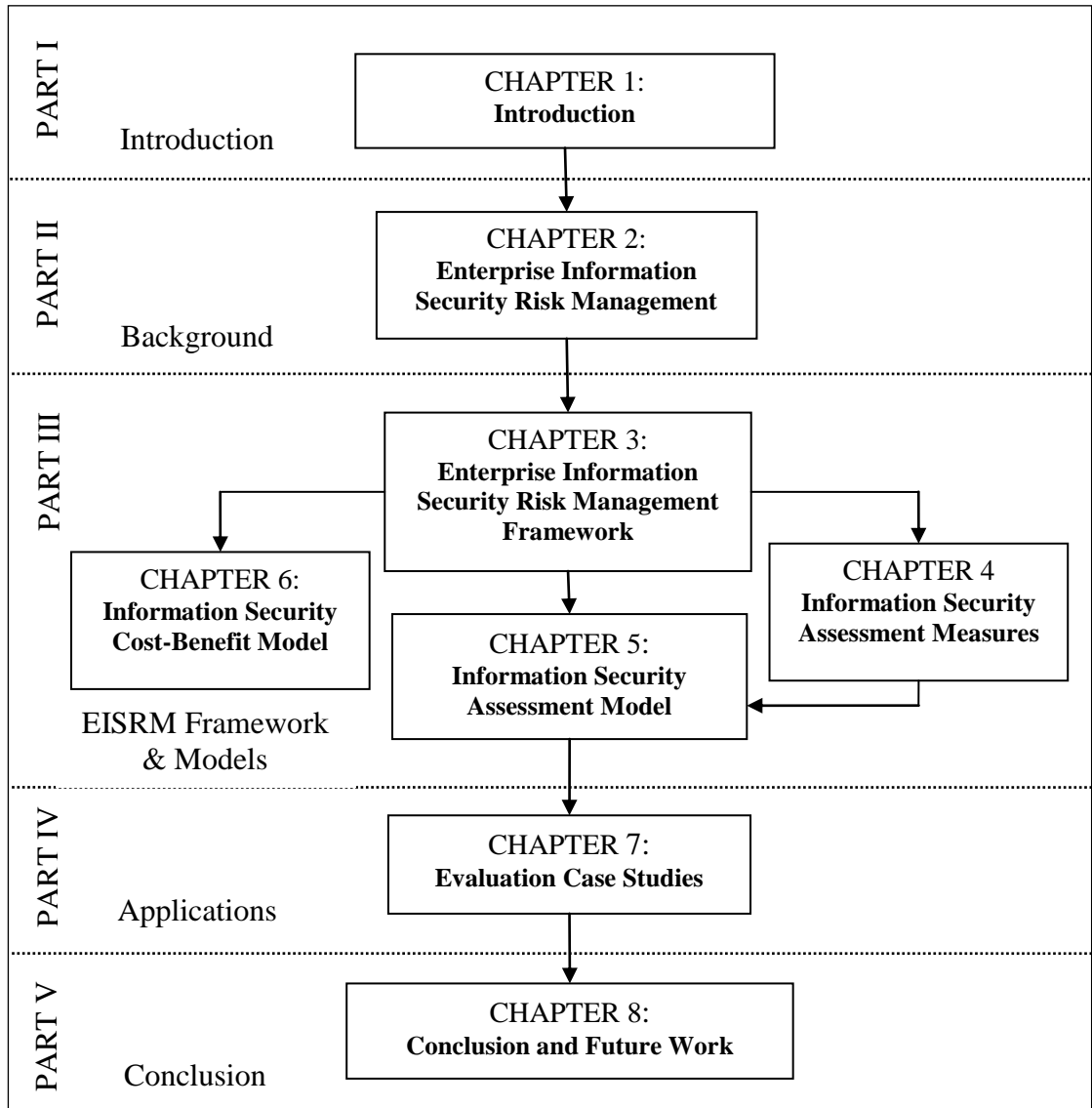
The second part provides the required background of the thesis and introduces the literature review of the problems considered. This part has one chapter as follows:

- Chapter 2 has four sections. The first section provides the needed background for the work presented by the thesis. The second section provides an overview of the existing risk-analysis based risk management methodologies followed by critical evaluation and comparison of these methods. The third section provides a critical

review of the best-practice approach for information security risk management. The fourth section of this chapter identifies the main requirements for developing a comprehensive enterprise information security risk management framework.

The third part is the theoretical part which provides the achieved theoretical contributions of the thesis. This part has four chapters as follows:

- Chapter 3 provides the developed comprehensive EISRM reference framework. The scope of the framework is based on the TOPE view and the management process of the framework is associated with the six-sigma DMAIC cyclic phases. The steps for running the proposed EISRM process are also discussed in detail. In addition, an approach for the application of the standard considering the information security policy in a way that emphasising continuous improvement is also presented. The structure and job description of the proposed team for the implementation of the work is also suggested.
- Chapter 4 presents the extracted ISO/IEC 27002 information security assessment measures that will be used as a base for conducting the assessment of enterprises information security readiness. An incremental assessment approach of enterprise information security is also presented. This approach has three levels of assessment with increasing security measures that can be used by enterprises for the gradual implementation of ISO security controls.
- Chapter 5 introduces a multi-level mathematical model for enterprise information security readiness assessment and describes its security readiness indicators at all levels.



**Figure 1-2 Thesis outline**

- Chapter 6 introduces a mathematical model which provides analytical tools for cost-benefit analysis of information security challenges versus the expected benefit from applying the recommended protection measures.

The fourth part is for the implementation studies. This part has one chapter as follows:

- Chapter 7 introduces the results of the assessment model and provides an analysis of the data collected from nine Saudi business

enterprises working in different fields. A real world example for the application of the cost-benefit model in one of the investigated enterprises is presented to illustrate its practical use for reaching the required protection level cost effectively.

Finally, conclusions and future work appear in part five with only one chapter. The final chapter, Chapter 8, concludes the findings of the research, and provides some suggestions for future research in the field of information security risk management and presents a number of recommendations for future improvements of the current situation information security risk management practices at Saudi enterprises.

## **1.11 Summary**

This chapter has outlined the structure of the research. It introduced the background of the study, and presented the research problem and objectives. The research was then justified; the research methodology is introduced; the thesis contributions and its parts are outlined. The coming chapter will proceed with a detailed description of the general background of the research to achieve the ultimate research objectives.

**PART II**  
**BACKGROUND**

**Chapter 2 ENTERPRISE INFORMATION**  
**SECURITY RISK MANAGEMENT**

# Chapter 2

## ENTERPRISE INFORMATION SECURITY RISK MANAGEMENT

### 2.1 Introduction

This chapter discusses the current approaches for enterprise information security risk management that are available in literature. These approaches are investigated in detail to identify basic elements, essential components and main steps of each one of them. A compiled list of high-level requirements is identified from the investigated approaches that could be used as a base for the development of the target reference comprehensive enterprise information security risk management framework. Based on these requirements, a suitable framework for enterprise information security risk management will be developed in Chapter 3.

#### 2.1.1 Enterprise Information Security

An enterprise is a complex system of cultural, process and technology components engineered together to accomplish organisational goals (Johnson and Whitman 1998). According to the European Commission (EC) definition, an enterprise is “*any entity engaged in an economic activity, irrespective of its legal form*” (EC 2009, p.5). If one applies these definitions, an enterprise is a complex system of people and technology organised together and working in a specific environment to achieve the strategic goals of the business. In fact, information is now becoming the lifeblood of any enterprise, and it has become the most valuable asset to any enterprise. In this respect, information like

knowledge, facts or data are important business assets that have greater value to any enterprise and needs to be properly protected (Solms and Eloff 2002).

Information security is defined as “*preservation of confidentiality, integrity and availability of information*” (ISO/IEC 27002 2005, p.1). The modern information security definition extends the previous definition to include authentication and non-repudiation, but they are not included in the ISO standard definitions till now, and throughout this thesis the standard ISO definitions will be used. Confidentiality of information is “*the property that information is not made available or disclosed to unauthorised individuals, entities or processes*” (ISO/IEC 7498-2 1989, p.5). Integrity is “*the property of safeguarding the accuracy and completeness of asset*” (ISO/IEC 13335-1 2004, p.4). Availability is “*the property of being accessible and usable upon demand by an authorised entity*” (ISO/IEC 7498-2 1989, p.5). Information security requirements, on the other hand according to Gerber et al. (2001), are concerned with the amount and specifics of security required for effective protection of the information resources.

From the above definitions one can conclude that the aim of enterprise information security is to achieve the protection of the enterprises’ information and information systems from unauthorised access, use, disclosure, modification, disruption or destruction of information and information resources whether accidental or deliberate (Tipton and Krause 2008).

### **2.1.2 Risks to Information Security**

The definition of risk varies based on different businesses and environments. Within information security context, risk is defined by ISO as “*the combination of the probability of an event and its consequence*” (ISO/IEC Guide 73 2002,



p.2). Carroll (1996) defines risk as *“the probability that a threat agent will exploit a system vulnerability to create a loss to confidentiality, integrity and availability of an asset”*. Threat is *“a potential cause of an incident that may result in harm to a system or organisation”* (ISO/IEC TR 13335-1 2004, p.4). According to Whitman and Mattord (2004), threat is defined also as *“any person or object that presents danger to an asset”*. Vulnerability is defined as *“a weakness of an asset or group of assets that can be exploited by one or more threats”* (ISO/IEC TR 13335-1 2004, p.4). Stephenson (2004) defines vulnerability as *“a weakness, flaw, hole or anything that maybe exploited by a threat that then results in a damaging outcome”*.

Depending on the above definitions, one can conclude that risks to information security can result from processes of modification, destruction, fabrication, disclosure, interruption, denial of service and theft of hardware, software or data. In order to manage these risks effectively, each enterprise must run a regular and effective risk management exercise to understand the nature of these risks and the possible outcomes. Hong et al. (2002) consider the running of regular information security risk assessment programmes by enterprises is among five main components to ensure effective information security architecture.

### **2.1.3 Importance of Risk Management**

The importance of managing information security risks continues to grow worldwide, as a result of the increasing breaches that affect the protection of information resources and consequently the business activities. The information security breaches survey of 2006 reported that the cost of security breaches to UK companies is of order of ten billion pounds per annum (ISBS

2006). This view is further supported by the Australian Computer Crime and Security Survey (ACCSS) of 2007 which reported that the total average annual losses for electronic attack, computer crime and computer access misuse or abuse reached \$ 241,150 per enterprise (ACCSS 2007).

The lack of properly implemented security measures to mitigate the rising information security risks has been reflected in recommendations by the governments and industry requirements for enterprises in running regular and effective risk management programmes. For example, the Sarbanes-Oxley Act of 2002, which is mandatory for all the enterprises working inside the United States of America (USA) irrespective of their size or business, requires the issuer of securities publicly traded on the USA financial markets to create a risk management model for their stakeholders (Raval 2004). Also, one of the main responsibilities of agencies under the FISMA (Federal Information Security Management Act) of the USA is to perform a regular risk assessment exercise (FISMA 2002).

It is clear from the previous published surveys that enterprises are potentially losing profit as a result of the absence of effective information security risk management programmes that proactively share in the protection of the enterprises' information resources. Therefore, enterprises are required to acquire and run effective information security risk management programme to not only achieve better protection of their information resources and consequently reduce the financial losses, but also to comply with the governmental laws and mandatory regulations which was applied in their environments (CSI 2007; BERR 2008; Ponemon Institute 2009).

## 2.2 Existing Risk Management Approaches

Today, there are various information technology and information security risk management methodologies; each of these methods has a different view and steps for identifying, analysing, evaluating, controlling and monitoring risks to information systems and information security. An extensive literature review reveals that there are two main approaches for enterprise information security risk management, namely the 'risk-analysis' approach and the 'best-practice' approach (ISO/IEC TR 13335-3 1998, p.2).

The risk-analysis approach for EISRM is concerned with the systematic in-depth identification and valuation of assets, the assessment of threats to those assets, the assessment of vulnerabilities and the use of different risk analysis techniques to calculate the value of risk. The results from these activities are then used to assess the identified risks and to recommend justified protection measures (Bott and Eisenhower 2002; ISO/IEC TR 13335-3 2004). The main characteristics of this approach are accurate results, appropriate identification of protection measures and detailed documentations that could be used in the management of security changes. Examples of methodologies under this approach include CRAMM, CORAS, EBIOS and OCTAVE (CRAMM 2001; CORAS 2003; EBIOS 2004; OCTAVE 2005).

On the other hand, the best-practice approach for enterprise information security risk management was developed to solve the major practical problems which appeared with the application of risk-analysis based methodologies. The main idea behind this approach is to use the best practice documents to standardise the security controls and to achieve a fast basic level of security inside the concerned enterprises. This approach utilises the checklist

technique to achieve its objectives, and it depends mainly on the compliance and certification processes to examine the existence of the required protection controls according to a specific standard (Solms B. and Solms R. 2001; Lech and Frank 2002; Fung et al. 2003; Tong et al. 2003). The main characteristics of this approach are reduced cost, ease in use, no training required and quick results (Warren and Hutchinson 2003). Examples of methodologies under this approach include the BSI-Germany, ISO/IEC 27002 and SOGP standards (BSI 2005; ISO 2005; ISF 2007).

The ISO/IEC 13335-3 document suggests the combination of the previous two approaches for achieving an improved comprehensive approach for enterprise information security risk management. However, the ISO/IEC 13335-3 document does not provide any guidance or explanation of the practical implementation of the suggested combined approach. Therefore, one of the main goals of this thesis is to show that combining these two approaches in an integrated comprehensive enterprise information security risk management framework shall benefit the information security risk management results.

The following sections provide an overview of the existing two approaches for information security risk management. Selective methodologies from each approach are investigated for the identification of basic elements, essential components and main steps that could be used to identify the main dimensions of the target EISRM framework defined for the purpose of this research study.

### **2.2.1 The Risk-Analysis Approach**

The enterprise information security risk-analysis approach has many different methods. These methods are structured here in three groups (according to the

source of the method); which are standard, professional and research methodologies. Selective key methods from each group will be discussed in terms of their objectives, structure, content, basic elements, essential components, steps and their ability to integrate technological, organisational, human and environmental components in studying enterprises' information security risks. The technological view in dealing with information security risk management is not sufficient for the development of comprehensive EISRM framework. Organisation, people and environment issues should also be addressed in the framework to ensure that it is comprehensive. These methods are selected because they are issued by well-known national and international standard organisations used internationally and often referenced in other methods.

#### **2.2.1.1 Standard Risk Management Methods**

National and International standard organisations suggested a number of risk management methods. Three of these methods are presented in the following:

##### **AS/NZS 4360 Risk Management Method**

The AS/NZS 4360 (2004) standard was prepared by the joint standards, Australia/New Zealand committee OB/7, as a second revision of the original Australia/New Zealand risk management standard, AS/NZS 4360 (1995). This standard is considered one of the first risk management standards to define a complete risk management method. The standard is very generic and independent of any industry or economic structure. The AS/NZS 4360 defines risk management process as the total process of identifying, controlling and eliminating or minimising uncertain events that may affect IT system resources, which are often best carried out by a multi-disciplinary team.

The AS/NZS 4360 standard includes five main steps and defines two parallel processes. Table 2-1 summarises the issues considered by each step and process. These issues are of general nature and can be associated with risk management problems in different fields, including IT. Davidson et al. (2004) checked the applicability of the standard for small and medium enterprises' information security risk management. The results showed that the AS/NZS 4360 structured risk management methodology should be supported by a database and outsourced skills to achieve better results.

**Table 2-1 The generic risk management steps & process of AS/NZS 4360**

<b>Steps</b>		<b>Issues Considered</b>
<b>1</b>	<b>Establish the context:</b> Define the basic parameters & set the scope for the rest of risk management process	External environment: Business, social, regulatory, cultural, competition, financial, political / Stakeholders & key business drivers / Organisation's: strengths, weaknesses, opportunities, threats.
		Internal environment: Stakeholders / Organisation's: strategy, goals, structure, resources (people, system, processes, capital), decision making.
		Risk management: The depth and breadth of the needed risk management activities.
		Risk criteria: Risk evaluation issues: environmental, legal, financial, social, humanitarian, operational, technical.
		Analysis: Define the structure of the analysis.
<b>2</b>	<b>Identify risks</b>	What can happen, when and where, why and how: events that could prevent, degrade or delay the achievement of objectives.
<b>3</b>	<b>Analyse risks</b>	Existing risk controls / Likelihood of occurrence of identified risks and their potential consequences / Levels of risks.
<b>4</b>	<b>Evaluate risks</b>	Levels of risk versus risk criteria considering risk treatment: balancing adverse outcomes with potential benefits of treatment, setting priorities and making decisions.
<b>5</b>	<b>Treat risks</b>	Specific cost-effective strategies and action plans for risk treatment: development and implementation (options, treatment, residual risk).
<b>The parallel process</b>		
	<b>Process</b>	<b>Issues Considered</b>
<b>1</b>	<b>Communicate and consult</b>	Plan / Consultative team / Stakeholders perceptions of risk / Understanding the basis of decision.
<b>2</b>	<b>Monitor and review</b>	The effectiveness of all steps for continuous improvement.

The AS/NZS 4360 standard is adopted later by ISO in 2008 to become the ISO/IEC 27005 standard. The ISO/IEC 27005 standard does not provide any specific methodology for information security risk management. The standard

leaves the decision to each enterprise to define its approach for risk management.

### **NIST SP 800-30 IT Risk Management Method**

The National Institute of Standards and Technology (NIST) of the USA issues a special publication NIST SP 800-30 (2002) “*Risk Management Guide for Information Technology Systems*”. The main objective of this publication was to help enterprises inside USA to assess their IT risks.

**Table 2-2 IT risk management steps & process of NIST SP 800-30**

<b>Steps</b>	<b>Input Issues</b>	<b>Output Issues</b>
<b>Risk assessment process</b>		
<b>1</b>	<b>System characterisation</b>	System: mission, hardware, software, interfaces, data and information.
<b>2</b>	<b>Threat identification</b>	System: boundary, functions / System and data: criticality, sensitivity.
<b>3</b>	<b>Vulnerability identification</b>	History of system attack / Data from intelligence agencies: NIPC (NIPC, 2007), OIG (OIG, 2007), FedCIRC (FedCIRC, 2007), mass media (SecurityFocus.com, SANS.org, etc).
<b>4</b>	<b>Control analysis</b>	Threat statement.
<b>5</b>	<b>Likelihood determination</b>	Reports from prior risk assessments / Audit comments / Security requirements / Security test results.
<b>6</b>	<b>Impact analysis</b>	List of potential vulnerabilities.
<b>7</b>	<b>Risk determination</b>	Current controls / Planned controls.
<b>8</b>	<b>Control recommendations</b>	List of current and planned controls.
<b>9</b>	<b>Results documentation</b>	Likelihood rating.
<b>Risk mitigation process</b>		
(1) Prioritise actions; (2) Evaluate recommended control options; (3) Conduct cost-benefit analysis; (4) Select controls; (5) Assign responsibilities; (6) Develop safeguard implementation plan; (7) Implement selected controls.		
Impact rating: Confidentiality / Integrity / Availability.		
Risks and associated risk levels.		

The NIST SP 800-30 document provides a foundation for the development of an effective risk management programme, containing both definitions and practical guidance necessary for assessing and mitigating identified risks

within IT systems. Table 2-2 summarises the issues associated with each of the NIST SP 800-30 main steps. For each step inputs, outputs and tasks are described under the form of guidelines, but without details concerning the implementation of the different tasks. The main characteristics of this method are specific for information systems, considered as a guide not a standard, have a tool for collecting the required data and self-directed by enterprise's stakeholders.

### **ISO/IEC TR 13335-3 IT Risk Management Method**

ISO/IEC TR 13335-3 (1998) is the third part of a five series technical reports, which adopts a more holistic approach for enterprises' information security management. This technical report provides guidance on the management of IT security presenting a foundation to assist enterprises in developing and enhancing their internal security architecture, and to establish commonality between enterprises. The document also provides guidance on the selection and use of safeguards which addresses the vulnerabilities of a particular network and its associated security risks. The IT security risk management method of ISO/IEC 13335-3 has five basic steps. Table 2-3 presents the issues associated with each of these steps.

The ISO/IEC 27005 standard, which appeared in 2008, revises the Management of Information and Communications Technology Security (MICTS) standards ISO/IEC TR 13335-3 (1998) plus ISO/IEC TR 13335-4 (2000). The ISO/IEC TR 13335-3 still appeared in literature as a guide for information security management. The MEHARI (MEthode Harmonisée d'Analyse du Risque Informatique) risk analysis method is compliant with ISO/IEC TR 13335 series of technical reports (Mehari 2007).



**Table 2-3 IT risk management steps & process of ISO/IEC TR 13335-3**

Steps		Issues Considered
1	Risk analysis	Boundaries: Technology & information / People: staff, subcontractors & others / Environment: building facilities / Activities: operations.
		Threats & vulnerabilities: Identifying both: accidental and deliberate risk sources / Assessing the likelihood of the occurrence of risk / Identifying weaknesses in: technology, people, physical environment, activities & procedures.
		Safeguards: Identifying existing and planned safeguards.
		Risks: Assessing the risks to which assets are exposed.
2	Safeguards selection	Constrains / Security architecture / Risk acceptance & residual risk.
3	Policy & plan	Policy: Why selected safeguards are necessary.
		Plan: How safeguards can be implemented.
4	Plan implementation	Practical implementation of safeguards according to plan / Awareness & training / Approval of plan.
5	Follow-up	Maintenance / Checking compliance / Monitoring / Incident handling / Change management.

### **Investigation of Standard Risk Management Methods**

The above standard organisations' risk management methods show that AS/NZS 4360 standard has a generic nature, NIST SP 800-30 is specific for IT systems and ISO/IEC 13335-3 is devoted for information security. NIST SP 800-30 considers only the surrounding technology, but ISO/IEC TR 13335-3 considers technology, people and environment, while AS/NZS 4360 considers technology, organisation, people and environment in assessing the boundary and the context of the risk management programme. Each method adopts its own risk management process, and the assessment of the current information security state is not addressed explicitly by these methodologies. Table 2-4 summarises the main issues considered by the standard organisations' risk management methods which could be adopted in developing the proposed EISRM framework presented in Chapter 3.

The above reviewed standard risk management methodologies are considered as high-level documents. They just provide guidelines and recommendations for running the risk management programme. These standards answer the "what?" question (what should be done regarding information security risk

management?) and leave the “how?” question to be answered by the professional risk management methods that will be discussed in the next section.

**Table 2-4 Relation of standard risk management methods and the proposed EISRM framework**

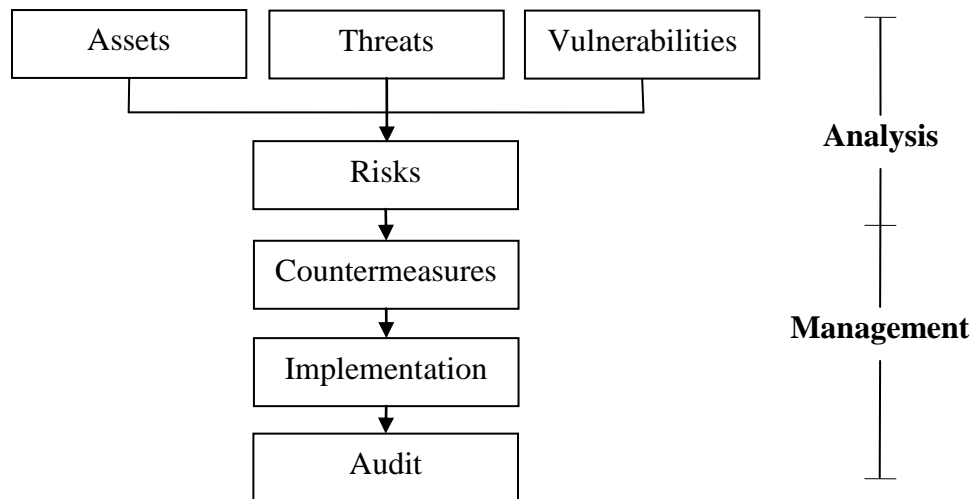
<b>Standard Method</b>	<b>Main Issues to be Considered by the EISRM Framework</b>
<b>AS/NZS 4360</b>	Fundamental concepts of risk management. Main steps of the risk management process. Cost-benefit strategies. Communicate and consult process.
<b>NIST SP 800-30</b>	Enrich the technology domain of the EISRM framework. Input/output technique for each step. Lists of assets, vulnerabilities and threats. Cost-benefit analysis. Impact analysis.
<b>ISO/IEC TR 13335-3</b>	The combined approach for risk management. Main terminologies of the risk management. Assessment of the current state information security. The lists of assets, vulnerabilities and threats. Follow-up (maintenance/checking compliance/monitoring/ incident handling) step.

### **2.2.1.2 Professional Risk Management Methods**

Professional organisations also suggest a number of risk management methods from four which are presented in the following.

#### **CRAMM IT Risk Management Method**

CRAMM (CCTA Risk Analysis and Management Method) is a qualitative risk analysis and management method developed by the UK government’s central computer telecommunication agency (CRAMM 2001). The method had undergone major revisions and is finally being distributed by a private company. The main objective of this method was to assess risks of the UK governmental agencies. CRAMM method has three main steps, as shown in Figure 2-1, and each of these steps is concerned with answering a specific question. In the following, the steps are given together with the questions they are supposed to answer.



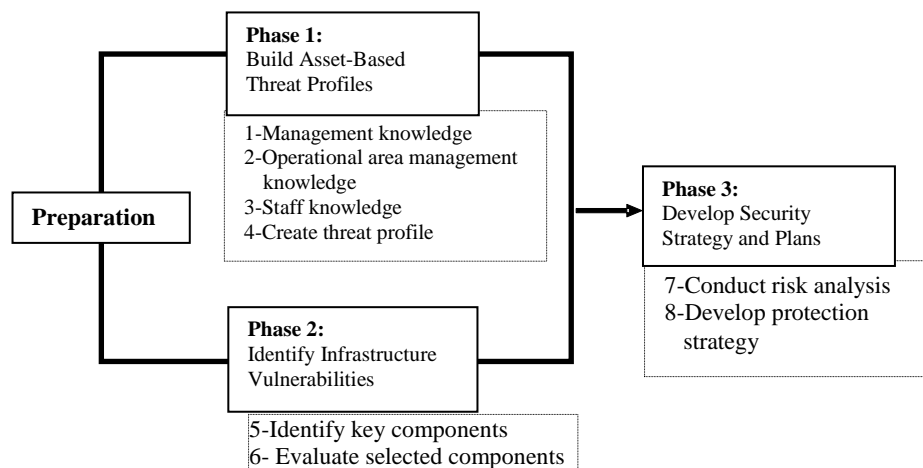
**Figure 2-1 CRAMM risk management process (CRAMM 2001)**

- **Asset identification and valuation;** this step answers the question of: Is there a need for security?
- **Threat and vulnerability assessment;** and the question for this step is: What and where is the security needed?
- **Countermeasures selection and recommendation;** and this should answer the question of: How can the security needs are met?

One of the main features of CRAMM is the identification of the IT assets. The information is gathered through interviewing the owners of the assets, the users of the system, the technical support staff and the security manager. The method neither helps in the calculation of return on investment for the proposed controls nor helps in the monitoring of the effectiveness of these controls. CRAMM does not assist in risk management improvement inside the considered enterprises, so no training, meetings or workshops are utilised. No steps in CRAMM are concerned with implementation and follow-up. CRAMM targeted a managerial level risk assessment, thus detailed technical system specific vulnerabilities are not addressed (Insight Consulting 2003).

## OCTAVE IT Risk Management Method

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method was developed at the Computer Emergency Response Team Coordination Center (CERT/CC) (CERT 2003). The method is considered as human centric qualitative risk analysis methodology. The main objective of this method is to examine enterprises' organisational and technological issues for developing a comprehensive picture for information security needs (Alberts and Dorofee 2003; Christopher and Audrey 2003). The method produced by OCTAVE has the following three main phases as shown in Figure 2-2.



**Figure 2-2 OCTAVE risk management process (Alberts 2003)**

- **Organisational view:** Building asset-based threat profile; this phase is associated with four processes.
- **Technological view:** Identifying infrastructure vulnerabilities; and this phase includes two processes.
- **Security strategy and plan development:** Developing security strategy and plan; and this phase also has two processes.

The method collects the required information at phase one through two workshops; the first with the senior management to define the scope of the

analysis, while the second with the staff that has more technical expertise. One of the main concepts of OCTAVE is self-direction. This concept means that people from various hierarchical levels of the enterprise are responsible to lead the information security risk evaluation programme. The outcome of the OCTAVE method is IT security strategy and plan. Therefore, it does not consider implementation and follow-up. The method does not consider the environmental factors under which the enterprise works (Lanz 2002; Passori 2004; Vennaro 2005; Broodryk 2005).

**CORAS Risk Management Method**

The CORAS (Consultative Objective Risk Analysis System) project was developed in 2003 as a scientific project in the European Union (EU), and it had partners from four countries: UK, Greece, Germany and Norway. The CORAS aims at addressing security-critical systems in general, but places particular emphasis on IT security (Raptis et al. 2002; Fu et al. 2008).

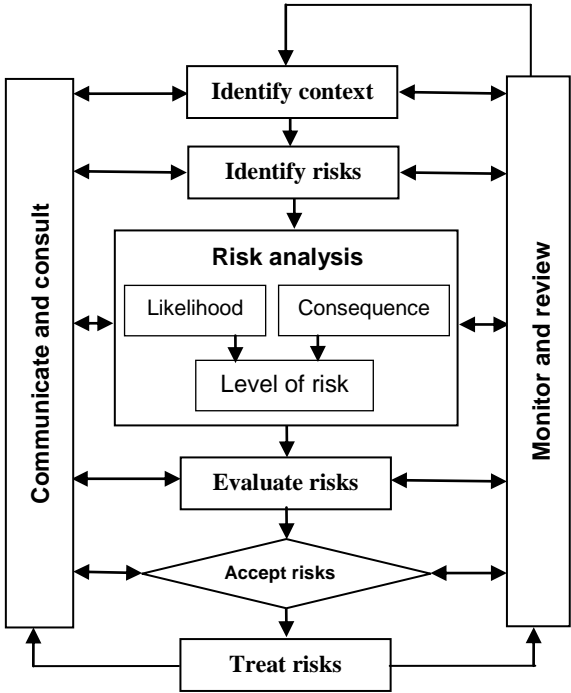
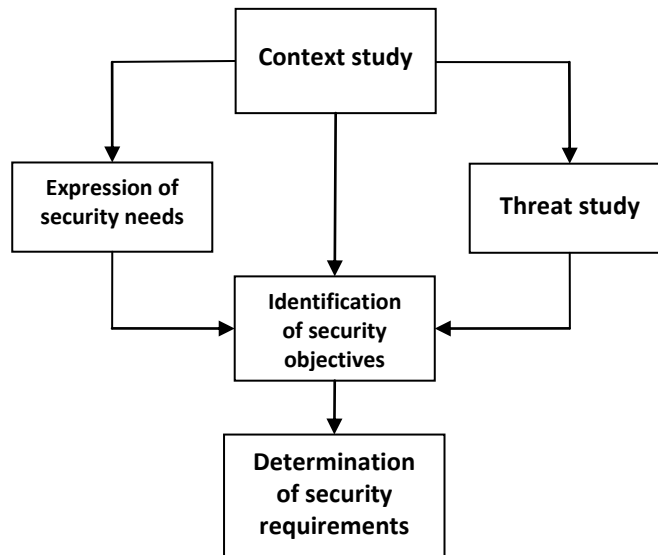


Figure 2-3 CORAS risk management process (Fredriksen et al. 2002)

The main objective of CORAS is to improve the traditional risk assessment methodologies to get better results by gathering well-known risk analysis techniques into an integrated security risk analysis method. The CORAS method considers a broad view to security that includes not only the technological aspects, but also the human interactions with technology and all relevant issues of the surrounding organisation and environment. The CORAS risk management process, as shown in Figure 2-3, adopts the risk assessment process of the AS/NZS 4360 risk management standard. The CORAS methodology has four dimensions namely the documentation framework, the risk management process, the integrated management and system development process and the platform for the inclusion of tools. The method has a scientific origin and depends on its own terminology for risk management process, which is considered as one of its main weaknesses. In addition, the method adopts the risk management process of the AS/NZS 4360 standard which is a generic risk management process and is not dedicated for information security (Vraalsen et al. 2005).

### **EBIOS Risk Management Method**

The EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) method has been created in 1995 by the DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) (EBIOS 2004). The method is used to assess and treat risks related to information system security. The EBIOS method is widely used inside France for the analysis of French military and governmental information systems. However, it is also used in industry and other business enterprises. The method is composed of the following five steps as shown in Figure 2-4.



**Figure 2-4 EBIOS risk management process (EBIOS 2004)**

- **Context study:** The enterprise is studied by analysing its mission, business, own values, constraints, structure and the regulatory references applicable to the enterprise. The output of this step is the description of the essential elements of the concerned enterprise.
- **Expression of security needs:** The purpose of this step is to allow the information system users to express their security needs for functions and information they handle.
- **Threat study:** This step aims at determining the threats affecting the information system.
- **Identification of security objectives:** In this step, the enterprise's security needs are compared with the identified threats. The risks are thus highlighted and can be treated by some security objectives.
- **Determination of security requirements:** The security requirements are finally selected to achieve the defined security objectives.

The method has analytical approach in dealing with risk, and it has an open-source software tool that is used especially for collecting data for an EBIOS study and for producing summary documents (Fenz et al. 2009).

## Investigation of Professional Risk Management Methods

The previous review shows that CRAMM and EBIOS have a technical nature. OCTAVE considers technical and organisational factors, while CORAS considers technical, organisational, human and environmental factors in dealing with the risk management programme.

OCTAVE and EBIOS methods use the stakeholders in running the risk management programme, but CRAMM needs outsourced expertise. Table 2-5 summarises the main issues of the above reviewed professional organisations' risk management methods that should be considered by the proposed EISRM framework presented in Chapter 3.

**Table 2-5 Relation of professional risk management methods and the proposed EISRM framework**

<b>Professional Method</b>	<b>Main Issues to be Considered by the EISRM Framework</b>
<b>CRAMM</b>	Identification of IT assets. Sources of threats and vulnerabilities.
<b>OCTAVE</b>	Analysis team from the enterprise itself to lead the whole risk management activities. Development of security strategy and plan.
<b>CORAS</b>	Integration of risk management techniques. Platform for the inclusion of tools.
<b>EBIOS</b>	Identification of security needs by the users of the system. The analytical approach in dealing with risks. Identification of the security objectives. Identification of the security requirements.

Table 2-6 summarises and compares the main issues considered by the above reviewed risk-analysis based methodologies. These methodologies, as shown in Table 2-6, have the following main limitations:

- Most of these methods are country based and devoted for specific domain.
- In general, these methodologies lack definite framework or common approach for running enterprise's wide risk management programme that is based on effective Information Security Management System (ISMS).



- Most of these methods are complex and depend on manual processes, and their results are informal most often in natural language.
- The assessment of the current state information security is not addressed by all of these methods.
- The results of these methods are not reusable to achieve continuous monitoring of the information security improvements.
- No reference standard economic model for the analysis of the proposed mitigation plans.

**Table 2-6 Comparison of the risk-analysis based methods**

Issue	Risk Analysis Method			
	CRAMM	OCTAVE	CORAS	EBIOS
<b>Origin</b>	UK	USA	Europe	France
<b>Target sector</b>	Business	Industry	Industry	Military
<b>Domain</b>	Information technology systems	Security critical systems	Security critical systems	Information systems security
<b>Standard terminologies</b>	No	No	No	No
<b>Users of the method</b>	Outside Expert	Stakeholders	Outside Expert	Stakeholders
<b>Standard ISMS</b>	No	No	No	No
<b>Type of results</b>	Reports	Reports	Reports & Graphs	Reports
<b>Comprehensiveness</b>	T	TO	TOPE	T
<b>Assess current state</b>	No	No	No	No
<b>Economic analysis</b>	No	No	No	No
<b>Type of analysis</b>	Qualitative	Qualitative	Qualitative	Qualitative
<b>Software tool</b>	Yes	Yes	Yes	Yes

### 2.2.1.3 Researchers Risk Management Methods

The management of information security risks has not only been the concern of standard or professional organisations, but they are also the concern of individual researchers and research projects. Key methods of this type are introduced in Table 2-7. The main steps that are considered by these methods also appeared in the same table. Most of the researchers' methods concentrated only on improving techniques for calculating the risk value.

**Table 2-7 Key researchers risk management methods and techniques**

Method / Title		Author/Year/Description/Steps/Technique
1	<b>RAMeX</b>	<p>Kaily and Jarrah (1995)</p> <ul style="list-style-type: none"> <li>• Has two main phases: risk analysis and risk management.</li> <li>• The risk analysis has five steps producing identifications of: assets, threats, vulnerabilities, existing security countermeasures and business impact.</li> <li>• The risk management has two steps: assessment of security countermeasures; recommendation of countermeasures to select from.</li> </ul>
2	<b>RiMaHCoF</b>	<p>Smith and Eloff (2002)</p> <ul style="list-style-type: none"> <li>• Concerned with IT risk in health-care.</li> <li>• Considers four steps for risk management, including risk assessment.</li> <li>• Risk assessment stage is based on a cognitive fuzzy-logic technique.</li> </ul>
3	<b>BPIRM</b>	<p>Robert and Rolf (2003)</p> <ul style="list-style-type: none"> <li>• Combines the security focus with the business focus.</li> <li>• Has two elements: a process and a content model.</li> <li>• The process has six phases, and the content model has seven layers.</li> <li>• The content model is based on the "value chain" business view.</li> </ul>
4	<b>Ontology-based</b>	<p>Liu (2007)</p> <ul style="list-style-type: none"> <li>• Ontology is a collection of concepts, which represent higher level knowledge in the knowledge hierarchy in a given enterprise.</li> <li>• Enables knowledge sharing among security personnel, to support the management of risk for "Supply Chain Management (SCM) information security".</li> <li>• Uses the ontology principles of the "Unified Problem-solving Method Development Language (UPML).</li> <li>• Has three parts: "domain" associated with knowledge acquisition and modelling; "task" related to risk rating &amp; management; and "resolution" concerned with minimising SCM information security risks using problem solving method based on ontology.</li> </ul>

#### **2.2.1.4 Summary**

The above standard, professional and researchers' information systems and information security risk management methods are discussed in details. However, the major issues of all previously reviewed methods are of similar nature, these methods are structured in different ways. The previous review provides two main benefits: on one hand, it gives a broad view of the steps of how IT risk management can be performed, and on the other hand, it identifies the risk management issues that need to be taken into account as seen by different methods.

## **2.2.2 The Best-Practice Approach**

The best-practice approach for information security risk management depends mainly on the information security management best-practice standard documents in assessing enterprises' information security according to the requirements of these standards. Eloff and Solms, (2000a) mention that best-practices are the combined experiences of several companies that have already had great influence in the information security environment. Recently, there are many different information security standards and recommended security best-practice documents that evolved to address the issues of enterprise's information security risk management from different perspectives. These standards are becoming increasingly important for assessing enterprises' information security readiness and for establishing a common safe environment for their business activities (Eloff and Solms 2000b; Allen 2001; Tsoumas and Tryfonas 2004).

National and international organisations, such as International Standards Organisations (ISO), the German Bundesamt für Sicherheit in der Informationstechnik (BSI Germany) and the Information Security Forum (ISF), have published information security management standards (ISO/IEC 2005; BSI-Germany 2004; ISF 2007). Two of the above mentioned best-practice standards will be presented in the following sections.

### **2.2.2.1 The Standard of Good Practice for Information Security**

The ISF is an international independent organisation dedicated to benchmarking and best practices in information security. It was established in 1989 as a European security forum, and then expanded its mission and membership in the 1990s. Nowadays, it includes hundreds of members,

including a large number of 300 leading organisations concerned with information security from all over the world (ISF 2008).

The ISF published the first issue of the Standard Of Good Practice (SOGP) for information security in 1996. The SOGP standard is based on the extensive knowledge and expertise of ISF members, the views of other national and international standard organisations and the results of earlier ISF information security status surveys. The standard is free for the members and the most recent version of the SOGP standard was published in 2007. Participants can make a comprehensive assessment of how well their enterprises are conforming to the standard (ISF 2007).

**Table 2-8 The standard of good practice for information security aspects, areas and sections**

<b>Aspect</b>		<b>Description</b>	<b>Area</b>	<b>Section</b>
<b>1</b>	<b>Security management</b>	Covers topics relating to high-level direction for information security, arrangements for information security across the organisation and establishing a secure environment.	7	36
<b>2</b>	<b>Critical business applications</b>	Covers topics relating to requirements for securing business applications, identifying information risks and determining the level of protection required to keep information risks within acceptable limits.	6	25
<b>3</b>	<b>Computer installations</b>	Covers topics relating to the design and configuration of computer systems, management activities required to establish a secure computer installation and maintain service continuity.	6	31
<b>4</b>	<b>Networks</b>	Covers topics relating to network design and implementation, management activities required to run and manage secure networks including: local and wide area networks and voice communication networks.	5	25
<b>5</b>	<b>Systems development</b>	Covers topics relating to the application of information security during all stages of systems development including: design, build, testing and implementation.	6	23
<b>6</b>	<b>End user environment</b>	Covers topics relating to local security management, protecting corporate and desktop applications, and securing portable computing devices.	6	26
<b>Total areas and sections</b>			<b>36</b>	<b>166</b>

The SOGP standard presents a comprehensive set of practical security specific controls. The standard comprises ten main parts including: high-level summary information, six detailed 'aspects' and a comprehensive index. The six aspects of security include: security management, critical business applications, computer installations, networks, systems development and end user environment. The standard has a total number of 36 security areas and 166 sections that address the six main aspects, as shown in Table 2-8. The standard is structured to cover the full spectrum of security related topics. However, such a structure means that there is some repetition of topics across these aspects.

#### **2.2.2.2 The ISO/IEC 27002 standard**

The ISO/IEC 27002 is a management standard providing a code of practice for information security management. The standard was originated from the British standard BS 7799 and was first issued in 2000. It was revised and reissued in 2005. It is used by enterprises in managing their information systems security. The standard is adopted by various countries and used as a base for their regional information security standards. The ISO/IEC 27002 standard, as shown in Table 2-9, states 11 clauses, 39 security objectives and provides 133 controls to achieve those objectives.

In the past, various papers have advocated the use of international information security management standards. Solms (1999) emphasised the need for using such standards considering the problem of information security as a global problem not a domestic one. He considered the British standard, BS 7799, as a possible standard that would provide the basis for safe driving on the information super-highway.

**Table 2-9 The ISO/IEC 27002 clauses, objectives and controls**

Clause		Description	Objective	Control
1	<b>Security Policy</b>	Aims to provide management direction and support for information security.	1	2
2	<b>Organisation of information security</b>	Organisation of the process implemented to manage information security.	2	11
3	<b>Asset Management</b>	Concentrate on asset inventories, information classification and labeling.	2	5
4	<b>Human resources security</b>	Considers permanent, contractor and third party user responsibilities.	3	9
5	<b>Physical and environmental security</b>	Controls the allowance of only authorised access to facilities and secure areas.	2	13
6	<b>Communications and operations management</b>	Focus on the correct and secure operation of information facilities.	10	32
7	<b>Access control</b>	Manage user access to information and include clear desk, network access and operating system access principles.	7	25
8	<b>Information systems acquisition development and maintenance</b>	Ensure the security of user-developed and the information system products.	6	16
9	<b>Information security incident management</b>	Ensures that incidents are communicated in a timely manner and that corrective action is taken.	2	5
10	<b>Business continuity management</b>	Focuses on business continuity plans and testing.	1	5
11	<b>Compliance</b>	Achieve it accordance with statutory, regulatory or contractual requirements or obligations, laws, audit and policy.	3	10
<b>Total objectives and controls</b>			<b>39</b>	<b>133</b>

Solms B. and Solms R. (2001) recommended the use of the first version of ISO 17799, which appeared a year before. In this respect, they presented an approach of incremental certification of information security. According to this approach, standard security requirements are divided into levels and are implemented gradually in steps, level by level, until all requirements of all levels are covered. Janczewski and Xinli (2002) reviewed the AS/NZS 4444 standard, which is based on the British standard BS 7799, considering a

specific application concerned with health information systems' requirements. Eloff J. and Eloff M. (2003) stressed the need for using ISO 17799, in order to provide baseline security, which is the basic information security that needs to be acquired by enterprises working in different fields. In addition, a method, based on adequacy of security, for the evaluation of the use of ISO 17799 is presented in Fung et al (2003). The method considers four security protection classes ranging from inadequate to adequate classes of protection through minimal and reasonable classes. Bellone (2008) presents a practical approach for information security management system implementation. The approach is used to attain the necessary escape velocity to achieve the expected results. The escape velocity concept is defined as the momentum a project must have in order to escape resisting forces without reverting back and failing. The approach is simple and straightforward in applying ISO/IEC 27002 to the enterprises using a computer tool. The approach did not provide any criteria for the priority in applying this standard, and it also did not include an evaluation approach for the implemented security controls. The adopted Key Performance Indicators (KPIs) of COBIT (Control Objectives for Information and related Technology) by this approach do not appear to be effective in measuring the performance of ISO/IEC 27002, as its success in measuring the performance of COBIT sub-domains DS4 "*Ensure business continuity*" and DS5 "*Ensure systems security*".

The above reviewed research studies agreed on the need for using international information security management standards, BS 7799 in the beginning and then the first version of ISO/IEC 27002. They provided various ways for this use, including incremental use and evaluations of use based on adequacy of security. However, according to the author's knowledge, neither

of these research papers nor any known publication has, so far, developed a numerical assessment model based on a comprehensive standard information security risk management framework, for the use of ISO/IEC 27002 standard. The process of development of a comprehensive information security assessment model that is based on the international information security standards will be addressed later in Chapter 5 of this thesis.

### **2.2.2.3 Information Security Management Methods**

Researchers also suggest a number of information security management methods, two of these methods are presented in the following.

#### **The PROTECT Information Security Management Method**

Eloff J. and Eloff M. (2005) introduced a comprehensive approach towards information security, namely PROTECT, which is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance and Team. The seven components of the PROTECT method are aimed at implementing and managing an effective information security programme from technology to people perspective. They are summarised below:

- Policy component includes information security policies, procedures and standards, as well as guidelines.
- Risk methodologies such as CRAMM and OCTAVE, as well as automated tools to identify system vulnerabilities.
- Objective component refers to implementation of controls by considering the risk environment of the enterprise and not implementing more or less controls than what is required.
- Technology component includes hardware, software and systems' product components of the IT infrastructure.



- Execute component refers to a proper information security management system environment.
- Compliance component covers both internal compliance, with the enterprise's policies, and external compliance, with information security expectations set by outside parties.
- Team refers to the people component, i.e. all the employees of the enterprise, where each has a responsibility towards securing information.

### **The Capability Maturity Model Security Management Method**

The Capability Maturity Model (CMM) methodology provides components used to protect information assets against unauthorised access, modification or destruction (MCCarthy and Campbell 2001). The method is based on a holistic view of information security and it encompasses seven main components, as follows:

- Security leadership by means of an executive level security representative and an information security strategy.
- A security programme with defined roles and responsibilities for information security tasks.
- Security policies, standards and guidelines that are used to direct information security tasks.
- Security management that constitutes day-to-day operations and monitors users and technology.
- User management that focuses on awareness of policies and manages user profiles.
- Information asset security that encompasses the technology aspects of information security.

- Technology protection for the environment and continuity, which focuses both on business continuity and disaster recovery.

#### **2.2.2.4 Summary**

The above reviewed standards and researchers best-practice information security management methods introduce a base for information security management. However, these methods do not provide any application rules or numerical measures that can lead to information security readiness assessment indicators (Karabacak and Sogukpinar 2006). Such indicators would be essential for identifying information security weaknesses in enterprises so that these enterprises can establish suitable security enhancement directions, in order to satisfy the requirements of the security management standards (Solms 2005; Bellone 2008). Eloff and Solms (2000b) show that the nature of the available information security best-practice standards is qualitative. They raised the issue of the importance of designing and implementing a measuring instrument that could be customised and utilised by enterprises in quantifying their information security status. Their paper concluded that there is an urgent need for developing a quantification model for measurement, specifically against the ISO/IEC 17799 standard.

In light of the above reviewed standard, professionals and researchers risk management approaches, and according to the recommendations given by the ISO/IEC 27005 risk management standard, the author of the thesis proposed a set of main requirements for developing an effective enterprise information security risk management framework that will be discussed in the next section.

### **2.3 Risk Management Main Requirements**

A thorough investigation of the main applied information security risk management approaches highlighted the need for a new comprehensive

information security risk management framework that enables enterprises to address all aspects of information security risk management in an effective and efficient manner. Therefore, an information security risk management framework should consider the following main requirements:

- Incorporate the basic elements of the risk management methodologies.
- Possess a comprehensive scope in that not only limit the analysis of the information security risk management on the technical issues, but also include organisation, people and environment issues as well.
- Depend on a management process that integrates the main approaches for information security risk management and incorporates the essential components of the risk management methodologies.
- Assess numerically the current situation enterprise information security using valid and reliable modelling technique.
- Base the selection of the recommended ISO/IEC 27002 security protection measures on an economical analysis.

In addition to the previous main requirements, a well defined information security policy, a trained supporting team from inside enterprises and a clear identification of risk management terms and concepts play a crucial role in successfully developing an effective information security risk management framework. Each of the previously stated main requirements will be discussed in more detail in the following sections.

### **2.3.1 Risk Management Basic Elements**

There is a need for underlying standard that provides precise definitions for the basic elements, essential components, concepts and terminologies of the whole process of enterprises information security risk management. This standard will clarify the confusion resulted from inconsistent use of terms and

concepts in the field of information security (Hogganvik and Stolen 2005; Matulevicius et al. 2008). Based on the literature review presented in Section 2.2, a list of basic elements was compiled from the AS/NZS 4360, NIST SP 800-30, ISO/IEC TR 13335-3, OCTAVE, CORAS, EBIOS and CRAMM risk management methodologies. Table 2-10 holds the proposed list of information security risk management basic elements which, in the opinion of the author of the thesis, could aid in formulating the proposed EISRM framework. Table 2-10 shows the alignment between the basic information security risk management elements with different concepts involved in the studied resources.

### **2.3.2 Risk Management Scope**

Most IT risk management methodologies have focused mainly on technology solutions and have not yet fully adopted a comprehensive approach that addresses organisational, human and environmental factors in studying the information security issues.

Beznosov and Beznosova (2007) discuss the imbalance of the security problem space. They noticed that over 94% of the public research in computer security has been concentrated only on the technological factors. Chang and Ho (2006) study the effect of the organisational factors on the implementation of the information security management system. The results show direct influence of the organisational factors on the effective implementation of the BS7799 standard. Kraemer et al. (2009) study the effect of human and organisational factors in computer and information security. They proved that human and organisational factors play a significant role in the development of the computer and information security vulnerabilities.

**Table 2-10 Mapping the basic elements & concepts of key risk management methods to the identified basic elements of the proposed EISRM framework**

Concept	Key Risk Management Methods					
	AS/NZS 4360	NIST 800-30	OCTAVE	CRAMM	EBIOS	CORAS
<b>Asset</b>	Asset Primary asset Supporting asset		Asset Key component	Asset	Asset Essential element Entity	Asset
<b>Security criterion</b>	Property criterion	Security goal	Criterion Classification criterion	Property	Security criterion	Security property
<b>Threat</b>	Threat Threat source Origin of threat	Threat Threat source Threat action	Area of concern Actor		Threat Event Threat agent Attack method	
<b>Vulnerability</b>	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability
<b>Impact</b>	Impact Consequence	Impact Consequence	Outcome impact	Impact	Impact	Unwanted incident
<b>Risk</b>	Risk	IT-Risk	Risk	Risk	Risk	Risk
<b>Control</b>	Control	Control	Protection practices Countermeasure	Countermeasure	Security solution	

Werlinger et al. (2009) suggest an integrated framework to view the human, organisational and technological challenges of IT security management. Table 2-11 shows the alignment between the TOPE scope and the different resources discussed in Section 2.2. This alignment shows the main aspects that should be considered in each of the TOPE domains by different information security management standards. In addition, it shows that the ISO/IEC 27002 information security management standard is comprehensive enough, compared to other standards and methods to be adopted as a base for assessing enterprises information security readiness.

### **2.3.3 Risk Management Process**

The management system is the framework of processes and procedures used to ensure that an enterprise can fulfil all tasks required to achieve its objectives. The main purpose of the management system is to put the enterprise in a continuous improvement for the concerned domain. The above review shows that each of the reviewed risk management methods adopts its own management system in conducting the risk management process. ISO depends on the Plan, Do, Check and Act (PDCA) process for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the information security management system of any enterprise. The concept of PDCA model was originally developed in 1930 by Walter Shewhart. The PDCA concept was taken up and promoted very effectively from the 1950s by W. Edwards Deming, and is consequently known by many as "*Deming Wheel*". The application of the PDCA for information security risk management is presented in Table 2-12 (ISO/IEC 27005 2008). The application of the PDCA model in the risk management process lacks the fair alignment of the risk management activities. It is apparent that the scientific origin of the PDCA

**Table 2-11 Mapping the contents of key information security management methods to the TOPE scope**

TOPE	Key Security Management Methods			
	ISO/IEC 27002	SOGP	PROTECT	Capability Maturity Model
<b>Technology</b>	<ul style="list-style-type: none"> <li>- Communications and operations management</li> <li>- Access control</li> <li>- Information systems acquisition, development and maintenance</li> </ul>	<ul style="list-style-type: none"> <li>- Computer installations</li> <li>- Networks</li> <li>- System developments</li> </ul>	<ul style="list-style-type: none"> <li>- Technology controls</li> <li>- Implementation of controls</li> </ul>	<ul style="list-style-type: none"> <li>- Technology protection</li> </ul>
<b>Organisation</b>	<ul style="list-style-type: none"> <li>- Security policy</li> <li>- Organisation of information security</li> <li>- Asset management</li> <li>- Information security incident management</li> <li>- Business continuity management</li> </ul>	<ul style="list-style-type: none"> <li>- Critical business applications</li> <li>- Security management</li> </ul>	<ul style="list-style-type: none"> <li>- Risk methodologies</li> <li>- Policy component</li> <li>- Information security</li> </ul>	<ul style="list-style-type: none"> <li>- Security policies</li> <li>- Security programme</li> <li>- Information asset security</li> <li>- Security management</li> </ul>
<b>People</b>	<ul style="list-style-type: none"> <li>- Human resources security</li> </ul>	<ul style="list-style-type: none"> <li>- End user environment</li> </ul>	<ul style="list-style-type: none"> <li>- Team</li> </ul>	<ul style="list-style-type: none"> <li>- Security leadership</li> <li>- User management</li> </ul>
<b>Environment</b>	<ul style="list-style-type: none"> <li>- Physical and environmental security</li> <li>- Compliance</li> </ul>		<ul style="list-style-type: none"> <li>- Compliance</li> </ul>	

“hypothesis, experiment and evaluate” hinder its ability to capture the risk management activities in a proper way (Anderson and Moore 2006).

**Table 2-12 The ISO information security risk management process**

ISMS Process		Explanation
1	<b>Plan</b>	Establish the context Risk assessment Developing risk treatment plan Risk acceptance
2	<b>Do</b>	Implementation of risk treatment plan
3	<b>Check</b>	Continual monitoring and reviewing of risks
4	<b>Act</b>	Maintain and improve the information security risk management process

Boynton (2007) suggests using improved methodologies within security environment. The six-sigma process is suggested as a suitable and well established management process that could be used in achieving continuous improvement of enterprises’ information security practices. Table 2-13 maps the processes of the key risk management methods to the six-sigma cyclic phases. This mapping shows how DMAIC process can accommodate risk management main processes, providing a potential risk management process.

### **2.3.4 Assessment of Information Security Situation**

The ISO/IEC 27004 measurement standard stated that, in order to provide convincing arguments to the top management for initiating an information security programme, the information security officers must identify risks to organisational processes. The standard also suggests developing a measurement system capable of determining the effectiveness of controls introduced in accordance with Annex A of the ISO/IEC 27001 standard. The need for new techniques for assessing the effective use of the ISO/IEC 27002 in protecting the information resources is an important consideration by many papers and research studies. Siponen (2000) urged the need for an adequate maturity measurement system for information security management practices.



**Table 2-13 Mapping the processes of key risk management methods to the DMAIC phases of the six-sigma model**

Six-Sigma	Key Risk Management Methods					
	AS/NZS 4360	ISO/IEC TR 13335	NIST SP 800-30	OCTAVE	CRAMM	EBIOS
<b>Define</b>	Establish the context	Risk analysis	System characterizations Threat identification Vulnerability identification	Management knowledge Operational area management knowledge Staff knowledge Create threat profile Identify key components Evaluate selected components	Asset identification Asset valuation Threat and vulnerability assessment	Context study Expression of security needs Threat study
<b>Analyse</b>	Identify risks Analyse risk Evaluate risk		Control analysis Likelihood determination Impact analysis Risk determination	Conduct risk analysis		Identification of security objectives
<b>Improve</b>	Treat risk	Safeguards selection Policy & plan Plan implementation	Control Recommendations Risk assessment report Cost-benefit analysis and selection of controls Implementation	Develop protection strategy	Countermeasure selection and recommendation	Determination of security requirements
<b>Control</b>	Communicate and consult Monitor and review	Follow-up	Results documentation Test and evaluate		Audit	

Boehmer (2008) evaluated the effectiveness of the information security management based on a measurement technique that includes the coverage of the business process, the controls operationalisation and the completeness of the security policy. Wiander (2007) mentioned that ISO/IEC 27002 certification can give enterprises a false sense of security. He suggested that enterprises should develop and implement an information security measuring system that internally assesses the readiness of their information security protection measures.

### **2.3.5 Economical Analysis of Security Investments**

The cost versus benefit from applying the mitigation plans need to be evaluated using efficient techniques. Applying conventional financial justification techniques (i.e. return on investment, internal rate of return, annual net present value, etc...) are often inadequate to measure the overall effectiveness of security controls. These inadequacies mainly stem from exclusion of the qualitative nature of the involved factors. Various factors should be considered in this evaluation including: the risk of loss that may result from the different challenges and the cost of the protection measures and its effect on the operation of the enterprise. An efficient technique has to deal with both financial and non-financial aspects to achieve satisfied results (Cavusoglu et al. 2004a; Tsiakis and Stephanider 2005; Anderson and Moore 2006; Johansson et al. 2006).

### **2.3.6 Other Requirements**

One of the important requirements in designing an effective EISRM framework is the identification of a suitable strategy for creating enterprise information security policy. This policy should be based on the international information

security standards and possess a continuous nature to evolve with the changes of the information security domain (Bakry 2003a). In addition, the involvement of a trained team consists of the system owners, custodians and users of the concerned enterprise in the process of planning, designing and implementing the information security risk management programmes is of important consideration for the success of these programmes.

## **2.4 Summary**

The conclusion from reviewing the key enterprise information security risk management standard, professional and researchers methods is that they provide different tools and techniques for reaching generally the same goal of protecting enterprises information resources by defining suited security protection measures with the help of a risk management approaches. However, these methods achieve this goal by different approaches: risk-analysis approach and best-practice approach, and have different levels: some methods are high-level just for providing guidelines, while others are more detailed and concentrate mainly on achieving better risk analysis results. Most of the available risk management methods have technical nature and ignore the assessment of the current state enterprise information security. In addition, these methods are not depending on standard economical approach in selecting the relevant security protection measures. Each method has its own strengths and weaknesses, and it is believed that integrating these methods in a reference comprehensive enterprise information security risk management framework will achieve better results.

# **PART III**

## **THEORETICAL ANALYSIS**

**Chapter 3 AN ENTERPRISE INFORMATION SECURITY  
RISK MANAGEMENT FRAMEWORK**

**Chapter 4 ENTERPRISE INFORMATION SECURITY  
ASSESSMENT MEASURES**

**Chapter 5 A MODEL FOR ENTERPRISE INFORMATION  
SECURITY READINESS ASSESSMENT**

**Chapter 6 AN ENTERPRISE INFORMATION SECURITY  
COST-BENEFIT MODEL**

## **Chapter 3**

# **AN ENTERPRISE INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK**

### **3.1 Introduction**

This chapter is concerned with the development of a comprehensive enterprise information security risk management (EISRM) framework that could contribute in effective establishment of the required enterprise IT safe environment. The proposed framework is designed to integrate the main approaches for enterprise information security risk management from one hand, and incorporate the basic elements, main steps and essential components of the key risk management methodologies from the other hand. The EISRM framework is developed to serve, in turn, as a base for the development of analytical models for enterprise information security readiness assessment and for economical analysis of the recommended protection measures. The proposed EISRM framework contributes in addressing the first research question, namely to identify what should a comprehensive enterprise information security risk management framework comprise of in order to integrate the current available enterprise information security risk management approaches.

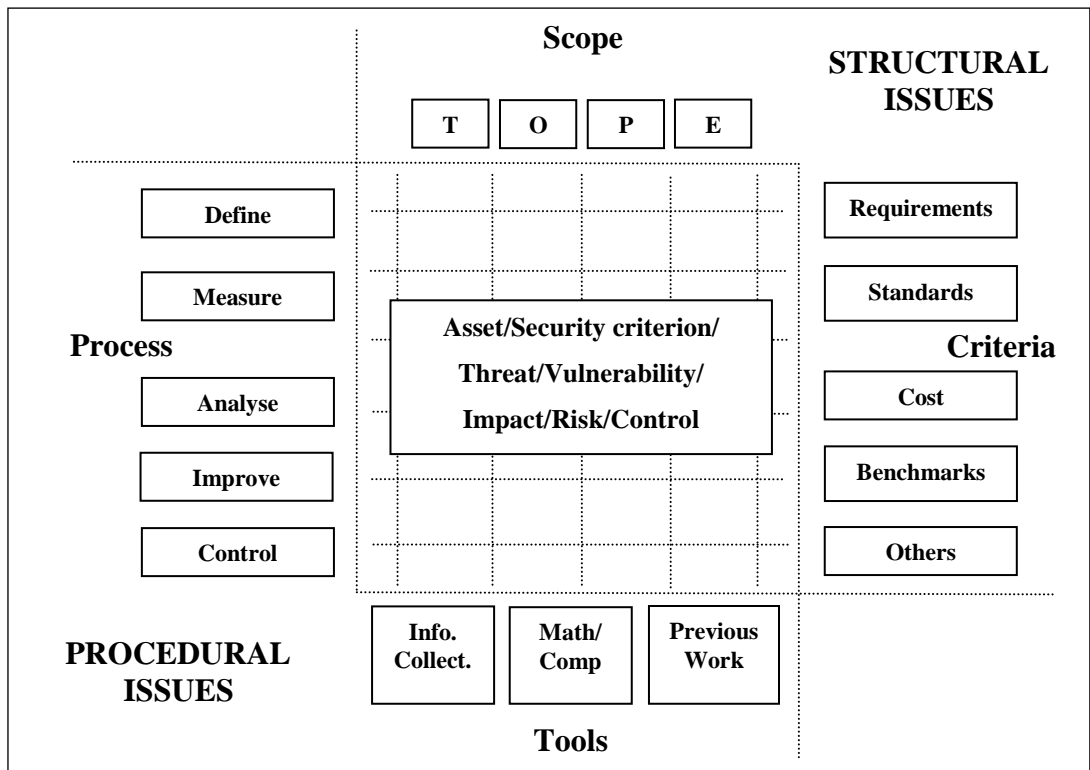
### **3.2 Proposed EISRM Framework**

The Merriam-Webster Dictionary (2010) defines a framework as a basic conceptual structure (as of ideas). In this respect, an information security risk

management framework can be seen as a structure upon which information security risk management elements, concepts and components are arranged for the purpose of minimising risks that may affect the information resources. Based on the investigation of different approaches for enterprise information security risk management which is discussed before in Chapter 2, a comprehensive EISRM framework is developed.

The proposed EISRM framework has two main parts: one part is concerned with its structural view, while the other is associated with its procedural view. The structural view has, in turn, two dimensions: scope and criteria, while the procedural view also has two other dimensions: process and tools. The framework is described in the following in terms of these four dimensions.

- The “**scope**” dimension of the framework is based on the four TOPE domains of technology, organisation, people and environment with different levels of detail associated with each domain.
- The management “**criteria**” dimension of the framework is considered to be associated with the controls of the ISO family of information security standards. However, other requirements including: standards, cost-benefit and benchmarks can also be considered.
- The “**process**” dimension of the framework adopts the five cyclic phases of the six-sigma model DMAIC: define, measure, analyse, improve and control with identified input and output issues at each phase.
- The support “**tools**” dimension of the framework includes the various means that would promote the work including: survey tools, mathematical models, computer tools and considering previous work.



**Figure 3-1 The structure of the proposed EISRM framework**

The research methodology in the choice of these four dimensions was based on the extensive literature review of Chapter 2 and on the knowledge acquisition techniques, as will be discussed later in Chapter 4. Figure 3-1 illustrates the structure of the proposed framework. Further explanations of both of its structural and procedural issues are given in the following sections.

### **3.2.1 EISRM Structural Issues**

The structural issues of the proposed EISRM framework are described here in terms of its two dimensions: the TOPE based scope and the management criteria.

#### **3.2.1.1 The TOPE Concept**

The emphasis upon technical issues in studying information system security risk management is prevailing in most of the reviewed risk management methodologies. Whilst technology is a necessary concern, it is not the only

factor requiring recognition. One of the main requirements of the proposed EISRM framework, as stated before in Chapter 2, is to extend the general focus on technical issues of most of the reviewed risk management methods to be more comprehensive. The comprehensive view in dealing with information security risk management means that organisational concerns, human factors and environmental effects also directly and indirectly affect the security risk management results (Beznosove and Beznosova 2007; Kraemer et al. 2009; Werlinger et al. 2009). In the following, the main technological, organisational, people and environmental issues that should be considered in studying enterprise's information security risk management issues will be discussed.

### **Technology Domain**

This domain involves the technical and physical mechanisms that are implemented to secure enterprises' IT environment. All aspects related to the technological issues of information security are grouped together under this domain. The technical considerations include, for instance, telecommunication facilities, electronic equipment and devices and computer hardware and software. Security related to technical issues would include protection of stored and transmitted data by for instance encryption, firewalls, intrusion detection systems, access restriction devices and authentication devices.

### **Organisation Domain**

This domain includes considerations of the organisational aspects that are affecting the information security at the strategic, management and operational levels. All considerations of organisational nature are included together under this domain. The important issues at the strategic level include: structure and management style, organisational culture and policies. Issues at the



management level include aspects that are deployed to ensure the effective management of information security. For instance, asset management, information security management and information security incident management are included in this domain. Issues at the operational level include job design, workflow and any practices associated with general operations. In addition, awareness of security responsibilities of enterprise members at all levels, the security programme itself (i.e. policies, planning, education, etc...) and the audit function of ongoing control and management are considered as important organisational issues.

### **People Domain**

The human considerations are concerned with the behavioural issues and consider the different perspectives of the people involved. All aspects that are related to the people involvement in information security are grouped together under this domain. People who are stakeholders of a given information system include: owners of the system, people who use the system directly, people who rely on the system and people who design, build and maintain the system (Theoharidou et al. 2005). For instance, processes like education and training, as well as concepts like trust are associated with this domain. The social environment within the system operates also is an important consideration. The social, cultural and religious elements influence the attitude of a person towards the protection of information resources.

### **Environment Domain**

The natural and management environment in which the concerned enterprise and its IT systems operate are an important consideration. All aspects relating to the environmental effects on information security are grouped together

under this domain. This includes weather conditions and man-made environmental issues, on one hand and professional and cultural behaviour management rules and legal aspects, on the other. In addition, physical security and internal as well as external compliance with information security standards are considered under this domain.

### 3.2.1.2 EISRM Scope Dimension

The TOPE-based scope of the framework would enable the mapping of the basic elements of the enterprise, associated with IT, to the domains of technology, organisation, people and environment. The basic elements of an enterprise as identified previously in Chapter 2 with regards to the proposed EISRM framework, are considered to be its: assets, security challenges (threats and vulnerabilities) and security controls. These are addressed in the following according to the TOPE-based scope.

**Table 3-1 Enterprise assets considered by different references mapped on the TOPE domains (ISO/IEC TR 13335 1998; CRAMM 2001; BSI 2004)**

TOPE	Assets Main Groups	
	Tangible ( <i>examples</i> )	Intangible
<b>Technology</b>	Information: ( <i>Data files</i> ). IT Services: ( <i>Messaging-active directory</i> ). Software: System( <i>Solaris</i> ), Application ( <i>Oracle</i> ), Utilities ( <i>management tools</i> ). Hardware: Hosts ( <i>Servers</i> ) other ( <i>Printers</i> ). Communication: Network ( <i>Routers</i> ), ( <i>Cables</i> ).	-Goodwill -Service to clients -Public confidence -Public trust -Competitive advantage -Image of the organisation -Reputation -Trust in services -Employee moral -Productivity -Loyalty -Ethics
<b>Organisation</b>	Information: ( <i>Policy document-Research</i> ). Documents: ( <i>Management commitment</i> ). Agreements: ( <i>Confidentiality-third party</i> ). Other: ( <i>User manuals-training material</i> ).	
<b>People</b>	IT staff: ( <i>IT security manager</i> ). Employee: ( <i>Senior management</i> ). Users: ( <i>Inside / Outside</i> ). Contractors: ( <i>Consultants</i> ). Owners: ( <i>Stakeholders</i> ).	
<b>Environment</b>	Services: ( <i>Heating-lighting-power-AC</i> ). Equipment: ( <i>Desks-Fax machines</i> ). Physical: ( <i>infrastructure</i> ) ( <i>IT rooms-facilities</i> ).	

## Assets

One of the main clauses of the ISO/IEC 27002 standard is the asset management, which has two objectives: responsibility of assets and information classification. Asset is defined by ISO as "*anything that has value to the organisation*" (ISO/IEC 27002 2005, p.1). This definition brings up the consideration of two types of assets: tangible and intangible. Table 3-1 maps the tangible assets considered by different references presented in Chapter 2 to the four TOPE domains. This is a high-level mapping that can be refined into sub-levels for further details. Table 3-1 also considers intangible assets that are associated with multiple domains.

**Table 3-2 Threats and vulnerabilities considered by different references mapped on the TOPE domains (ISO/IEC TR 13335 1998; CRAMM 2001; BSI 2004)**

TOPE	Challenges Main Groups	
	Threats (examples)	Vulnerabilities (examples)
<b>Technology</b>	Malicious codes: ( <i>Viruses</i> ) D Software: ( <i>Failures</i> ) D&A Hardware: ( <i>Failures</i> ) D&A Communication: ( <i>Infiltration</i> )D	Software: ( <i>Configuration errors</i> ) Hardware: ( <i>Missing patches</i> ) Communication: ( <i>Unnecessary protocol</i> ) Media: ( <i>Electrical interference</i> )
<b>Organisation</b>	Policy: ( <i>Inadequate</i> ) Agreement: ( <i>Inadequate</i> ) D Information: ( <i>Errors</i> ) D Planning: ( <i>Problems</i> ) D Procedures: ( <i>Incorrect</i> ) D&A	Document: ( <i>No care at disposal</i> ) Procedures: ( <i>Violations not reported</i> )
<b>People</b>	Employee: ( <i>Sabotage</i> ) D Users: ( <i>Inside/Outside/Theft</i> ) D Crackers: ( <i>Malicious hacking</i> ) D	Employee: ( <i>Insufficient training</i> )
<b>Environment</b>	Industrial: ( <i>Espionage</i> )D Natural: ( <i>Earthquake</i> )A Services: ( <i>Power outage</i> ) D&A	Natural: ( <i>Facility in flood zone</i> ) Physical: ( <i>Unlocked doors</i> )

## Challenges

Challenges can be viewed as negative coins of two faces: threats and vulnerabilities. ISO defines threat as "*a potential cause of an unwanted incident, which may result in harm to a system or organisation*"; and it defines vulnerability as "*a weakness of an asset or group of assets that can be exploited by one or more threats*" (ISO/IEC 27002 2005, pp.5). Table 3-2 maps

threats and vulnerabilities considered by different references presented in Chapter 2 to the four TOPE domains. With regards to threats, Table 3-2 marks them as either: deliberate (D), accidental (A) or both (D&A).

### Controls

ISO defines controls as “*means of managing risk including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management or legal nature*” (ISO/IEC 27002 2005, p.1). Table 3-3 maps ISO/IEC 27002 information security clauses, objectives and controls to the four TOPE domains. The methodology in mapping the controls of ISO/IEC 27002 information security management standard to the TOPE domains will be discussed later in Chapter 4.

**Table 3-3 ISO information security clauses, objectives and controls mapped on the TOPE domains (ISO/IEC 27002 2005)**

TOPE		ISO/IEC 27002:2005 Basic Parts			
		Part No.	Clause	No. of Objectives	No. of Controls
T	Technology	10	Communications and Operations Management	10	32
		11	Access Control	7	25
		12	Information Systems Acquisition, Development and Maintenance	6	16
O	Organisation	5	Security Policy	1	2
		6	Organisation of Information Security	2	11
		7	Asset Management	2	5
		13	Information Security Incident Management	2	5
		14	Business Continuity Management	1	5
P	People	8	Human Resources Security	3	9
E	Environment	9	Physical and Environmental Security	2	13
		15	Compliance	3	10
<b>Total ISO/IEC 27002 objectives and controls</b>				<b>39</b>	<b>133</b>

### 3.2.1.3 EISRM Criteria Dimension

The management criteria dimension appears at all domains of the TOPE-scope of the proposed EISRM framework, as shown in Figure 3-1, to illustrate

that it should be considered across all TOPE domains. The criteria could specify the required security controls on the various TOPE domains relative to cost-benefit analysis. For the controls considered, it could provide benchmarks to their acceptable levels. In general, the management criteria would be associated with the policy and business requirements of the concerned enterprise.

### **3.2.2 EISRM Procedural Issues**

The procedural issues of the proposed EISRM framework are described here in terms of its two dimensions: the six-sigma based process and the support tools. In the following section, background on the main risk management components as seen by the ISO/IEC 27000 (2009) standard that should be considered by any risk management methodology will be presented.

#### **3.2.2.1 Risk Management Main Components**

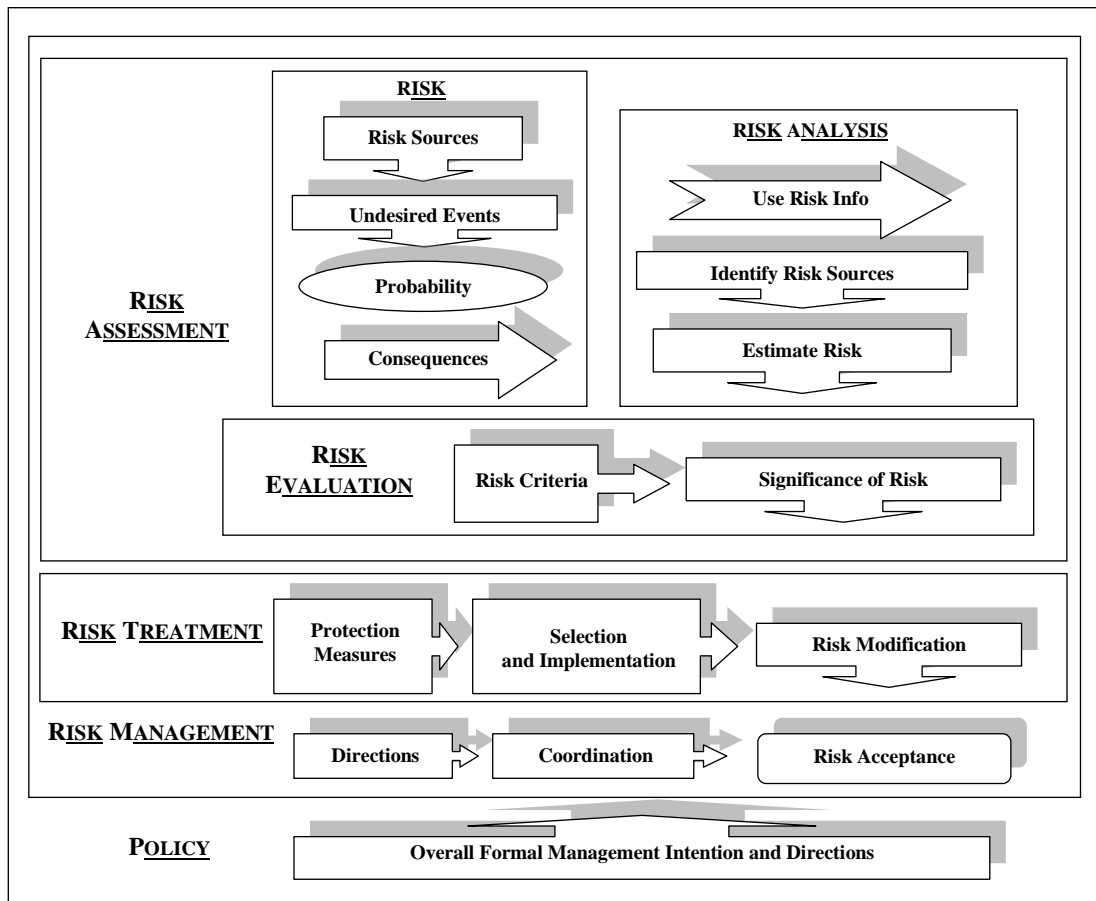
For better understanding of the whole risk management process, it is important to analyse the various definitions that appeared in literature for its associated components. Hoo (2000) explains the difference between risk assessment and risk management. Risk assessment is the process of identifying, characterising and understanding risk; that is studying, analysing and describing the set of outcomes and likelihoods for a given endeavour. On the other hand, risk management is a policy process where alternative strategies for dealing with risk are weighted and decisions about acceptable risks are made.

According to the NIST SP 800-30 standard, risk assessment is synonymous with risk analysis and is considered as part of risk management that entails identifying risks to system security, ascertaining the probability of occurrence, evaluating the resulting impact then suggesting safeguards that would reduce this impact to an acceptable level. The standard also defines risk management

as the process of identifying, controlling and mitigating information system related risks and encompasses risk assessment, cost-benefit analysis and the selection, implementation, test and evaluation of safeguards (NIST SP 800-30 2002, E-2). The AS/NZS 4360 risk management standard has its own definitions for these risk management components, which is mainly based on the ISO/IEC 51 guide (1999) and the ISO/IEC 73 guide (2002).

From the previous discussion, there are many different definitions for risk management components, in one context, risk analysis is considered as part of risk assessment, and in other context, risk analysis is interchangeable with risk assessment. The problem is the lack of precise definitions of the risk management terminologies (Hogganvik and Stolen 2005). Consequently, in order to develop common understanding among enterprises, ISO in 2009 published the ISO/IEC 27000 overview and vocabulary standard to provide generic definitions for the risk management components. The core of the ISO/IEC 27000 standard is a list of definitions on risk management components including risk management tasks as follows:

- **Risk:** the combination of the probability of an event and its consequence.
- **Risk analysis:** the systematic use of information to identify sources and to estimate risk.
- **Risk evaluation:** the process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
- **Risk assessment:** the overall process of risk analysis and risk evaluation.



**Figure 3-2 An illustrative view of ISO risk management components**

- **Risk treatment:** the process of selection and implementation of measures to modify risk.
- **Risk management:** the coordinated activities to direct and control an organisation with regards to risk.
- **Risk policy:** the overall formal risk management intentions and directions.

Figure 3-2 provides an integrated view of the above ISO components illustrating their inter-relationships. According to the ISO standard, the main objective of the risk analysis process is to estimate risks from potential events, with a view to reduce these risks to an acceptable level. On the other hand, the objective of risk assessment is to comprehend risks of particular environment and to evaluate these risks according to defined criteria. The risk treatment

objective is to propose a plan to mitigate these risks to an acceptable level. The objective of risk management is to use one or more methods to identify and evaluate new risks, then select risk mitigation strategy and also monitor, review and communicate information about existing risks so as to optimise the performance of the whole enterprise information security risk management programme.

The introduction of the above definitions of risk management related components and concepts will help to provide unified terminology between different information security risk management approaches, and therefore will help to go towards a common understanding of the EISRM framework and its associated models presented in this thesis .

#### **3.2.2.2 EISRM Process Dimension**

The adoption of the six-sigma five phase cyclic process DMAIC by the proposed EISRM framework will be explained in the following sections. This is enhanced further by giving the function of each phase in the context of information security risk management process, as shown in Figure 3-3 and summarised in Table 3-5.

#### **The Six-Sigma Model**

Six-Sigma is a method for designing an efficient business that runs as error-free as possible. The six-sigma was invented by Motorola in the late 1980s. The phases of the six-sigma cyclic process is abbreviated by: DMAIC, that is: define, measure, analyse, improve and control (Pyzdek 2003). The process is presented in Table 3-4. A mapping between the key risk management processes and the six-sigma cyclic phases had been presented before in Table 2-13. This mapping shows the possibility of adopting the DMAIC process in the proposed EISRM framework.



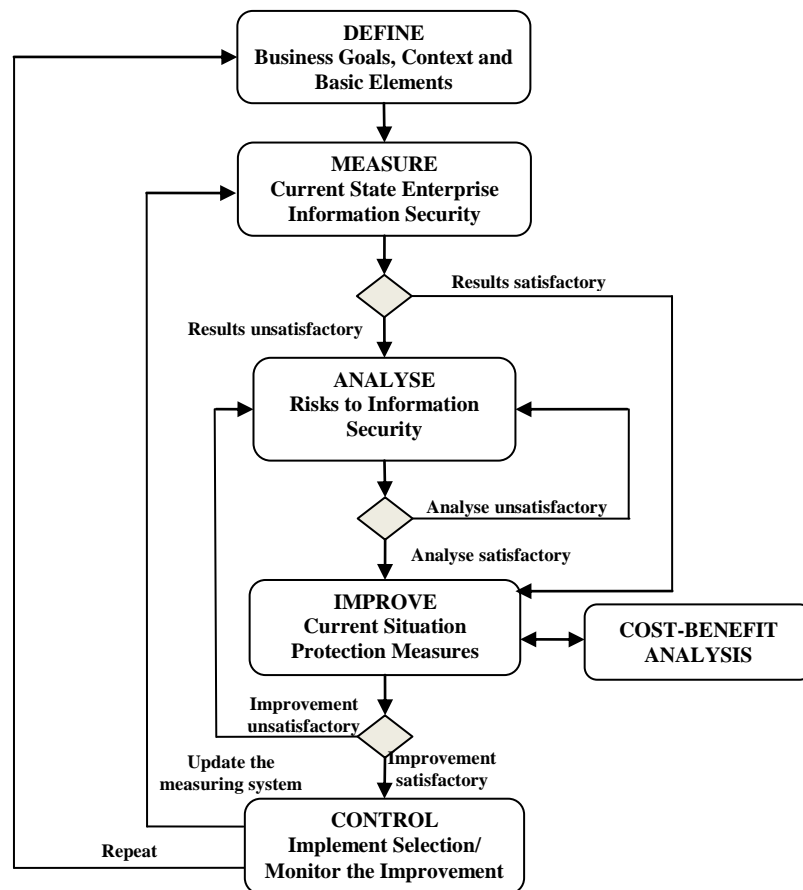
**Table 3-4 DMAIC process (Pyzdek 2003)**

<b>Phase</b>		<b>Explanation</b>
<b>1</b>	<b>Define (D) opportunity</b>	Encapsulate the problem to determine what needs to be improved. In this phase, a problem statement, a goal statement, constraints assumptions and a project plan is documented.
<b>2</b>	<b>Measure (M) performance</b>	Compare the current state against the wanted state. Going deeper into the problem and trying to answer why it exist and this will bring a more detailed understanding of the problem.
<b>3</b>	<b>Analyse (A) opportunity</b>	By analysing the information that has been acquired from the previous phase, the aim is to confirm why the problems exist.
<b>4</b>	<b>Improve (I) performance</b>	Based on all the earlier phases, a list of actions and methods are documented. If there are different ways to attack the problem, an evaluation is made so that the best of the alternative is chosen and implemented.
<b>5</b>	<b>Control (C) performance</b>	The problem area that has been discovered in the define-phase is being monitored to ensure that it dose not reoccur.

### **The Define Phase**

The main objective of this phase is: to define the main business goals; to identify the context of the enterprise under consideration and to specify the basic elements of the risk management process. The process starts with a study of the enterprise's context and identification of its main assets and basic elements. The enterprise and its environment are described, focusing on the sensitive activities that are related to information security, according to the TOPE scope. The security needs in terms of confidentiality, integrity and availability properties of the assets are then defined. This phase would use the output of a previous cycle of the DMAIC process or start a new process, depending on the case considered. This phase has a number of steps as follows:

- Identify the main business goals;
- establish the context of the reviewed area;
- map the existing basic elements of the enterprise (assets, threats, vulnerabilities and controls) to the TOPE domains;
- specify the owner of each asset;



**Figure 3-3 The proposed process for the EISRM framework**

- specify the location of each asset;
- specify the source of the threat; and
- give security requirements.

The output of this phase would be a TOPE view of the current state of the basic elements of information security in the considered enterprise.

### **The Measure Phase**

The main objective of this phase is to assess the basic elements of the considered enterprise according to specified criteria. This phase is mainly devoted for the assessment of the enterprise current state information security.

The assessment will be conducted against the ISO/IEC 27002 standard with security readiness indicators. These indicators will be assigned and presented later in Chapter 4. The assessment indicators should indicate how far the

information security practices in the concerned enterprise from the ISO/IEC 27002 standard and identify areas that need further improvement.

This phase will receive the output of the "define" phase and add the following information to each element:

- Assessment of the current value of assets;
- assessment of the current state of threats;
- assessment of the current state of vulnerabilities; and
- assessment of the current state of controls.

The output of this phase would be a TOPE view of the critical assets associated with the assessment of threats and vulnerabilities they are facing, and with the security controls used. The output of this phase will help the enterprise in the first decision as shown in Figure 3-3 regarding the need for moving to the next step of running enterprise wide risk analysis exercise or improving the current state according to the ISO/IEC 27002 standard. The enterprise will also have a measurement system that could be used in the future for monitoring and improving its information security practices.

### **The Analyse Phase**

The main objective of this phase is to analyse the gap between the current state and the required state of protection from threats. This will be based on the output of the "measure" phase, on one hand, and on the required "criteria" on the other hand. In this respect, the analyse phase is devoted for running a risk analysis exercise for the considered enterprise based on the unsatisfaction of its performance in accordance to its security needs. The basic steps of this phase are as follows:

- Development of an analytical model for gap analysis;
- using the model for evaluating current state versus required state; and

- determination of the security gap between the current state and the required state.

The output of this phase is a TOPE view of the gap between security requirements and the current state of security, considering all critical assets. In addition, the enterprise will then move to the second decision, as shown in Figure 3-3, of repeating the analysis phase for better results or moving to the next step of improving the current state information security.

### **The Improve Phase**

The objective of this phase is to decide the best risk mitigation strategy. The cost-benefit model that will be developed later in Chapter 6 could be used in this phase to select the most economical solution from the identified subset of the ISO/IEC 27002 protection controls. This phase considers the security state and the required state. It has the following main steps:

- Development of directions to close the security gap and achieve the required improvement; and
- designing an action plan that follows the directions.

The output of this phase is a TOPE view of an action plan of what should be done to close the gap and achieve the required security improvement. This output will include a treatment plan with levels of risks and the suggested protection measures to mitigate the identified risk. The decision for the risk treatment can include avoiding, reducing, transferring or retaining risk. The output of this phase will help the enterprise also in the third decision, as shown in Figure 3-3, regarding the need for moving to the next step of running, controlling and monitoring the new implemented protection measures, or repeating both of the “analysis” and the “improve” phases according to unsatisfactory results.

**Table 3-5 The use of six-sigma five phase cyclic process DMAIC for EISRM**

6 Sigma	Explanation		Output
<b>Define</b>	<b>Business goal:</b> Identify the business objectives according to its stated goals (innovation, dynamic environment, competences etc...)		A TOPE view of the current state of the basic elements of information security in the considered enterprise.
	<b>Objective:</b> Specify current state enterprise information security		
	<b>Input:</b> Collect information about enterprise basic elements.		
	Assets	tangible/intangible/owner/location	
	Threats	deliberate/accidental	
	Vulnerabilities	technical/organisational	
	Controls	existing/planned	
<b>Measure</b>	<b>Objective:</b> Assess the current state information security.		A TOPE view of the critical assets, associated with the assessment of the threats and vulnerabilities they are facing, and with the security controls used.
	<b>Input:</b> Define stage outputs/expert or owner view		
	Assets	valuation (direct/indirect)	
	Threats/assets	possible damage	
	Vulnerabilities / assets	weaknesses in the security measures	
	Controls / assets	TOPE/ISO based evaluation approach for control analysis (Saleh et al. 2007)	
<b>Analyse</b>	<b>Objective:</b> Find the gap between the current state and the required state of protection.		A TOPE view of the gap between security requirements and the current state of security, considering all critical assets.
	<b>Input:</b> Assessment of the current state from the "measure" phase; and the "required security protection criteria" of the enterprise concerned.		
	Model	development of an analytical model for gap analysis	
	Evaluation	using the model to evaluate the current state of security versus the required one.	
	Gap	determination of the security gap that needs to be closed, so that the required improvement is achieved	
<b>Improve</b>	<b>Objective:</b> Specify required improvements to close the gap between the current state and required state.		A TOPE view of an action plan of what should be done to close the gap and achieve the required security.
	<b>Input:</b> Required state and current state		
	Directions	development of directions to close the security gap and achieve the required improvement	
	Plan	designing an action plan that follows the directions	
<b>Control</b>	<b>Objective:</b> Implement improvement, monitor and evaluate; then repeat the whole process.		Implementation of the plan, operation, performance, understanding and process activation
	<b>Input:</b> Action plan for improvement		
	Implementing	the action plan for improvement	
	Monitoring	the changing state	
	Documentation	documenting the work	
	Re-initiating	The DMAIC process	

## **The Control Phase**

The objective of this phase is to attest that the risks are properly identified and the selected mitigation strategy is adequate. This phase has feedback to the “measure” phase by the new applied protection measures to be included in the information security assessment model. This phase considers the improvement plan and performs the following main steps:

- Implementation of the mitigation plan;
- monitoring the changing state;
- documenting the work; and
- re-initiating the DMAIC process.

The output of this phase is an improved enterprise’s security practices, in addition to going into another cycle for responding to new requirements and changes.

The above process is iterative and should be performed by enterprises many times until reaching an acceptable level for all risks, taking into account new risks that may arise during the process. The decision-makers and the stakeholders should be informed throughout the process about the risk management activities. This will be achieved by the parallel risk communication process and will be monitored by the illustration graphs of the information security assessment model. Table 3-5 illustrates how the process can be applied for information security risk management considering basic steps, input and output of each phase.

### **3.2.2.3 EISRM Tools Dimension**

The proposed framework considers that "support tools" would be required for the execution of the various DMAIC phases. Such tools have also been considered by previous methods, as given in Chapter 2. The tools would

include, but are not limited to, information collection and survey management tools, modelling and mathematical analysis, computational methods and software packages.

In the following section, an example is presented to illustrate the benefits that can be obtained from applying the above EISRM framework in identifying security challenges to the business goals and in showing how these goals can be badly affected as a result of the undefined security challenges to enterprise information resources.

### **3.2.3 Using EISRM Framework**

Each enterprise has its own unique business objectives. These objectives often change over time to reflect the new requirements of the business. For instance, an enterprise in its recognition that wireless and mobile technology have become increasingly critical enablers of innovation, operational cost and service delivery in major applications, would like to rely on business infrastructure with robust wireless mobility services to improve the efficiency of the communication between the different employees. As a result, the decision is taken to provide state-of-the-art mobile technology to the employees. Accordingly, it is agreed that a wireless network access point should be deployed to allow all employees to have remote access to enterprise IT resources.

The scenario presented above is an example that needs investigation tools to provide a reasonable decision that from one hand guarantee the protection of the enterprise information resources and from the other hand satisfies the business objectives. In this respect the proposed EISRM framework presented

above is suggested to conduct the required investigation to assess risks that may affect enterprise information resources.

In the “**Define**” phase, the objective of the enterprise was to improve the quality of its working environment and to achieve an efficiency of its activities through the use of wireless technology. The basic elements of the enterprise are then identified using the TOPE view. This new technology naturally involves security concerns. The information that each employee will have access must respect confidentiality. The integrity of sensitive information must be respected. The availability of the whole system is essential to have access to the information resources at all times. The “**Measure**” phase is then used to assess the current state information security according to the ISO/IEC 27002 standard. A list of missing controls according to the ISO/IEC 27002 information security management standard is identified which include: network controls; Information exchange policies and procedures; user authentication for external connections; segregation in networks; and mobile computing and communication. These controls and their associated protection measures satisfy the enterprise top management at this stage to achieve the stated business objectives. The “**Improve**” phase is then used to cost effectively select the most economical security protection measures that should be implemented to achieve the required level of information security. The “**Control**” phase will be used to monitor and control the implemented security protection measures and to assess their effective use.

The business, economical and operational benefits that the enterprise may have could be that the enterprise sees itself as dynamic, innovative and moving with latest technology. The decision to introduce wireless access to all employees could be a result from the belief that sales and profits would be



improved through better customer service in more remote locations. The failure to implement the required protection measures as a result of running the proposed EISRM framework could have a profound impact on the profit of the enterprise. Confidential information might be disclosed to unauthorised people, the availability of the IT systems could be affected by inside and outside attackers and compliance with legal and regulatory regulations could be lost.

### **3.3 The Information Security Policy**

As mentioned before, in Chapter 2, ISO/IEC 27002 emphasises the need for a policy document for information security management. The information security policy is used mainly to provide employees with a clear understanding of management's direction and support for information security as stated by the ISO/IEC 27002 standard. This will influence the employee's decision, action and behaviour in dealing with the business assets and in turn in achieving the business main goals. The six-sigma based approach is suggested by the researcher as a tool for the development, implementation and continuous improvement of the enterprise information security policy based on the TOPE view of ISO/IEC 27002 standard. The information security policy document is addressed, emphasising its structure and its continuous improvement. The information security policy document is one of the early requirements of ISO/IEC 27002, and it has priority when starting to manage information security inside any environment or business (Fulford and Doherty 2003).

#### **3.3.1 Information Security Policy Process**

The phases of the six-sigma cyclic process explained above are used also for the development of the information security policy. The process is briefly described in the following:

**Table 3-6 Six-sigma based cyclic process for the use of ISO/IEC 27002: 2005**

Six Sigma Process			Application of ISO/IEC 27002: 2005
<b>D</b>	<b>Define</b>	<b>Goals: requirements</b>	Application of international security management standard: ISO 27002: 2005 (TOPE view), with continuous improvement.
		<b>Reasons: explanation</b>	For world class information security quality and adaptability.
		<b>Case: application specific issues</b>	Find: relevant legal issues, business and enterprise requirements, internal and external use.
		<b>Indicators: measurability</b>	Identify relevant evaluation indicators, based on ISO/IEC 27002: 2005 TOPE view and on case specific issues.
		<b>Policy document</b>	Construct policy document base (see Table 3-8)
<b>M</b>	<b>Measure</b>	<b>Current state: indicators</b>	Evaluate current state information security management using indicators (see Chapter 4,5).
		<b>Policy document</b>	Update policy document (see Table 3-8).
<b>A</b>	<b>Analyse</b>	<b>Evaluation</b>	Analyse current state identifying its strengths, weaknesses, opportunities and threats considering risks and protection measures using resulted indicators (see Chapter 4).
		<b>Risk assessment / management</b>	
		<b>Policy document</b>	Update policy document (see Table 3-8).
<b>I</b>	<b>Improve</b>	<b>Design: for improvement (new state)</b>	Design how the current state can be improved towards achieving the requirements using the results of the analysis given above.
		<b>Implement: new state</b>	Put the new state into practical use.
		<b>Policy document</b>	Update policy document (see Table 3-8).
<b>C</b>	<b>Control</b>	<b>Monitor: new state</b>	Monitor and evaluate the new state that resulted in emphasising the achievements resulting from the improvements.
		<b>Evaluate: new state</b>	
		<b>Look ahead: progress cycle</b>	Look for continuous improvement repeating the process.
		<b>Policy document</b>	Update policy document (see Table 3-8).

- The “define” phase of the process involves stating or restating the goals, the reasons behind the goals, the case considered together with its specific requirements, the ISO/IEC 27002 TOPE view indicators and the basic structure of the policy document as will be discussed later.

- The “**measure**” phase involves using the indicators to investigate the current state of information security management in the enterprise considered and updating the policy document accordingly.
- The “**analyse**” phase includes the evaluation of the Strengths, Weaknesses, Opportunities and Threats (SWOT) of the current state, considering the risks and the protection measures and using the indicators. The policy document should also be updated.
- The “**improve**” phase responds to the “**analyse**” phase by providing new design state to improve information security management, and by giving the opportunity to implement the new state. Policy update is also needed here.
- The “**control**” phase is concerned with the culture of continuous improvement. It involves monitoring and evaluating the new state, updating the policy document and looking ahead to repeating DMAIC six-sigma process.

Table 3-6 illustrates how the process can be applied using ISO/IEC 27002 TOPE view for information security management.

### **3.3.2 The Policy Document Structure**

A TOPE view structure for the proposed information security policy document is introduced in Table 3-7. The table suggests building the progress of continuous improvement into the practical use of the document. In this respect, three versions of the documents are recommended: a version dealing with the required new improved state; a version dealing with the current state; and a version dealing with the previous state. The phases of DMAIC six-sigma process consider the development and continuous updates of the document.

**Table 3-7 Information security policy document: structure and progress**

	Identification	Cover	Summary	Table of Content
<b>Document Structure</b>	Main parts	An integrated view of goals and directions: Laws & regulations / Business & organisation specific issues / Intranet, Extranet & Internet / Continuous improvement		
		Technology	Organisation	People
	Evaluation	SWOT: Strengths, Weaknesses, Opportunities (for improvements), Threats (improvement obstacles)		
<b>Progress Tools</b>	Document Versions	Son: Required state	Father: Current state	Grandfather: Previous state

### 3.4 EISRM Work Team

As mentioned before in Chapter 2, the success of any risk management method stems from the expertise of people who apply the steps of the method. A well trained team from the enterprise itself which take the responsibility for the required work could achieve better results than outside expertise. Six-sigma recommends the formation of an effective work team, in order to perform the above DMAIC process successfully. The structure of the recommended work team is supposed to carry the ingredients of the successful work. This structure is proposed by the author and presented in Table 3-8 with regard to information security management and some explanations are introduced in the following:

- **Leadership** is associated with the top executive of the enterprise concerned, the Chief Executive Officer (CEO). The basis of this is that information security management affects the performance of the basic functions of any enterprise, and therefore it requires support from the top leader.
- **Championship** is associated with the top management of the enterprise, maybe with a Vice President (VP), but the role of the person here is to provide close follow-up of what needs to be done for information security management and its continuous improvement.

**Table 3-8 Six sigma team for the application of the ISO/IEC27002 standard**

<b>Level</b>	<b>Who</b>	<b>Role</b>
<b>Leadership</b>	Enterprise President / CEO: Chief Executive Officer	Support for better organisation performance due to better information security management.
<b>Champions / Sponsors</b>	Six sigma leader: usually with high position (e.g. VP: Vice President / CIO: Chief Information Officer)	Influential leader (at high position) providing close follow-up and support.
<b>Master black belt</b>	CISO: Chief Information Security Officer (Highest technical level).	Technical leader of six sigma information security management work.
<b>Black belt</b>	Technical IT staff.	Involved in the technical issues of the work under the supervision of the Master Black Belt.
<b>Green belt</b>	Staff using IT with technical capabilities.	Work with black belt staff to help achieving effective improvements.
<b>Staff level</b>	Staff using IT.	Cooperation.

- **Master black belt** is the technical manager of information security management. He should be experienced and well trained; similar in this respect to a top karate person.
- **Black belts** are the technical staff concerned with information security management.
- **Green belts** are selected from the IT users of the concerned enterprise to provide support to information security management.
- **Staff level** consists of the IT users who should co-operate and support information security management.

### **3.5 Summary**

The aim of this chapter was to develop a framework for enterprise's information security risk management. The proposed framework has two structural dimensions, and two procedural dimensions. From a structural viewpoint, the TOPE scope of the framework enables it to incorporate the wide range of issues associated with EISRM in a well structured manner, and the use of six-sigma DMAIC process allows it to accommodate the various

methods concerned with EISRM. In addition, the framework responds to the need of using a management criteria and permits various criterion to be taken into account, including ISO information security controls and considering pre-determined benchmarks. The framework also considers the support tools for performing the various phases efficiently; and in this respect it allows the use of different tools for this purpose. In addition, to support the developed EISRM framework, a methodology, based on the six-sigma principles, on how to apply the TOPE view of the standard to the evaluation and continuous improvement of enterprise information security policy document is presented. Finally, the structure of the proposed six-sigma based work team is presented in order to effectively perform the risk management process.

# **Chapter 4**

## **ENTERPRISE INFORMATION SECURITY ASSESSMENT MEASURES**

### **4.1 Introduction**

The ISO/IEC 27001 (2005) information security management standard requires enterprises to undertake regular reviews of the effectiveness of their information security management system. This process, according to ISO, should measure the effectiveness of the implemented information security controls to verify that the security requirements, according to the business objectives, have been met. In light of the above, ISO/IEC 27001 requirement and the main objective of the “measure” phase of the developed EISRM framework, this chapter focuses on the identification of a set of assessment measures that could be used in assessing enterprise information security readiness according to the recommended security controls of the ISO/IEC 27002 information security management standard. This chapter, therefore addresses partially the second research question stated in Chapter 1 which relates to the choice of the suitable security measures that could be used as an input to an analytical model for numerically assessing enterprise information security readiness.

### **4.2 Development of ISO Based Assessment Measures**

An information security measurement programme provides enterprises with a number of organisational and financial benefits. Major benefits include

increasing accountability for information security performance; improving effectiveness of information security activities; demonstrating compliance with laws, rules and regulations; and providing quantifiable inputs for resource allocation decisions (NIST SP 800-55 rev1 2008, pp.19). The ISO/IEC 27004 (2009) information security management – measurement standard summaries the main requirements that contribute to the success of information security measurement programme as follows:

- Management commitment supported by appropriate resources;
- existence of ISMS process and procedures;
- a repeatable process capable of capturing and reporting meaningful data to provide relevant trends over a period of time;
- quantifiable measures based on ISMS objectives; and
- easily obtainable data that can be used for measurement.

To fulfil the above stated requirements by NIST SP 800-55 and ISO/IEC 27004 standards towards the development of an effective information security assessment model, enterprises should first choose the most suitable assessment measures. The theory of measurement states that goodness of an assessment is specified in terms of validity and reliability (King et al. 1994). Good validity of the measure is often defined as the extent to which a measure accurately reflects the concept that it is intended to measure. On the other hand, good reliable measure is defined as the extent to which a measure yields consistent, stable and uniform results over repeated measurements of the same unit (Wang 2005).

Regarding the validity of the assessment, it is important that the measure really assess what is considered as information security concerns. Also, these



measures should be consistent with common conceptions from both academic and practitioners point of view, and be based on valid information security source. Regarding the reliability of the assessment, the measures should reflect objective rather than subjective view of the evaluated controls. Also, the selected measures should be operationalised with respect to aggregation of the assessment data. The former requirement is discussed in this chapter, and the later will be discussed in Chapter 5.

## **4.2.1 Knowledge Acquisition**

In searching for measures that represent information security domain, the researcher uses hybrid knowledge acquisition techniques. The preliminary analysis, text analysis and interview analysis knowledge acquisition techniques are used in this research in searching for a valid and reliable information security measures. These measures, in turn, will represent an input for the developed assessment model presented in Chapter 5.

### **4.2.1.1 Preliminary Analysis**

The preliminary literature survey was performed to obtain an overview of the problem and to determine potential categories that would be useful in classifying the various types of measures. The preliminary knowledge acquisition utilises text and interview analysis. The literature was searched for documented manuals for information security controls and for investigating the common characteristics of these controls. The data obtained in these two steps was used to identify the source of information security controls and to assign domains or categories for these controls to address the primary security measures that could be associated with any type of enterprise.

The first step in the preliminary analysis was based on a literature survey (Chapter 2), including three families of sources that fully support the research scope as follows:

- Standard risk management methods including: AS/NZS 4360, NIST SP 800-30 and ISO/IEC TR 13335-3 standards.
- Professional risk management methods including: CRAMM, OCTAVE, CORAS and EBIOS.
- Information security management standards including: SOGP and ISO/IEC 27002 standards.

The ISO/IEC 27002 code of practice for information security management standard was chosen as a base for the development of the assessment measures. Reasons of interest in choosing this standard are summarised as follows:

- The standard is accepted internationally as code of practice for information security management standard.
- It contains most of the required controls for practically representing the information security concerns, as discussed before in Chapter 2 and shown in Table 2-11.
- The standard is referenced in most of the key information security risk management methods, and in other standards.
- The design of the standard eases the alignment of its contents with the TOPE (Technology, Organisation, People and Environment) view presented in this thesis, and consequently facilitates the process of elicitation of the information security measures.

In this respect, the proposed enterprise information security assessment model developed in Chapter 5 will utilise the ISO/IEC 27002 code of practice for information security management standard, as a base for the development of its information security assessment measures.

The second step of the preliminary analysis was devoted for developing a modular approach for classifying the information security controls of the ISO/IEC 27002 standard along categorical lines that represent technology, organisation, people and environment. Table 4-1 shows the suggested alignment between the TOPE domains and the ISO/IEC 27002 main clauses.

**Table 4-1 TOPE view of ISO/IEC 27002 main clauses**

Domain		ISO/IEC 27002 Main Parts	
		Part No.	Clause
T	Technology	10	Communications and Operations Management
		11	Access Control
		12	Information Systems Acquisition, Development and Maintenance
O	Organisation	5	Security Policy
		6	Organisation of Information Security
		7	Asset Management
		13	Information Security Incident Management
		14	Business Continuity Management
P	People	8	Human Resources Security
E	Environment	9	Physical and Environmental Security
		15	Compliance

This alignment was validated through experts view. The validation was carried out by practitioners, academic researchers and standardisation experts. Five practitioners (IT managers from the participated enterprises), five academic researchers (Professors working at King Saud University) and three standardisation experts (Researchers from King Abdulaziz City of Science and Technology) were involved in this review. The evaluation was based on open discussions about the TOPE domains, and the most suitably aligned ISO/IEC 27002 clause to each of these domains. All of their comments were analysed and discussed to reach the optimum alignment which appeared in Table 4-1.

#### **4.2.1.2 Text Analysis**

The knowledge acquisition continue with an in-depth text analysis of the ISO/IEC 27002 clauses, objectives and controls to identify the most suitable information security assessment measures associated with each ISO security control. The results of this analysis yielded extensive security measures (682 measures). Considering the number of controls and measures to be aligned through the TOPE domains, it is not realistic to describe in a detailed manner the alignment and iteration performed. An example to show how the process of choosing and refining the security measures of the ISO/IEC 27002 information security policy clause will be presented in the next section.

#### **4.2.1.3 Security Policy Measures**

The information security policy objective of ISO/IEC 27002 is stated as follows: *“to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations”*. The required response, to this main objective, is expressed in terms of the following two controls (ISO 2005).

- *“An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties”*.
- *“The information security policy should be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness”*.

The above strategic objective and associated controls indicate that the information security policy of organisations should take the following main factors into consideration.

- “Relevant laws and regulations”, so that no violation of the “legal infrastructure” of both the organisation concerned, and its work environment, can take place.
- “Business requirements”, so that the protection measures associated with business in general, and with the target business in particular, are taken into account.
- “Employees of the organisation”, so that the Intranet activities of the organisation are protected.

**Table 4-2 Assessment measures considering the ISO/IEC 27002 security objective of "information security policy document" with two controls**

ISO Objective		Information security policy document “ <i>to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations</i> ”	
ISO Controls		Security Measures	
Control 1	<b><i>An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties</i></b>	1	A clear definition of information security
		2	The policy document contain statement of management intent, in supporting the goals and principles of information security
		3	The policy document contains a framework for setting control objectives
		4	The policy document contains a brief explanation of the security policies, principles and standards
		5	The policy document contains definition of general and specific responsibilities for information security management
Control 2	<b><i>The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.</i></b>	6	The policy document contains references to documentation, which may support the policy (e.g. more detailed security policies).
		7	The policy document is reviewed at planned intervals to check its suitability
		8	The policy document is reviewed at planned intervals to check its adequacy
		9	The policy document is reviewed at planned intervals to check its effectiveness
		10	The policy document is reviewed if significant changes occur to check its suitability
		11	The policy document is reviewed if significant changes occur to check its adequacy
		12	The policy document is reviewed if significant changes occur to check its effectiveness

- “External parties”, so that Extranet and Internet activities of the organisation are also protected.
- “Continuous attention”, so that response to change is achieved, and so that the required protection is sustained.

Table 4-2 presents the elected twelve primary assessment measures associated with the security objective of the information security policy document. These measures will be refined later in the interview analysis knowledge acquisition step.

#### **4.2.1.4 Interview Analysis**

The main purpose of this step was to refine the number of the measures revealed from the text analysis step and to give the importance weight for each of these measures and its associated controls, objectives and clauses. The experts in this step of the knowledge acquisition analysis were selected based upon their expertise in concerned domain and years of experience. A total of 4 experts for each TOPE domain were chosen. The domain expert selection was devoted to obtain individuals with well understanding of aspects of each of the four domains identified in the preliminary analysis. The output of this step reveals 283 most important security measures out of the 682 security measures that represent effectively the 133 ISO/IEC 27002 security controls. The steps used to refine the number of the extracted measures of the above text analysis step and to assign weights for each of the 283 measures, 133 controls, 39 objectives, 11 clauses and 4 TOPE domains are as follows:

- Present the expert with a list of measures for each of the 133 ISO controls and let the expert express his/her perception of the importance of these measures to each of the ISO controls using the scale in Table

4-3. In this study, the multiple-item Likert scales are used to measure the variables because it is an appropriate interval scale that measures behavioural variables. There are no general rules in deciding on the type and number of scale point. It could be odd or even numbers and it normally ranges between five and ten categories (Parasurman 1986).

**Table 4-3 Reference table for the importance values of the measures**

<b>Grade</b>	<b>Explanation</b>
<b>Very High</b>	The measure is directly associated with the conformance of the ISO/IEC 27002. The absence of the measure is directly associated with a sever vulnerability.
<b>High</b>	The measure is somewhat associated with the conformance of ISO/IEC 27002. The absence of the measure is directly associated with an important vulnerability.
<b>Moderate</b>	The measure is a moderate associated with the conformance of the ISO/IEC 27002. The absence of the control is directly associated with an insignificant vulnerability.
<b>Low</b>	The measure is a little associated with the conformance of the ISO/IEC 27002. The absence of the control is directly associated with an insignificant vulnerability.
<b>Not at all</b>	The measure has no importance associated with the conformance of the ISO/IEC 27002.

- For each control, a matrix of “ $n*m$ ” is extracted which “ $n$ ” represents the number of experts and  $m$  represents the number of measures.
- The calculation of the aggregated weight for each measure is performed using the average for each measure.

The output of this step is a refined list of these measures appeared in Table 4-4, and the details appeared in Appendix A. In addition, the calculated weights for 283 security measures, 133 controls, 39 objectives, 11 clauses and 4 TOPE domains are also appeared in Appendix A.

The purpose of using hybrid of knowledge acquisition methodologies was to ensure thorough coverage of the knowledge necessary to identify the information security measures. The details of the mapping process between

the TOPE domains and the ISO/IEC 27002 standard will be introduced in the following sections.

**Table 4-4 TOPE view of ISO/IEC 27002 main security clauses, objectives, controls and assessment measures**

Domain	ISO/IEC 27002 Basic Parts				
	Part No.	Clause	No. of Objectives	No. of Controls	No of Measures
<b>Technology (T)</b>	10	Communications and Operations Management	10	32	65
	11	Access Control	7	25	41
	12	Information Systems Acquisition, Development and Maintenance	6	16	27
<b>Organisation (O)</b>	5	Security Policy	1	2	5
	6	Organisation of Information Security	2	11	25
	7	Asset Management	2	5	14
	13	Information Security Incident Management	2	5	14
	14	Business Continuity Management	1	5	11
<b>People (P)</b>	8	Human Resources Security	3	9	25
<b>Environment (E)</b>	9	Physical and Environmental Security	2	13	32
	15	Compliance	3	10	24
<b>Total objectives, controls and measures</b>			<b>39</b>	<b>133</b>	<b>283</b>

### 4.3 ISO/IEC 27002 Assessment Measures

In the knowledge acquisition steps explained above, the main clauses of the standard, together with their objectives and security controls, are structured according to the TOPE domains. For each security control, measures are introduced, as shown in Table 4-4. The tables appeared in the following sections are the results of applying the methodology explained above (preliminary analysis, text analysis and interview analysis), and after several iterations of each step, based on the updated information at each of the previous knowledge acquisition steps.



### 4.3.1 Technology Issues

Technology issues in the management of information security are the issues associated with the technology itself that enables ICT applications and services, and with accessing and using the technology applications and services. Based on this, three parts of ISO/IEC 27002 would be associated with technology issues, and these are the following:

#### 4.3.1.1 Communications and Operations Management

This part is concerned with ten main technology issues: operational procedures, third party service delivery, system planning and acceptance, protection against malicious codes, software and information back-up, network security, media handling, exchange of information and software, e-commerce services and monitoring activities. The protection measures associated with these issues are given in Table 4-5. These measures are derived from the “controls” of the standard, as shown above. It should be noted here that the protection measures introduced in the following tables are given in the same way.

**Table 4-5 Technology: protection measures for “communications and operations management”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Operational procedures and responsibilities: correct and secure operation of “Information Processing Facilities (IPF)”</b>	IPF operating procedures (Documented / Maintained / Made available to the right users)
	Control of changes to IPF
	Segregation of duties: to reduce unauthorised or unintentional or misuse of IPF
	Separation of development, test and operational system: to reduce risk of unauthorised access or change to the operational system
<b>Third Party (TP) service delivery management</b>	Agreement with TP: service definitions, service delivery, and security controls (Implemented/Operated/Maintained)
	TP: services, reports, and records (Monitored / Reviewed / Audited regularly)
	Changes to TP services (Maintaining & improving security / Matching business requirements / Risk-reassessment)

<b>System planning and acceptance: minimising system failure</b>	Performance protection: capacity of resources (Monitoring / Tuning / Future need)
	Acceptance of new & upgraded systems (Criteria / Testing)
<b>Protection against malicious and mobile code: software &amp; information integrity</b>	Protection against malicious code: such as viruses (User awareness / Detection / Prevention / Recovery)
	Use of mobile code: software that moves between computers for automatic execution (Authorisation / Policy)
<b>Back-up: software &amp; information</b>	Back-up policy (Back-up copies / Regular testing)
<b>Network security management: network operation and services</b>	Protection of network function (Authorisation / Responsibilities / Techniques)
	Services agreements: in-house and outsourced (Management requirements / Service level / Security features)
<b>Media handling: information &amp; software protection</b>	Protection procedures for "removable" media
	Protection procedures for "disposable" media
	Protection procedures for information (Handling/Storage)
	Preventing unauthorised access to system document
<b>Exchange of information &amp; software: within an organisation and with any external entity</b>	Protection of information exchange through all types of communication facilities
	Agreements on information exchange with external parties
	Protection of physical media in transit
	Protection of electronic messaging
	Protection of information in interconnected business systems
<b>Electronic commerce services</b>	Protection associated with the public media (Fraud / Dispute / Unauthorised action)
	Protection of on-line transactions (Incomplete transmission / Miss-routing / Unauthorised action)
	Protecting the integrity of public information
<b>Monitoring: detecting unauthorised processing activities</b>	Producing and keeping audit logs: user activities, security events
	Monitoring the use of IPF, with regular reviews
	Protection of Logging (Facilities / Information)
	Logging the activities of system (Administrator / Operator)
	Fault (Logging / Analysis / Action)
	Clock synchronisation of relevant systems

#### 4.3.1.2 Access Control

This part is concerned with seven main technology issues: access to business resources, user access management, user access responsibilities, network access, operating systems access, access to applications and information and access to mobile computing and tele-working. The protection measures associated with these issues are given in Table 4-6.

**Table 4-6 Technology: protection measures for “access control”**

<b>Issue</b>	<b>ISO/IEC 27002 Controls (Protection Measures)</b>
<b>Access to business</b>	Access policy according to business requirements (Established / Recommended / Reviewed)
<b>User access management: authorisation</b>	User registration & de-registration procedures
	Privileges allocation control
	Password allocation procedure
	Regular reviews of access rights
<b>User access responsibilities</b>	Selection and use of passwords according to security practices
	Appropriate protection of unattended equipment
	Clear desk (Paper / Media) / Clear screen policy
<b>Network access control: network services</b>	Access to services should be restricted to the right users
	Remote access control using appropriate authentication
	Automatic equipment identification to authenticate connections from specific locations
	Physical and logical access control to remote Diagnostic and configuration ports
	Segregation of (Information services / Users / Information systems)
	Access control to shared networks according to the requirements of business applications
	Routing control along with the access control policy
<b>Operating system access control</b>	Secure log-on procedures for access to operating systems
	Unique user identifier (ID) / ID authentication technique
	Interactive password management system that ensures quality passwords
	Control of utility programmes that may override system and application controls
	Shutdown policy after a defined period of inactivity
	Limit on connection time for high-risk applications
<b>Application and information access control</b>	Control of access to information and application system functions according to access policy
	Dedicated (isolated) environment for sensitive systems
<b>Mobile computing and tele-working</b>	Security policy and protection measure for (Mobile computing / Communication facilities)
	Control of tele-working activities (Policy / Operational plans and procedures)

#### **4.3.1.3 Information Systems Acquisition, Development and Maintenance**

This part is concerned with six main technology issues: information systems security requirements, correct processing in applications, cryptographic controls, security of system files, security in development and support processes and technical vulnerability management. The protection measures associated with these issues are given in Table 4-7.

**Table 4-7 Technology: protection measures for “information systems acquisition, development and maintenance”**

<b>Issue</b>	<b>ISO/IEC 27002 Controls (Protection Measures)</b>
<b>Information systems security requirements</b>	Security controls should be specified with the business requirements of new or renewed information systems
<b>Correct processing in applications(*)</b>	Validation of input data: to applications
	Incorporating validation checks into applications
	Ensuring message integrity in applications
	Validation of output data: from applications
<b>Cryptographic controls</b>	Cryptography policy: for confidentiality, authenticity & integrity (Developed / Implemented)
	Key management policy to support the use of cryptographic techniques
<b>Security of system files</b>	Control procedures for the installation of software on operational systems
	Care for test data (Selection / Protection / Control)
	Control of access to source code of programmes
<b>Security in development and support processes</b>	Control procedures for the implementation of changes
	Protection of critical business applications from change in operating systems (Reviewing / Testing)
	Limiting changes to software packages / Strict control on necessary changes
	Preventing information leakage
<b>Technical vulnerability management(*)</b>	Controlling outsourced software (Supervision / Monitoring)
	Protection against technical vulnerabilities (Obtaining information / Evaluation / Risk assessment / Developing measures/ Implementation)

### 4.3.2 Organisation Issues

The organisation issues are concerned with handling resources and managing events. ISO/IEC 27002 has five parts associated with these issues as shown in Table 4-4, and these are given below.

#### 4.3.2.1 Information Security policy document

This part has one main organisation issue: security policy. The protection measures associated with this issue are given in Table 4-8.

**Table 4-8 Organisation: protection measures for “security policy”**

<b>Issue</b>	<b>ISO/IEC 27002 Controls (Protection Measures)</b>
<b>Information Security Policy</b>	Information security policy (approved / published / communicated)
	Review of the information security policy (suitability / adequacy / effectiveness)

#### 4.3.2.2 Organisation of Information Security

This part has two main organisation issues: internal organisation, i.e. within the enterprise concerned, and the enterprise concerned with external parties. The protection measures associated with these issues are given in Table 4-9.

**Table 4-9 Organisation: protection measures for “organisation of information security”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Internal organisation</b>	Management commitment to information security (Directions / Commitment / Assignment of responsibilities)
	Coordination of information security activities by representatives from different departments (Roles / Job functions)
	Clear definition of information security responsibilities(*)
	Authorisation process for new information processing facilities (Identified/Implemented)
	Organisation’s confidentiality requirements agreements should be (Identified / Regularly reviewed)
	Maintaining appropriate contacts with relevant authorities
	Maintaining appropriate contacts with (Special security forums / Professional associations)
	Regular reviews by an independent body, or in case of change, should take place (Objectives / Policy / Procedures)
<b>External parties</b>	Risks to IPF from business processes involving “external parties” should be (Identified & Appropriate controls implemented) before access is granted
	Security requirements should be addressed before granting “customers” access to information or assets
	Agreements with third parties should cover all relevant security requirements (Accessing / Processing / Communicating / Managing IPF)

#### 4.3.2.3 Asset Management

This part also has two main organisation issues: responsibility for organisation’s assets, and the classification of information. The protection measures associated with these issues are given in Table 4-10.

**Table 4-10 Organisation: protection measures for “asset management”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Responsibility for assets</b>	Assets (Identification / Inventory)
	Assigning owner, “a responsible person or entity: not a property owner”, to the relevant assets (Information / IPF)
	Rules of acceptable use should be (Identified / Documented / Implemented)
<b>Information classification</b>	Classification of information according (Value / Legal requirements/Sensitivity/Criticality to organisation)
	Procedures for information (Labelling / Handling)

#### 4.3.2.4 Information Security Incident Management

This part also has two main organisation issues: reporting information security events and weaknesses, and managing information security incidents. The protection measures associated with these issues are given in Table 4-11.

**Table 4-11 Organisation: protection measures for “information security incident management”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Reporting information security events and weaknesses</b>	Reporting security events as quickly as possible
	Reporting security weaknesses in (Systems/ Services) by (Employees / Contractors / Third party users)
<b>Management of information security incidents(*)</b>	Response procedures (Quick / Effective / Orderly)
	Mechanisms to (Quantify / Monitor) security incidents according to (Type / Volume / Cost)
	Evidence on incident (Collecting / Retaining / Presenting to jurisdiction)

#### 4.3.2.5 Business Continuity Management

This part is concerned with the security aspects that enable managing interruption events and ensures keeping business continuity. The protection measures associated with these issues are given in Table 4-12.

**Table 4-12 Organisation: protection measures for “business continuity management”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Information security aspects of business continuity management (*)</b>	Management process addressing information security requirements for business continuity (Developed / Maintained)
	Business interruption events should be (Identified with their Probability / Impact / Consequences)
	Plans to restore operation and information at the required level and in the required time scale should be (Developed / Implemented)
	A framework of business continuity plans should be maintained for consistency in (Addressing security requirements / Identifying priority for testing & maintenance)
	Regular (Testing / Update) of business continuity plans

### 4.3.3 People Issues

Three main types of issue are associated with people; they include: issues of concern prior to employment, issues of importance during employment and issues related to employment termination or change of employment. The protection measures associated with these issues are given in Table 4-13.

**Table 4-13 People: protection measures for “human resources security”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Prior to employment</b>	Security roles and responsibilities of (Employees / Contractors / Third party users) should be (Defined and Documented) according to security policy
	Verification checks on all candidates for (Employment / Contractors / Third party users) should be carried out in accordance with relevant (Laws / Regulations / Ethics) considering (Business requirements / Classification of information to be accessed / Risks)
	Contractual security obligations should be agreed and signed by (Employees / Contractors / Third party users)
<b>During employment</b>	(Employees / Contractors / Third party users) should apply security in accordance with established policies
	(Employees / Contractors / Third party users) should receive appropriate awareness and training with regular updates(*)
	Establishing a formal disciplinary process for employees who have committed a security breach
<b>Termination or change of employment</b>	Clear (Definition / Assignment) of responsibilities for performing employment termination or change of employment
	(Employees / Contractors / Third party users) should return all assets in their possession upon termination of their work
	Access rights of (Employees / Contractors / Third party users) should be removed upon termination of their work

### 4.3.4 Environment Issues

The environment issues are concerned with the physical environment on the one hand, and with professional environment on the other hand. ISO/IEC 27002 has two parts associated with these issues, and these are given below.

#### 4.3.4.1 Physical and Environmental Security

This part has two main issues: an issue concerned with providing secure areas, and another concerned with equipment security. The protection measures associated with these issues are given in Table 4-14.

**Table 4-14 Environment: protection measures for “physical and environmental security”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Secure areas</b>	Barriers (Walls / Card controlled entry gates / Manned reception desks) to protect information and information processing facilities
	Entry controls to secure areas
	Physical security to (Offices / Rooms, / Facilities)
	Physical protection from environmental threats (Flood / Earthquake / Explosion / Civil unrest / Other threats)
	Protection and guidelines for working in secure areas should be (Designed / Applied)
	Access points including (Delivery & Loading areas) should be (Controlled / Isolated) from IPF.
<b>Equipment security</b>	Equipment sitting or protection to: reduce environmental threats (Flood / Earthquake / Explosion / Civil unrest / Other threats) / avoid unauthorised access
	Equipment protection from (Power failures / Other disruptions)
	Protection of cabling (Power / Telecommunications) carrying data or supporting information services from interception or damage
	Correct maintenance of equipment
	Protection of off-site equipment from the different risks of working outside the organisation’s premises
	Checking media prior to disposal to ensure the absence (Sensitive data / Licensed software)
	No movement of (Equipment / Software / Information) without prior authorisation

#### **4.3.4.2 Compliance**

This part has three main issues: compliance with legal requirements, compliance with security policies and standards and information system audit considerations. The protection measures associated with these issues are given in Table 4-15.

The above view of the ISO/IEC 27002 has integrated the various issues of the standard around the TOPE domains. It has also summarised the protection measures around these domains with indicators that can help future evaluation.

It should be noted here that the standard gives more emphasis to some of the protection measures given above. The policy document of the organisation domain is one of these measures, the rest are marked by (\*) in the above



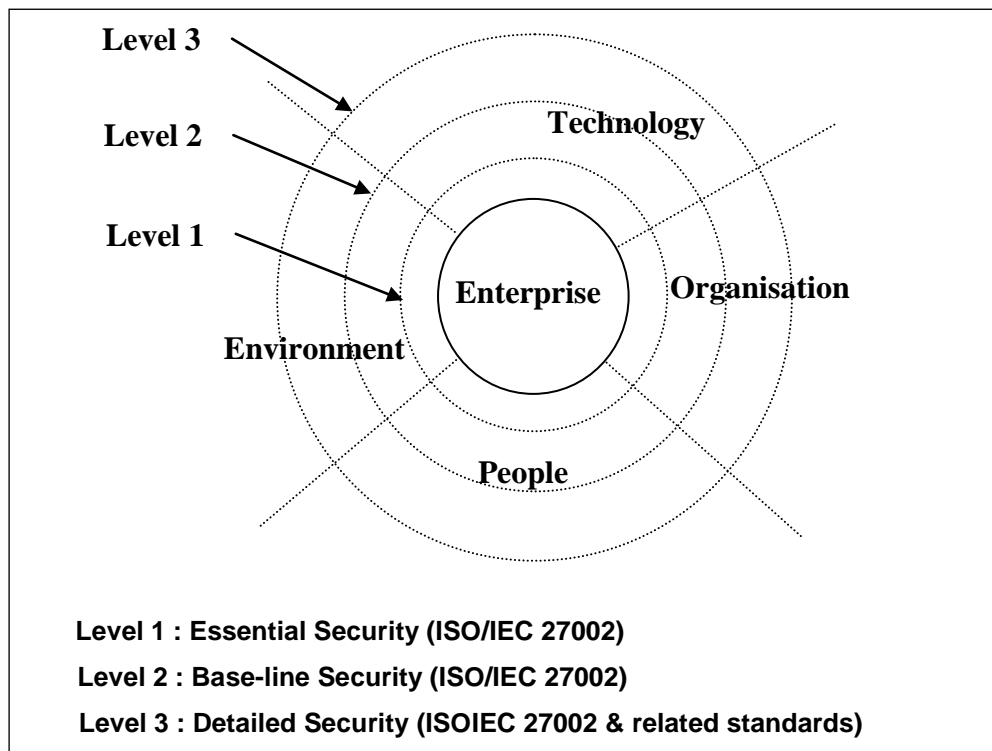
tables. These can be assigned extra weight in the assessment process as will be discussed later in Chapter 5.

**Table 4-15 Environment: protection measures for “compliance”**

Issue	ISO/IEC 27002 Controls (Protection Measures)
<b>Compliance with legal requirements</b>	Relevant requirements (Statutory / Regulatory / Contractual) & Approach to meet them should be (Defined / Documented / Kept up to date) for (Each information system / the Organisation)
	Implementing technical procedures that ensure compliance with (Legislative / Regulatory / Contractual) / and are Concerned with the (The use of material that may enjoy Intellectual Property Rights (IPR) / The use of proprietary software products)(*)
	Protection of important records from (Loss / Destruction / Falsification) in accordance with (Statutory / Regulatory / Contractual / Business requirements)
	Data protection and privacy according to requirements in (Legislation / Regulations / Contracts)
	Deterring users from using IPF for unauthorised purposes
	Cryptographic controls should be used in compliance with (Relevant agreements / Laws / Regulations)
<b>Compliance with security policies and standards,</b>	Managers should ensure that all security procedures, (Within their area of responsibility) are carried out correctly according to (Security policy / Standards)
	Regular checks of information systems for compliance with security implementation standards
<b>Information systems audit considerations</b>	Audit requirements and activities involving (Checks on operational systems) should be carefully planned and agreed to minimise disruption
	Access to audit tools should be protected to prevent (Misuse / Compromise)

#### **4.4 Incremental Assessment Approach**

This section presents an incremental approach for the assessment of enterprise information security. The assessment approach is based on the TOPE scope, on one hand, and on the information security management recommendations of the ISO/IEC 27002 standard, on other hand. The proposed approach is of incremental nature, and has three levels of assessment, as shown in Figure 4-1, with increasing security controls. The first level considers the ISO/IEC 27002 19 essential and common security controls, as stated by the standard, which are refined into 45 measures. The second level is concerned with all the ISO/IEC 27002 133 base-line security controls,



**Figure 4-1 A TOPE scope for information security requirements**

including those of level one, which are refined into 283 basic measures. The third level adds to the second level other security controls considered by other standards related to the ISO/IEC 27002, or required by various individual enterprises, depending on their business and information security strategies.

The method has the following features:

- It provides an incremental approach for assessing and consequently applying information security according to three levels of increasing protection.
- It considers the refinement of each security control into a number of basic measures that ease both assessment and application of the ISO/IEC 27002 information security controls.

The incremental method considered here has three levels of increasing information security protection. Figure 4-1 illustrates these levels which are described in the following.

#### 4.4.1 Level 1: Essential and Common Security Measures

The first level is concerned with the essential and common ISO/IEC 27002 eight security objectives, and their associated 19 information security controls as shown in Table 4-16 (ISO/IEC 27002 2005, p.x). This level represents the initial starting level that should enjoy priority in enterprises seeking information security protection. The controls of this level have been refined into 45 security protection measures that ease the assessment and support the application of this level. Table 4-16 gives the security objectives and protection controls of this level according to the TOPE scope; and it also shows the number of measures associated with each control.

**Table 4-16 TOPE view of ISO/IEC 27002 essential security objectives, controls, together with the number of measures associated with each control**

D	Clause	Objective	Protection Control	measure
T	Information systems acquisition, development and maintenance	Correct processing in applications	Validation of input data: to applications	1
			Incorporating validation checks into applications: to detect any corruption of information through processing errors or deliberate acts	1
			Ensuring message integrity in applications	2
			Validation of output data: from applications	1
		Technical vulnerability management	Protection against technical vulnerabilities ( <i>obtaining timely information / evaluation / risk assessment / developing measures/ implementation</i> )	3
O	Security policy	Information security policy document	Information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	3
	Organisation of information security	Internal organisation	Clear definition of information security responsibilities	2
	Information security	Management of information	Response procedures ( <i>quick / effective / orderly</i> )	3

	<b>incident management</b>	<b>security incidents and improvement</b>	Mechanisms to ( <i>quantify / monitor</i> ) security incidents according to( <i>type / volume / cost</i> )	3
			Evidence on incident ( <i>collecting / retaining / presenting to jurisdiction</i> )	3
	<b>Business continuity management</b>	<b>Information security aspects of business continuity management</b>	Management process addressing information security requirements for business continuity ( <i>developed / maintained</i> )	2
			Business interruption events should be( <i>identified with their: probability / impact / consequences</i> )	2
			Plans to restore operation and information at the required level and in the required time scale should be ( <i>developed / implemented</i> )	2
			A framework of business continuity plans should be maintained for consistency in ( <i>addressing security requirements / identifying priority for testing &amp; maintenance</i> )	3
Regular ( <i>testing / Updating</i> ) business continuity plans	3			
<b>P</b>	<b>Human resources security</b>	<b>During employment</b>	People ( <i>employees / contractors / third party users</i> ) should receive appropriate awareness and training with regular updates in organisational policies and procedures relevant to their job functions	3
<b>E</b>	<b>Compliance</b>	<b>Compliance with legal requirements</b>	Implementing technical procedures that ensure compliance with ( <i>legislative / regulatory / contractual</i> ) / and are concerned with the ( <i>use of material that may enjoy intellectual property rights: IPR / use of proprietary software products</i> )	3
			Protection of important records from ( <i>loss / destruction / falsification</i> ) in accordance with ( <i>statutory / regulatory / contractual / business requirements</i> )	3
			Data protection and privacy according to requirements in( <i>legislation / regulations / contracts</i> )	3
<b>Total</b>		<b>8</b>	<b>19</b>	<b>45</b>

#### 4.4.2 Level 2: ISO/IEC 27002 Security Measures

The second level is associated with all ISO/IEC 27002 39 objectives and their associated 133 controls, including those of the first level. This level represents the internationally recommended base-line information security protection that should be followed by all enterprises. The controls of this level have been

refined into 283 basic security protection measures, as shown in Table 4-4 that ease the assessment and support the application of this second level.

### 4.4.3 Level 3: ISO Other Security Standards

The third level goes beyond the base-line security protection provided by ISO/IEC 27002. It considers the additional security controls of other ISO standards.

**Table 4-17 TOPE view of ISO/IEC 27002 related ISO standards**

TOPE	ISO/IEC 27002		Related Standards		
	Clause	Objective	Standard	Related Issues	
T	Communications and Operations Management	Network security management	ISO/IEC 18028	IT security techniques: IT network security	
	Information Systems Acquisition, Development and Maintenance	Security requirements	ISO/IEC 13335	Risk management processes to identify requirements for security controls	
			ISO/IEC 15408	Evaluation criteria for IT security products	
		Cryptographic controls	ISO/IEC 11770	Management of cryptographic keys	
			ISO/IEC 9796	Public key encryption and digital signature	
			ISO/IEC 14888		
		Other cryptographic control standards: JTC 1 SC 27 and other standards			
		Security of system files	Security in development and support processes	ISO/IEC 10007: TC 176 Management	Configuration management
				ISO/IEC 12207: SC 7 Software	Software lifecycle process
			ISO/IEC 15408	Evaluation of systems and software for high integrity	
O	Security Policy	Information Security Policy	ISO/IEC 13335-3	Risk assessment	
			ISO/IEC 13335-1	Concepts and models for security management	
	Organisation of Information Security	Internal organisation	ISO/IEC 13335-1	Management commitment to information security	
			ISO 19011: TC 176 Management	The establishment and recommendation of a review programme	
	Asset	Responsibility	ISO/IEC 13335-3	To value assets and	

	Management	for assets		represent their importance
	Information Security Incident Management	Reporting events and weaknesses	ISO/IEC 18044	Reporting of information security events and management of incidents
<b>E</b>	Compliance	Compliance with legal requirements	ISO 15489-1 TC 46 Information and documentation	Managing organisational records

Table 4-17 gives a TOPE view of the other ISO standards associated with the various clauses of the ISO/IEC 27002 standard, and it also shows the related issues addressed by these standards. This level may also consider other security controls related to various national standards, and it may also include the special information security protection requirements of individual enterprises, that related to their business objectives.

## 4.5 Summary

The work presented in this chapter supports the future use of the ISO/IEC 27002 information security management standard in two main ways. On the one hand, it gives an integrated view of the standard, according to the TOPE domains, with illustrations of how to provide valid security measures for evaluating the effectiveness of applied information security management practices, according to the standard. On the other hand, it introduces an incremental approach for assessing and consequently managing information security inside enterprises according to three levels of increasing protection measures. The chapter promotes the use of the ISO/IEC 27002 standard and helps enterprises to move gradually and in a well structured approach toward enhancing their information security according to the ISO international information security management standards.

# **Chapter 5**

## **A MODEL FOR ENTERPRISE INFORMATION SECURITY READINESS ASSESSMENT**

### **5.1 Introduction**

This chapter presents a mathematical model that enables numerical investigation of enterprise information security readiness, with regards to the security requirements of the ISO/IEC 27002 information security management standard. The proposed model has a multi level structure that coincides with the hierarchical design of the ISO/IEC 27002 standard. It depends on a modelling technique that enables aggregation of lower level information security assessment values into upper level comprehensive scores. It has the ability to capture the employees' perception about the effective use of information security protection measures. The developed model serves as a base for designing an information security investigation form that can be used to collect the required enterprise information security assessment data. Chapter 5, therefore, contributes in addressing the second research question stated in Chapter 1 which is related to the assessment of enterprise information security readiness by using an efficient, valid and reliable modelling technique.

### **5.2 Assessing Enterprise Information Security**

Enterprises willing to obtain ISO/IEC 27001 information security certification that promotes their e-services image should normally pass through three

successive stages as follows:

- The first stage is for the alignment of the enterprise's information security management system with the one in the ISO standard.
- The second stage is the conformance with the ISO requirement which typically involves the enterprise to implement ISMS using ISO/IEC 27001 and ISO/IEC 27002 standards. By doing so, the enterprise asserts internally that its ISMS system is compliant with the standard, but without any proof.
- The third stage is to have a formal certification of the enterprise's ISMS against ISO/IEC 27001 by an accredited certification body.

The first and second stages stated above are running internally by the enterprise information technology department. The results of the conformance process are a list of the missing ISO/IEC 27002 security controls that should be implemented before the enterprise moves to the third stage of getting a formal certificate. In this respect, the assessment model presented in this thesis is expected to provide enterprises with a tool that helps in the identification of the missing ISO/IEC 27002 controls. In addition, it will provide these enterprises with an assurance measure of the effective use of these controls.

The ISO/IEC 27004 (2009) measurement standard recommends the following general steps for the development and implementation of enterprise information security measurement system.

- Developing measure (i.e. base measures, derived measures and indicators);



- implementing and operating an information security management programme;
- collecting and analysing data;
- developing measurement results;
- communicating developed measurement results to the relevant stakeholders;
- using the measurement results as contributing factors to ISMS-related decisions;
- using the measurement results to identify the needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
- facilitating continual improvement of the information security measurement programme.

The above steps are found to be aligned with the approach presented in this thesis for developing an information security assessment model. The proposed model could be used by enterprises to measure the effective use the ISO/IEC 27002 security controls and to provide an assurance measure of enterprises' information security management system (Saleh et al. 2007).

### **5.3 Information Security Assessment Approach**

The approach described below can be used for practical investigation of an enterprise with the ISO/IEC 27002 information security management standard and with its associated standard ISO/IEC 27001. The approach is described in terms of the following:

- The TOPE view of the approach that re-arranges the clauses, objectives and controls of the ISO/IEC 27002 according to the TOPE domains (see

Chapter 4). This will present the structure of the evaluation that is the structure of the quantitative indicators for evaluating information security readiness.

- The assessment model that enables the evaluation of enterprises with the ISO/IEC 27002 controls upon which the assessment provided by the method is based.
- The basic steps of the assessment method to show how the measures are evaluated.

### **5.3.1 The TOPE View of the ISO/IEC 27002 Standard**

Chapter 4 suggests mapping between the TOPE domains and the main clauses of the ISO/IEC 27002 standard. Table 4-4 showed how the ISO/IEC 27002 clauses, and their associated objectives, controls and measures have been mapped to the TOPE domains of technology, organisation, people and environment. The numbers of measures required for investigating information security readiness with regards to the ISO/IEC 27002 protection controls associated with each TOPE domain are as follows: 133 for the technology domain, 69 for the organisation domain, 25 for the people domain and 56 for the environment domain. Appendix A holds a complete list of these measures.

### **5.3.2 The Assessment Model**

The proposed mathematical model for practical investigation of information security readiness within an enterprise is presented in the following three stages:

- The first stage is concerned with identifying the TOPE based structure of the model that integrates the various parts and issues of the ISO/IEC 27002 standard.

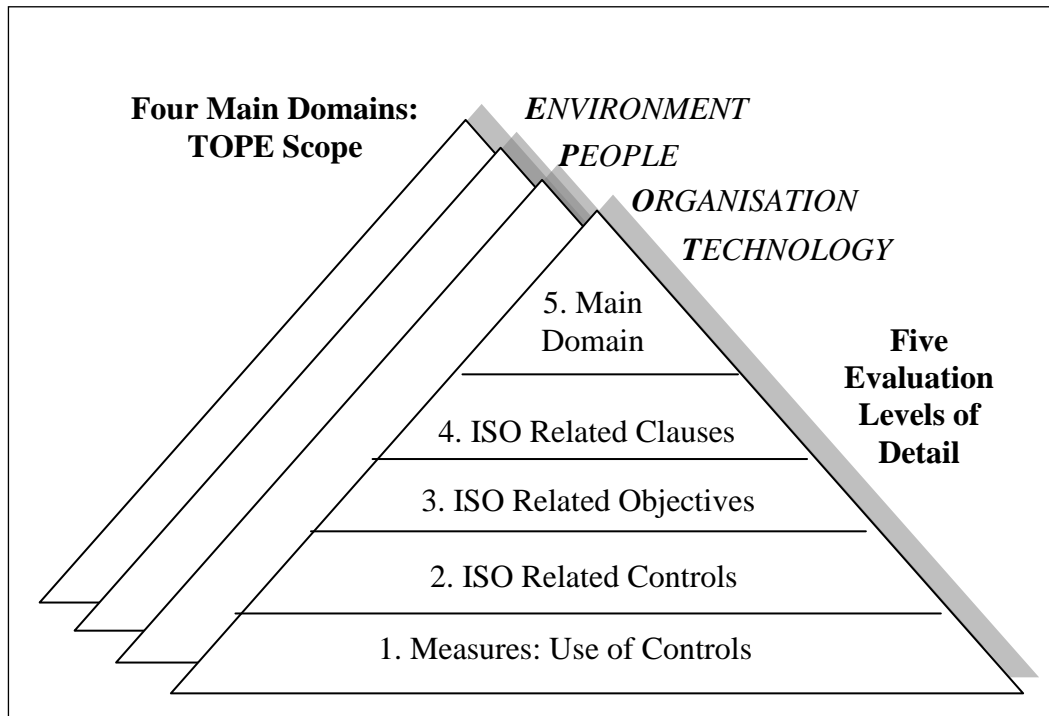
- The second stage is associated with describing how the information security readiness assessment, for the various issues of the TOPE based structure, can be investigated.
- The third stage is related to providing guidelines on the application of the model in the investigation of practical case-studies.

### **5.3.2.1 Model Structure**

The proposed approach considers the evaluation of the indicators to be associated with the following five main levels:

- The first level is concerned with the assigned information security measures, that developed in Chapter 4, for the evaluation of the effective use of security controls of the ISO/IEC 27002 standard;
- the second level is associated with the security controls recommended by the standard for the achievement of its objectives;
- the third level is related to the security categories of the clauses of the standard, which are concerned with its objectives;
- the fourth level is concerned with the clauses of the standard organised according to their relationship with each of the TOPE domains; and
- the fifth level is associated with the TOPE domains.

Figure 5-1 illustrates the multi-level structure explained above. This structure integrates the issues of the standard over the TOPE domains and provides five main levels of detail for each domain, considering the divisions of the document of the standard. The four domains give the integrated scope of the standard, while the five levels of detail provide the depth according to which each domain can be investigated.



**Figure 5-1 The structure of the TOPE model concerned with the investigation of enterprises with the ISO/IEC27002 standard**

### **5.3.2.2 Investigation of Information Security Readiness**

The investigation of information security readiness, described below, has the following main features:

- It provides evaluation indicators for each of the TOPE domains, and at all levels of detail, as shown in Figure 5-1;
- it recognises that the evaluation of the indicators starts at the bottom level and moves gradually from one level to another, where the evaluation of each of the higher levels is based on the evaluation of its preceded level; and
- in accumulating the indicators from one level to another, it assigns weights to the values of the indicators, so that each indicator is valued according to its importance weight to the information security of the enterprise considered.

The investigation also provides an overall ISO/IEC 27002 information security indicator for the enterprise considered. This can be called the security(s)-readiness indicator of the enterprise.

### **5.3.2.3 The Mathematical Model**

Table 5-2 translates the above investigation features into mathematical forms. It provides mathematical representations of the issues of the TOPE domains and their levels of detail. It defines the investigation indicators and provides the mathematical equations needed for their evaluation. It refines the target investigation of information security readiness assessment into the following five main steps:

- The first step considers the investigation of indicators at the bottom level. It is concerned with the information security measures associated with the evaluation of the effective use of the ISO/IEC 27002 security controls. In this respect, it considers that various measures of using a security control have different relative weights representing their shared effect on the use of that control, as discussed before in Chapter 4. In addition, it also considers that the performance grades of these security measures can be evaluated based on the following four metrics:
  - Whether management is aware of the importance of the measure;
  - if monitoring of the measure is performed;
  - if the measure and its inputs and outputs are documented; and
  - if the measure improvement actions take place on regular basis.

These four metrics are used to evaluate each measure, and finally the average represents the performance grade of the concerned measure.

The assessment of the security measures at the lower levels will be conducted using the scale in Table 5-1.

- The second step moves up to the investigation concerned with the achievement of the ISO/IEC 27002 objectives. It shows how the indicators of this achievement can be found. The evaluation of these indicators depends mainly on the evaluation indicators of the effective use of security controls related to the objectives concerned. Relative weights are also taken into account here, with respect to the relationships of the security controls with their related objectives.

**Table 5-1 Reference table for performance values of the assessment measures**

<b>Grade</b>	<b>Explanation</b>
<b>Excellent</b>	The management is aware of the importance of the measure. The measure is monitored. Documentation is present. The measure is under continuous improvement.
<b>Very Good</b>	The management is somewhat aware of the importance of the measure. No monitoring is performed. Documentation is present. No continuous improvement.
<b>Good</b>	The management is aware of the importance of the measure. No monitoring is performed. No documentation is present. No continuous improvement.
<b>Poor</b>	Some of the management personal aware about the importance of the measure. No monitoring performed. No documentation exists. No continuous improvement takes place.
<b>None</b>	The management is not aware of the importance of the measure. No monitoring performed. No documentation exists. No continuous improvement.

- The third step is concerned with the investigation of information security readiness in accordance with ISO/IEC 27002 clauses. It shows how the indicators of this investigation can be found. The evaluation of these indicators depends on the achievement of ISO/IEC 27002 objectives. Relative weights are also taken into account, with respect to the relationships of the objectives with their related ISO/IEC 27002 clauses.

**Table 5-2 The TOPE model issues, equations and steps concerned with the investigation of enterprises with the ISO/IEC 27002 standard**

<b>Indexes of the issues of the TOPE structure and their ranges</b>	<b>TOPE domains</b>	<i>i</i>	Domain index.
		<i>l</i>	Number of domains: <i>l</i> = 4 (TOPE)
	<b>ISO clauses</b>	<i>j</i>	ISO clause index.
		<i>J</i> [ <i>i</i> ]	Number of ISO clauses related to domain [ <i>i</i> ]
	<b>ISO objectives</b>	<i>k</i>	ISO objective index.
		<i>K</i> [ <i>i</i> , <i>j</i> ]	Number of ISO objectives related to part [ <i>j</i> ] of domain [ <i>i</i> ].
	<b>ISO controls</b>	<i>l</i>	ISO security control index.
		<i>L</i> [ <i>i</i> , <i>j</i> , <i>k</i> ]	Number of ISO security controls associated with objective [ <i>k</i> ] of clause [ <i>j</i> ] of domain [ <i>i</i> ].
<b>Evaluation measures</b>	<i>m</i>	Index of one measure of use of a security control.	
	<i>M</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> ]	Number of measures concerned with the use of security control [ <i>l</i> ] of objective [ <i>k</i> ] of clause [ <i>j</i> ] of domain [ <i>i</i> ].	
<b>STEP 1: Use of ISO controls</b>	<i>v</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> , <i>m</i> ]	Value assigned to one measure concerned with the use of a security control.	
	<i>w</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> , <i>m</i> ]	Relative weight of the measure for the security control considered.	
	<i>c</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> , <i>m</i> ]	Relative value of the measure: $c[i, j, k, l, m] = w[i, j, k, l, m] \cdot v[i, j, k, l, m]$	
	<i>C</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> ]	Indicator of use of the security control considered.	
	$C[i, j, k, l] = \sum_{m=1}^{M(i, j, k, l)} c[i, j, k, l, m]$		
<b>STEP 2: Achievement of ISO objectives</b>	<i>w</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> ]	Relative weight of a security control for its objective	
	<i>b</i> [ <i>i</i> , <i>j</i> , <i>k</i> , <i>l</i> ]	Relative indicator of use of the security control considered for its objective: $b[i, j, k, l] = w[i, j, k, l] \cdot C[i, j, k, l]$	
	<i>B</i> [ <i>i</i> , <i>j</i> , <i>k</i> ]	Indicator of achievement of the objective considered.	
	$B[i, j, k] = \sum_{l=1}^{L(i, j, k)} b[i, j, k, l]$		
<b>STEP 3: Conformance of ISO clauses</b>	<i>w</i> [ <i>i</i> , <i>j</i> , <i>k</i> ]	Relative weight of an objective for its clause	
	<i>p</i> [ <i>i</i> , <i>j</i> , <i>k</i> ]	Relative indicator of objective achievement for its clause: $p[i, j, k] = w[i, j, k] \cdot B[i, j, k]$	
	<i>P</i> [ <i>i</i> , <i>j</i> ]	Indicator of conformance of the clause considered.	
	$P[i, j] = \sum_{k=1}^{K(i, j)} p[i, j, k]$		
<b>STEP 4: Compliance of TOPE domains</b>	<i>w</i> [ <i>i</i> , <i>j</i> ]	Relative weight of a clause for its domain	
	<i>d</i> [ <i>i</i> , <i>j</i> ]	Relative indicator of clause conformance for its domain: $d[i, j] = w[i, j] \cdot P[i, j]$	
	<i>D</i> [ <i>i</i> ]	Indicator of compliance of the domain considered.	
	$D[i] = \sum_{j=1}^{J(i)} d[i, j]$		
<b>STEP 5: Security-readiness</b>	<i>w</i> [ <i>i</i> ]	Relative weight of a domain	
	<i>r</i> [ <i>i</i> ]	Relative indicator of the domain compliance: $r[i] = w[i] \cdot D[i]$	
	<i>R</i>	Indicator of overall security readiness: <i>s-readiness</i> .	
	$R = \sum_{i=1}^{I=5} r[i]$		

- The fourth step is concerned with the investigation of compliance with one TOPE domains. It shows how the indicators of this compliance can be found. The evaluation of these indicators depends on the evaluation of the indicators of conformance of ISO/IEC 27002 clauses. Relative weights are also taken into account, with respect to the relationship of the ISO/IEC 27002 clauses with their related TOPE domains.
- The fifth step is the final step, and it is concerned with the overall indicator of all TOPE domains, put together collectively, that is the indicator of enterprise security readiness. The evaluation of this indicator depends on the evaluation of the indicators of compliance of the four TOPE domains. The relative weights of these indicators are taken into account.

## 5.4 The Proposed Assessment Process

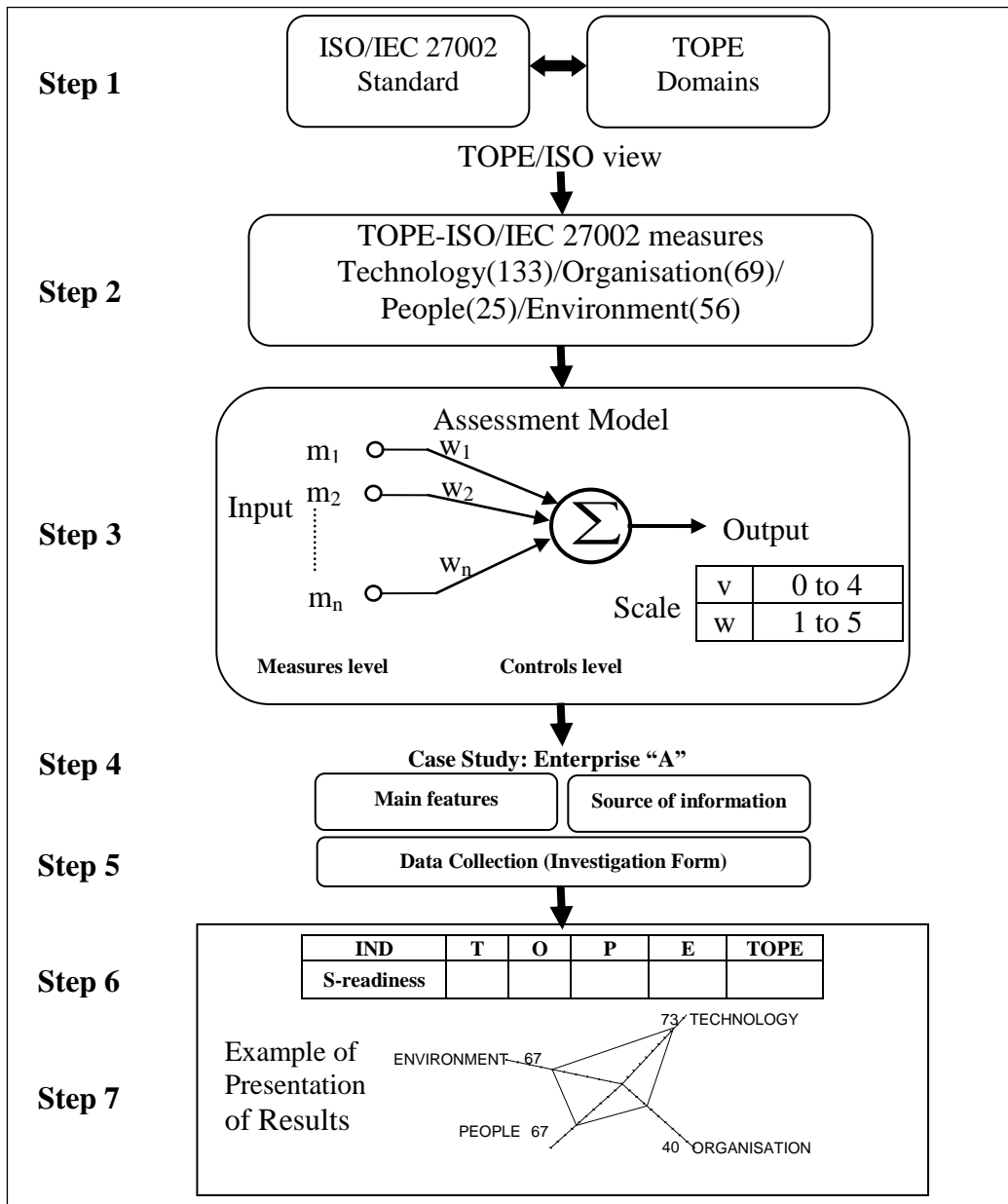
The proposed seven basic steps process to assess enterprise information security readiness are illustrated in Figure 5-2. The explanation of each step is given in the following:

- **Step 1:** Mapping the ISO/IEC 27002 over the TOPE domains; this has been addressed in Chapter 4 and presented in Table 4-1.
- **Step 2:** Providing measures for investigating enterprise conformance with each of the 133 ISO/IEC 27002 security controls; this step is explained also in Chapter 4 and presented in Table 4-4. The details of these measures are given in Appendix A.
- **Step 3:** Preparing an analytical mathematical model that inter-relates the various factors involved and identifies s-readiness assessment



indicators, based on both performance grades and importance weights, as will be explained in the following sections and given in Table 5-2.

- **Step 4:** Identifying the enterprise of the case-study considered. For this purpose, an investigation form including the following two main parts is designed as shown in Appendix A.



**Figure 5-2 The steps of the proposed information security readiness assessment process**

- The first part is concerned with identifying the main features of the enterprise for the case-study considered.
  - The second part is associated with the person providing information on the state of information security of the concerned enterprise.
- **Step 5:** Obtaining the required information on the case-study considered. For this purpose, the mathematical model described above is transformed into a questionnaire instrument which appeared in the third part of the proposed investigation form Appendix A. The resulting investigation form accepts performance grades and relative importance weights based on the scale presented in Tables 5-1 and Table 4-3 respectively for the assessment measures associated with the ISO/IEC 27002 security controls at the bottom level. It also accepts relative weights at the other levels for the controls, objectives, clauses and domains, as discussed before in Chapter 4 and presented in Table 4-3.
- **Step 6:** Deriving the s-readiness indicators at all levels by using the equations of Table 5-2 and the information filled into the investigation form of Step 5.
- **Step 7:** Presenting the obtained results in an illustrated manner. The results can be given at different levels, depending on the level of assessment that needs to be demonstrated. Since every intermediate level includes a number of elements associated with a lower level, the use of the radar graph is suggested to demonstrate the elements of an indicator at a specific level.

## 5.5 Practical Application of the Model

The above model enables practical investigation of enterprises working in different businesses, with the security requirements of the ISO/IEC 27002 standard, to be conducted. This type of investigations would produce indicators at the various levels of the proposed model structure. This would help diagnosing the strengths and the weaknesses of information security protection measures in the concerned enterprise; and it would also help directing their effort toward the issues that need improvements. The data derived from such assessment provides the enterprise with an indication of the level of assurance in their information security system according to the ISO/IEC 27002 standard, and whether there are areas that need improvement. In the application of the model to practical case-studies, the considerations, given below, would need to be taken into account.

- The use of the steps of the model given in Table 5-2 would require a comprehensive investigation form to be designed. The form should cover the scope of the four TOPE domains and the depth of the five levels of the model.
- For every measure concerned with the evaluation of a security control, two inputs need to be specified: the first evaluates the extent to which the measure is practically applied; and the second provides the relative weight of this measure, with regards to accomplishing the security control considered. Table 5-3(a) suggests the use of five grades for the evaluation of the measures depending on the scale presented in Table 5-1. Table 5-3(a) suggests also the use of five grades for the evaluation of the importance of the measure depending on the scale presented in

Table 4-3. The state of different measures can be represented collectively by a radar graph to illustrate their strengths and weaknesses. Table 5-3(b) gives an example concerned with a security control, with three measures involved. Table 5-3(c) provides examples of how the relative weights of three measures can be assigned, based on the scales of Table 4-3 and Table 5-1, and how the state of their security control can be determined.

**Table 5-3 Evaluation grades, weights and examples of measures, relative weights and indicators**

Evaluation Grades (Performance)					
0	1	2	3	4	
None	Poor	Good	Very Good	Excellent	
Evaluation Weights (Importance)					
1	2	3	4	5	
Not at all	Low	Moderate	High	Very high	
(a) Evaluation grades & weights: five states					
<b>(b) Given performance grades of the measures</b>	v [1] = 4 (Excellent)	v [2] = 3 (Very Good)	v [3] = 2 (Good)		
<b>Given relative weights</b>	w [1] = 33 %	w [2] = 50 %	w [3] = 17 %		
<b>Indicator: this can be applied at all levels</b>	$C = v [1] * w [1] + v [2] * w [2] + v[3] * w [3] = 3.16$ (Grade range: Very Good)				
<b>(c) Radar graph illustrating the three given measures: this can be applied at all levels</b>					

- For the evaluation of the achievement of an objective, the state of their security controls would be needed as an input. Another needed input value is the relative weight of each security control involved in the achievement of the objective. The radar graph and the relative weight considerations as shown before in Table 4-3 for the security controls can also be used here for the objective domain. The evaluation for the

higher levels: ISO/IEC 27002 clauses, TOPE domains and the s-readiness levels can then go in the same way, with each taking an input from its preceded level, and another input for the weights of its related issues.

The above guidelines are taken a step further in the following section which describes the basic components of the investigation form.

### **5.5.1 The Investigation Form**

In the application of the above approach to practical case studies, an investigation form would be used for collecting the required data. The design and structure of the investigation form will be based on the assessment approach presented in the previous section. The developed investigation form was extensive, and it was comprised of four major sections as shown in Appendix A.

#### **Design of the Investigation Form**

The investigation form to be used in the assessment has to meet the objectives of the assessment process and must be effective in identifying issues related to the subject matter being assessed. Various researchers have established principles that must be considered when designing the questions of the investigation form that will provide valid and reliable data. These principles include the following: Brevity and clarity; respondent's language ability and specialised knowledge; short sentences free of jargon; one concept, issue or problem; clearly diverging response choices and proper layout of questionnaire (Saunders et al. 2007).

The concept of validity of the questions of the investigation form implies that care must be taken to ensure that these questions assess what it claims to

assess. In other words, validity is concerned with whether the question is measuring the right concept or not. A valid investigation form consistently yields reliable and stable results over time. In this respect, the information security readiness questions must, therefore, focus on what constitutes information security in an enterprise and the user's perception thereof to correctly determine the effective use of the information security measures in the concerned enterprise (Bagozzi 1994; Cooper and Emory 1995). The main sections of the developed investigation form are described in the following:

### **Section "A"**

The first section of the investigation form is used mainly to collect information about the investigated enterprises such as: type of enterprise, size, field, how long has the enterprise been in business and the existence of separate information security department. This information was used to draw a 'business profile' for the participated enterprises in this research work. This helps providing and comparing assessment results associated with enterprises that share common features (Brace 2004).

### **Section "B"**

The second section of the investigation form is concerned with collecting information about the respondents to the investigation form such as: their level in the enterprise, their nationality, age, degree, subject of study, special qualifications in information security and their years of experience working in IT. This information was used to draw the 'Personal Profile' for the respondents of the investigation form. This helps ensuring the credibility of the obtained information.

## **Section “C”**

The investigation form would use the mathematical model presented above that considers and inter-relates all the issues concerned, according to the five levels as shown in Figure 5-1, and the ISO/IEC 27002 clauses, objectives, controls and the associated measures extracted in Chapter 4. So, for each of the four TOPE domains, the following components are taken into account:

- Every measure concerned with the evaluation of a security control, would need two inputs that is the two values explained above to be found manually or automatically if possible.
- Each security control can be evaluated from these measures and can also receive a relative weight value concerned with its association with the related objective.
- Each objective can then be evaluated in the same manner.
- The evaluation process can then be continued gradually to include the evaluation of the ISO/IEC 27002 clauses.

In this respect, the form was designed so that each question is given with the following two factors:

- Indicator for the practical use (performance) of the security measure for information protection in the enterprise. Five levels of indication are given as shown in Table 5-1.
- Indicator for using the security measure (importance) for information security. Five levels of relative importance are given as shown in Table 4-3.

The above components are given in the following tables for each TOPE domain.

## Technology Domain

Table 5-4 gives the three main clauses of the standard associated with the technology domain together with their 23 objectives, 82 protection controls and 133 evaluation measures.

**Table 5-4 Technology domain: Related ISO/IEC 27002 clauses, objectives, protection controls and evaluation measures**

<b>Subject: ISO Clauses</b>	<b>Issue: ISO Objectives</b>	<b>No. of Controls</b>	<b>No. of Measures</b>
<b>Communications and operations management</b>	Operational procedures and responsibilities	4	8
	Third party service delivery management	3	8
	System planning and acceptance	2	5
	Protection against malicious and mobile code	2	6
	Back-up	1	3
	Network security management	2	5
	Media handling	4	6
	Exchange of information	5	9
	Electronic commerce services	3	3
	Monitoring	6	12
<b>Access control</b>	Business requirements for access control	1	3
	User access management	4	6
	User responsibilities	3	5
	Network access control	7	9
	Operating system access control	6	10
	Application and information access control	2	3
	Mobile computing and tele-working	2	5
<b>Information systems acquisition, development and maintenance</b>	Security requirements of information systems	1	2
	Correct processing in applications	4	5
	Cryptographic controls	2	4
	Security of system files	3	4
	Security in development and support processes	5	9
	Technical vulnerability management	1	3

## Organisation Domain

Table 5-5 presents the five main clauses of the standard associated with the organisation domain, together with their 8 objectives, 29 protection controls, and 69 evaluation measures.



**Table 5-5 Organisation domain: Related ISO/IEC 27002 clauses, objectives, protection controls and evaluation measures**

<b>Subject: ISO Clauses</b>	<b>Issue: ISO Objectives</b>	<b>No. of Controls</b>	<b>No. of Measures</b>
<b>Security policy</b>	Information security policy	2	5
<b>Organisation of information Security</b>	Internal organisation	8	18
	External parties	3	7
<b>Assets management</b>	Responsibility for assets	3	8
	Information classification	2	6
<b>Information security incident management</b>	Reporting information security weakness	2	5
	Management of information security incidents	3	9
<b>Business continuity management</b>	Information security aspects of business continuity management	5	11

### **People Domain**

Table 5-6 gives the ISO/IEC 27002 clause concerned with the people domain that is the human resources security which has 3 objectives, 9 protection controls, and 25 evaluation measures.

**Table 5-6 People domain: Related ISO/IEC 27002 clause, objectives, protection controls and evaluation measures**

<b>Subject: ISO Clauses</b>	<b>Issue: ISO Objectives</b>	<b>No. of Controls</b>	<b>No. of Measures</b>
<b>Human resources security</b>	Prior to employment	3	9
	During employment	3	9
	Termination or change of employment	3	7

### **Environment Domain**

Table 5-7 presents the two main clauses of the standard associated with the environment domain together with their 5 objectives, 23 protection controls, and 56 evaluation measures.

**Table 5-7 Environment domain: Related ISO/IEC 27002 clauses, objectives, protection controls and evaluation measures**

<b>Subject: ISO Clauses</b>	<b>Issue: ISO Objectives</b>	<b>No. of Controls</b>	<b>No. of Measures</b>
<b>Physical and environmental security</b>	Secure areas	6	16
	Equipment security	7	16
<b>Compliance</b>	Compliance with legal requirements	6	19
	Compliance with security policies and standards	2	4
	Information system audit consideration	2	4

It should be noted that only numbers are considered above for both the protection controls and their evaluation measures. This avoids unnecessary details; but of course the controls themselves and their measures are important components of the practical investigation form. In addition, the evaluation grades and the relative weights of the various indicators are also important components of the form. Appendix A holds a complete list of these measures.

### **Section “D”**

The final section of the investigation form gives users the opportunity to present their views and comments and to identify the missing and/or the unnecessary factors in the developed investigation form using open ended questions.

In addition the investigation form was accompanied by a cover letter that explained why the enterprise had to complete the questions, what would be done with the feedback, how long it would take to complete the questions and the response would be anonymous.

### **Illustrating the Results**

The radar chart is a graphical method of displaying multivariate data in the form of two-dimensional chart of three or more quantitative variables represented on axes starting from the same point. The relative position and angle of the axes is typically uninformative. The radar graph can be used to answer the following questions: What variables are dominated for a given observation?; Which observations are most similar i.e. are there clusters of observations?; Are there outliers?. It is a useful way to display multivariate observations with an arbitrary number of variables. The radar graph was used

by Johansson and Johnson (2005) in comparing different information security standards based on three (purpose, scope and time) domains. Christian et al. (1996) use the radar graph to illustrate the distribution of funds among five (possession of control, confidentiality, availability, authenticity and integrity) data security factors. The radar graph will be used by the model developed in this chapter for demonstrating the assessment results.

### 5.6 An Illustrative Example

The example presented here illustrates the results that can be obtained from using the above approach and its investigation form for practical case-studies. The example emphasises the results concerned with the single objective and the two protection controls of the ISO/IEC 27002 clause of security policy, associated with the organisation domain. These results are related to two levels of the model which are the measures and the controls levels.

**Table 5-8 An example of the results concerned with the measures of the use of the protection controls of ISO/IEC 27002 “security policy”**

Measures of Protection Controls of Security Policy		Results		Illustration of Results
		v	w	
<b>Control (1): Policy document</b>	Approval by management	3	.5	
	Published throughout the organisation	4	.3	
	Communicated to concerned people	3	.2	
	<i>Indicator of use of security policy control no.1 = 3*.5+4*.3+3*.2 = 3.3</i>			
<b>Control (2): Policy review</b>	Continuing review	2	.7	
	Review if significant change occur	3	.3	
	<i>Indicator of use of security policy control no.2 = 2*.7+3*.3 = 1.32</i>			

- Table 5-8 gives the results concerned with the evaluation of use of the two protection controls, of the ISO/IEC 27002 security policy, using the five measures specified for this purpose. The measures of each control are illustrated in a radar graph. In addition, an indicator of the use of each control is given, considering the weights of the measures with respect to implementing the control.
- Table 5-9 gives the results concerned with the evaluation of the achievement of the single objective of ISO/IEC 27002 security policy, using the evaluation of the use of the related protection controls given in Table 5-8. The grades of the controls are illustrated in a radar graph. In addition, an indicator of objective achievement is given, considering the weights of the controls with respect to achieving the objective.

**Table 5-9 An example of the results concerned with the achievement of ISO/IEC 27002 security policy objective, considering the results of Table 5-8**

Protection Controls of Security Policy Objective		Results		Illustration of Results
		c	w	
<b>ISO Objective: Security Policy</b>	Information security policy document	3.3	.7	
	Review of the information security policy	1.3	.3	
	<b>Indicator of achievement of security policy objective = <math>3.3 \cdot .7 + 1.3 \cdot .3 = 2.71</math></b>			

The results concerned with other objectives and controls of the other ISO/IEC 27002 clauses, associated with the other TOPE domains would be of similar nature.

## 5.7 Impact of the Assessment

The above contribution of this research study will be of practical benefit for both enterprises wishing to test their own information security protection state relative to the information security standards for the purpose of improvement;

and for customers or potential partners concerned with testing the conformance of the enterprises with these standards.

The practical results of the assessment model will indicate the effectiveness of the implemented information security systems from the user perspective and will illustrate the state of their information security readiness. These results will show the weaknesses at all levels with numerical indicators that could be used by the directors of the considered enterprise to assign priorities and direct resources to improve their information security practices. The assessment results also provide the enterprise's officials with the following information:

- Evidence about the effectiveness of security controls in protecting the enterprise information resources. This will help to Identify information system weaknesses and deficiencies and to confirm that the identified weaknesses and deficiencies in the information system have been addressed;
- an indication of the quality of the risk management processes employed within the enterprise as the results of the assessment model will be used in the developed EISRM framework presented in Chapter 3;
- information about the strengths and weaknesses of information systems protection measures, which are supporting enterprise missions and business functions in an environment of increasing challenges;
- prioritise risk mitigating decisions and the associated risk mitigation activities; and
- support continuous monitoring activities and information security situational awareness.

## **5.8 Summary**

The mathematical model presented in this chapter provides a tool for the investigation of the conformance of enterprises information security system with the ISO/IEC 27002 information security management standard, and with its related standard ISO/IEC 27001. The investigation form associated with the model shows how the investigation can be conducted, and how results can be derived and presented. The presented example illustrates the multi-level, results concerned with one TOPE domain, and provides overall higher-level results associated with the TOPE level, together with the s-readiness indicator. Once the enterprise has applied the proposed model, it can assess the effectiveness of their information security system and identify the weaknesses security areas that need improvement.

# Chapter 6

## AN ENTERPRISE INFORMATION SECURITY COST-BENEFIT MODEL

### 6.1 Introduction

Chapter 6 aims to develop an analytical model concerned with the analysis of the cost of the recommended protection measures that could be used by enterprises for facing the information security challenges versus the benefits from acquisition and deployment of these protection measures in reducing the effects of these challenges. One of the essential objectives of the proposed EISRM framework presented in Chapter 3 is to base the mitigation process (the improve phase) on suitable financial metrics and to find the optimal enterprise security budget in the selection of the best-practice controls subset that is appropriate to its needs from the set of all possible best practices security controls. Herewith research question 3 is addressed namely to base the selection of the recommended information security protection measures on an economical analysis.

### 6.2 Background

The information security management, from the perspectives of business managers, is an investment to be measured in saved cost because of reducing loss (Lee et al. 2002; Borodin et al. 2005; Ryan J. and Ryan D. 2006). In contrary, information security management, from the perspectives of technical managers, is only the technical tools and organisational procedures that

should be implemented to reduce the expected risk to an acceptable level (Venter and Eloff 2003). The later approach was prevailing for decades in formulating the information security management financial decisions inside enterprises. The former one started recently to balance the information security expenditures with the expected benefit from these expenditures (Bojanc and Jerman-Blazic 2008; Schrecher 2004; Boehmer 2009).

Recently, a number of important surveys indicates that financial metrics start to direct the decision between the alternatives of information security protection measures. The computer crime and security survey started from 2008 to include a question to determine the popularity of Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) as financial metrics for quantifying the cost and benefits of computer security expenditures. The survey shows that 39% of the respondents indicated that their enterprises used ROI as a metric, 21% used NPV, and 17% used IRR (CSI, 2008, pp 9-10). The global information security breach survey also shows that 44% of the large UK business companies consider the decision on what to spend on information security as formal business, while 38% quantify the quality to business technique and 12% evaluate the ROI (ISBS 2006).

The remainder of this section is as follows: the economical directions stated by standard organisations will be presented first. Then a number of the most important financial metrics and their suitability in investigating information security mitigation plans will be discussed. Finally, the cost-benefit approach for information security risk management will be investigated in detail.



## **6.2.1 Standard Organisations Economic Directions**

The ISO/IEC 27002 information security management standard stated that appropriate controls for risk treatment should be selected and implemented to meet not only the requirements identified by the risk assessment, but also to satisfy other requirements including the cost of implementation and operation in relation to the risks being reduced and the need to balance the investment in implementation and operation of controls against the harm that is likely to result from security failures (ISO/IEC 27002 2005, pp.5-6).

In addition to the above ISO direction, different other standards and professional organisations also include directions and general guidelines for basing the selection of the information security protection measures on an economical analysis. Three of such standards and documents will be presented in the following.

### **6.2.1.1 AS/NZS 4360**

The AS/NZS 4360 risk management standard states that enterprises should adopted specific cost-effective strategies and action plans for risk treatment, development and implementation. The standard also added that the selection of the most appropriate mitigation option involves balancing the costs of implementing each option against the benefits derived from it. Furthermore, the standard suggests that when making such cost versus benefit judgments, the context of the enterprise under consideration should be taken into account considering all direct and indirect costs and benefits whether tangible or intangible, and measured in financial or other terms (AS/NZS 4360 2004, pp. 21-22).

### **6.2.1.2 NIST SP 800-30**

The NIST SP 800-30 document suggests running cost-benefit analysis for each of the proposed controls to determine which control is required and appropriate for the enterprise circumstances. The document emphasises encompassing the following steps in running cost benefit analysis for the new controls:

- Determining the impact of implementing the new or enhanced controls;
- determining the impact of not implementing the new or enhanced controls;
- estimating the costs of the implementation; and
- assessing the implementation costs and benefits against system and data criticality to determine the importance of implementing the new controls to the enterprise, given their costs and relative input (NIST SP 800-30 2002, pp.36-37).

### **6.2.1.3 Microsoft**

The Microsoft document for information security risk management states that the main goal of conducting decision support in selecting the treatment controls is to identify and evaluate control solutions based on a defined cost-benefit analysis process. The document also suggests considering the acquisition, implementation, ongoing, communication, training of both staff of IT & users, productivity & convenience and auditing & verifying the effectiveness of costs in conducting cost-benefit analysis. Table 6-1 provides an explanation for the different types of costs recommended by the Microsoft document (Microsoft 2006, pp.89-90).

**Table 6-1 Microsoft detailed new or enhanced control costs**

<b>Cost Type</b>		<b>Explanation</b>
<b>1</b>	<b>Acquisition</b>	Software, hardware or services related to a proposed new control.
<b>2</b>	<b>Implementation</b>	For staff or consultants who will install and configure the proposed new control.
<b>3</b>	<b>Ongoing</b>	Relates to continuing activities associated with the new control such as management, monitoring and maintenance.
<b>4</b>	<b>Communication</b>	Relates to communicating new policies or procedures to users.
<b>5</b>	<b>Training for IT Staff</b>	Associated with the IT staff that would need to implement, manage, monitor and maintain the new control.
<b>6</b>	<b>Training for Users</b>	Associated with users who would have to incorporate new behaviour in order to work with the new control.
<b>7</b>	<b>Productivity and Convenience</b>	Associated with users whose work would be impacted by the new control.
<b>8</b>	<b>Auditing and Verifying Effectiveness</b>	For ensuring that the control is actually doing what it was supposed to do.

#### **6.2.1.4 Summary**

The previous discussion revealed that all reviewed standard and professional organisations concerned with information security risk management recommend the use of economical analysis in the selection of the most appropriate protection measures for mitigating the discovered security flaws. However, enterprises wanted to manage risks based on economical analysis would be faced with a lack of indicators, rigorous methodologies and standard tools for conducting the suggested economical analysis (Liu et al. 2006; Cavusoglu et al. 2004b; Bernard 2007). Most of the above reviewed documents did not suggest standard procedures or systematic approach for developing and using financial metrics in adjusting the overall information security expenditures (Cavusoglu et al. 2004a; Tsiakis and Stephanider 2005; Anderson and Moore 2006; Johansson et al. 2006). In the paragraphs that follow, a summary is provided for the most important financial metrics that could be used in building the required cost-benefit model that will be presented later in this chapter.

## 6.2.2 Information Security Financial Metrics

There are a number of financial metrics that evolved from the information security risk management literature to assess information security risks. A brief description of each of these metrics and their related issues, as shown in Table 6-2, will be discussed in the following sections.

**Table 6-2 Information security financial metrics**

Metric/Symbol		Way of Calculation / Source	
a	Annual Loss Expected (ALE)	$ALE = \sum_{i=1}^n I(O_i)F_i$	$I(O_i)$ the impact of outcome $i$ in monetary value and $F_i$ the frequency of outcome $i$
		(Campbell et al. 1997; Hoo 2000)	
b	Return on Investment (ROI)	$ROI = \frac{Benefit}{(cost - of - safeguards)}$	
		(Tsiakis and Stephanides 2005; Anderson and Moore 2006).	
c	Return on Security Investments (ROSI)	$ROSI = \frac{(RiskExposur * \%RiskMitigated) - SolutionCost}{SolutionCost}$	
		(Purser 2004; Sonnrtrivh et al. 2006)	
d	Net Present Value (NPV)	$NPV = \frac{R_t}{(1+i)^t}$	$t$ is the time of the cash flow $i$ is the discount rate $R_t$ is the net cash flow
		(Tsiakis and Stephanides 2005; Anderson and Moore 2006)	
e	Internal Rate of Return (IRR)	$C_0 = \sum_{t=0}^n \frac{B_t - C_t}{(1+IRR)^t}$	$C_0$ is the initial cost of an investment $C_t$ respective cost in year $t$ $B_t$ respective benefit in year $t$
		(Tsiakis and Stephanides 2005; Anderson and Moore 2006).	

### 6.2.2.1 Annual Loss Expected (ALE)

In 1979, the national bureau of standards of the USA published the quantitative method for performing risk analysis known as the annual loss expectancy (FIPS PUB 65 1979). ALE metric became a common measure for the risk of a harmful event, which is the product of the yearly rate of occurrence of the event times the expected loss resulting from each occurrence. The main limitation of this metric is that it cannot distinguish between high-frequency,

low-impact events and low-frequency, high-impact events. In many situations, the former may be tolerable, while the later may be catastrophic.

Gordon and Loeb (2001) suggested using an improved version of ALE metric that is modified for situations in which at most one loss will occur. Thus, the dollar cost of a loss is multiplied by the likelihood of a loss, rather than the expected frequency of loss that used to calculate ALE. The probability that a breach will occur is modelled as a function of the dollars invested in security. Their theoretical work is considered as a step forward to solve the problem of estimating the frequency of harmful events. Bodin et al. (2008) suggested solving the problem of estimating the expected frequency of loss by using three measures: the expected loss, the expected severe loss and the standard deviation of the loss instead of using one measure in the ALE method. In their method, the calculation of the expected loss is by adding the product of each loss with its respective probability. The expected severe loss is focused on the breaches that would put the survivability of the enterprise at risk, and it is calculated by adding together the product of each loss, that is greater than or equal to the specified threshold loss, with its respective probability. The standard deviation of loss represents the dispersion around the expected loss. It is computed by taking the square root of the product of squares of the deviation of each loss from the expected loss with the probability of the loss.

The calculation of the frequency of occurrence of loss is not an easy task, especially in different environments and with scarcity of the available data and its suitability to the environment under consideration. The estimations of the factors of the ALE equation, as shown in Table 6-2(a), are mainly depending

on the expert judgment and on the little published data from insurance companies, academic research and independent surveys.

#### **6.2.2.2 Return on Investment (ROI)**

The ROI metric, as shown in Table 6.2(b), measures the productivity of an investment. A company's productivity is the ratio between the total outputs and the total inputs. The total inputs being the external and internal resources used by the company to make its activity work and the total outputs being the value of the production (Tsiakis and Stephanides 2005; Anderson and Moore 2006). The ROI metric is considered in terms of finance as the most important financial indicators. It clearly indicates how well money is used. ROI also helps to determine whether it is wise to invest in a project or in something else. Mizzi (2005) emphasised the need to precisely calculate the return on information security investment. His work identified specific factors concerned with the needed security expenditures, and it also introduced related factors concerned with the viability of these expenditures.

#### **6.2.2.3 Return on Security Investment (ROSI)**

Purser (2004) suggests using an improved equation for the ROI metric used in financial arena to be more suitable for information security. The risk mitigation, when security initiatives are concerned, is considered as an important component of the ROI and it is important to include it as an explicit factor in the ROI calculation. Sonnenreich et al. (2006) suggest using an improved equation, as shown in Table 6-2(c), for calculating the ROSI. According to their equation, measuring risk exposure is conducted by investigating the loss of highly confidential information and the productivity loss associated with a security incident. They recommended doing so using a good survey and scoring system by the enterprise itself. The mitigated risk, or in other words,

the benefits of security solutions could be calculated also by evaluating risk mitigation within the context of the considered problem. In quantifying solution cost, the impact of the solution on the productivity is considered an important factor.

#### **6.2.2.4 Net Present Value (NPV)**

The NPV metric is defined as the total present value of a time series of cash flows. It is a standard method for using the time value of money in assessing the financial value of long-term projects (Anderson and Moore 2006). The NPV metric, as shown in Table 6-2(d), is an indicator of how much value an investment or project adds to the value of the enterprise. In financial theory, if there is a choice between two mutually exclusive alternatives, the one yielding the higher NPV should be selected. The problem with using NPV for security investments is that the accuracy is quite critical in obtaining comparatively meaningful results.

#### **6.2.2.5 Internal Rate of Return (IRR)**

The IRR metric is often used in order to decide in which alternative to invest. Using IRR metric, as shown in Table 6-2(e), involves calculating the investments expected return, and can be used to compare different investment alternatives. The choice might stand between investing in a machine, and simply investing the money in a bank account that gives an interest on the money (Tsiakis and Stephanides 2005; Anderson and Moore 2006). The comparison is always done by calculation of the IRR factor between different alternatives using a discount factor compared to the bank account. The outcome of the calculation should equal zero and, therefore the better of the alternatives is then likely to invest in. There is no one perfect discount factor, and therefore different companies use different discount factors as they

believe it fits their enterprise and investment best suit their context. The IRR metric is considered as an indicator of the efficiency or quality of an investment, as opposed to NPV, which indicates value or magnitude.

#### **6.2.2.6 Summary**

In spite of the importance of each of the above financial metrics in assessing the information security expenditures, each one of them cannot work alone in producing reasonable results. Bojanc and Jerman-Blazic (2008) concluded that each of the previous metrics (ROI, NPV and IRR) has its benefits, and for producing better results they should be used together. In this respect a new approach is needed for addressing the financial considerations in dealing with information security expenditures.

#### **6.2.3 Cost-Benefit Analysis**

Cost-benefit analysis is a technique for comparatively assessing the costs and benefits of an activity or project over a relevant time period. It may also be defined as the process of comparing the various costs of acquiring and implementing an information security system with the benefits which the enterprise derives from the use of the system (Roper 1999; Tipton and Krause 2010). The cost-benefit analysis is generally developed to build a business case for the use of a particular technology solution by comparing the investment amount, net benefit, return on investment and cost effectiveness.

Hoo (2000) provides a traditional decision analytic framework to evaluate different IT security policies based on cost-benefit trade-off. The framework considers not only the costs of security controls and expected loss from security breaches, but also takes care of the additional profits expected from new opportunities. There is clear limitation to the applicability of this model.



This model overstates the reduction in risk resulting from the use of safeguards that act as substitutes for each other. In addition, the model fails to capture the effects of complimentary safeguards. Finally, the model leaves an open question of how to forecast the rate at which loss events will occur, and how to forecast the reductions in these rates that will result from adding safeguards. Instead, the methodology of the model requires, as its input, the fractional reduction in security breaches that can be expected from implementing each of the safeguards under consideration.

Gordon and Loeb (2001) suggested an economical model for the evaluation of information security investment based upon cost benefit technique. In their model, three quantities are identified: the total benefits of implementation of information security infrastructure 'B', the total cost of that implementation 'C' and different levels of information security 'S'. The goal is to determine the point where the gain denoted as 'G', related to 'S' is maximum. From mathematical point of view that point can be found by differentiating the related equation and making it equal to zero.

Butler (2002) summarises the results of using a cost-benefit analysis method called Security Attribute Evaluation Method (SAEM) to compare alternative security design in financial and accounting information system. The case study presented in his paper starts with a multi-attribute risk assessment that results in a prioritised list of risks. Security specialists estimate countermeasure benefits, and how the enterprise's risk is reduced. Using SAEM, security design alternatives are compared with the enterprise's current selection of security technologies to see if a more cost-effective solution is possible.

## **6.3 Information Security Economical Analysis**

The previous sections present a review of the recent literature in the subject. This review shows a gap that exists in the current research regarding the absence of a generic practical model for assessing the cost of the protection measures versus the benefit from applying these measures in reducing or eliminating the discovered risk. For addressing this problem, the following sections start by introducing the common technologies and management practices that are used by enterprises for mitigating the discovered information security risks. Second, the proposed model for information security cost-benefit analysis is presented. In this respect, the following sections will address the answers to the following three main related questions:

- How to protect the important asset of information in IT-based applications;
- how much information security is enough for such applications; and
- how to evaluate the resulting security benefits.

These questions given above, and of course their answers are of interrelated nature. They collectively provide a background for the target cost-benefit model for information security context.

### **6.3.1 Protection of Information**

The question of how to protect information in IT-based applications has been answered by professional organisations concerned with IT. They produced information security products including: firewalls, Intrusion Detection Systems (IDS), antivirus programmes, cryptographic techniques and other security products and tools. These tools increased very fast and became very sophisticated and powerful in providing different levels of protection to security

challenges. Venter and Eloff (2003) introduce taxonomy of the most used technologies by enterprises in controlling risk. These technologies are divided into two groups, proactive and reactive. Each of these groups has three layers of security technologies, network layer, host layer and application layer.

Table 6-3 gives related data from the annual computer crime and security survey of the computer security institute (CSI 2007). The data shows that the most frequently used information protection tools by enterprises, depending on information technology systems in their business, for the years 2006 and 2007.

**Table 6-3 Protection tools and their use according to the annual computer crime and security survey (CSI 2007)**

Seq.	Security Technologies	Percent Used (%)	
		2006	2007
1	Anti-virus software	97	98
2	Firewall	98	97
3	VPN (Virtual Private Network)	--	84
4	Anti-Spyware software	79	80
5	Intrusion detection system	69	69
6	Encryption for data in transit	63	66
7	Vulnerability/ patch management	--	63
8	Server-based access control list	70	56
9	Static account login / password	46	51
10	Encryption for data in storage	48	47
11	Intrusion prevention system	43	47
12	Application-level firewall	39	45
13	Log management software	41	44
14	Forensics tools	38	40
15	Smart card/one-time password token	38	35
16	Public key infrastructure	36	32
17	Specialised wireless security system	32	28
18	Endpoint security client software	31	27
19	Biometrics	20	18
20	Other	4	4

### 6.3.2 Required Protection

The question of how much security is enough has been addressed by national and international organisations concerned with IT risk management and information security management standards, as shown in Chapter 2. These organisations provided risk management methods and information security

management standards that recommend the use of various management rules and technical tools for the protection of information security. These recommendations usually provide common, or just enough security protection practices and not necessarily best possible practices. The ISO/IEC 27002 information security management standard is considered as one of the most important examples. Other examples of related standards are given in chapter 2. Chapter 5 presents an approach for enterprise information security readiness assessment that could be used to share in answering the above question.

### **6.3.3 Evaluation of Information Security Benefits**

The question of the evaluation of security benefits is of an economic nature. Such benefits usually come as a result of investment, where cost is the major factor. Different researchers have addressed this problem with various considerations. The Incident Cost Analysis Modelling Project (I-CAMP) is an early example in applying the Cost Benefit Analysis (CBA) in computer security (Mercuri 2003). The model was developed by the big ten universities during the 1990s. The model is appropriate for situations where the related usage losses are considered to be modest or ignored entirely. Xie and Mead (2004) investigated the System Quality Requirements Engineering (SQUARE) model and applied the cost-benefit analysis framework for information security improvement in small companies.

Anderson and Choobineh (2008) provided an extensive discussion of the cost and benefits of information security in enterprises. The discussion explored various factors concerned with the development of enterprise information security strategies. This is useful in highlighting what should be taken into

account in conducting cost-benefit analysis from which an information security strategy can be developed.

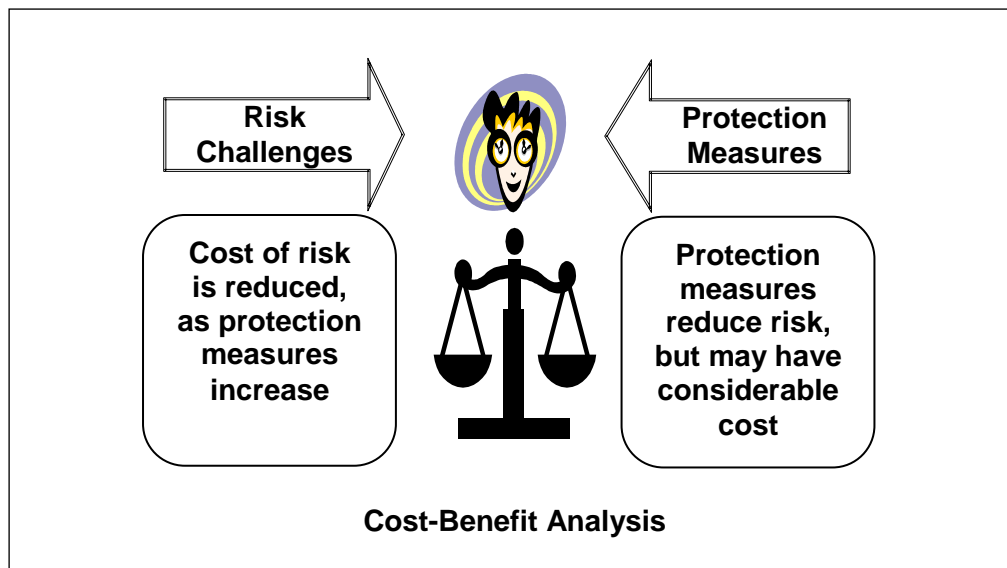
#### **6.3.4 Summary**

The above discussion shows that information security protection tools are not only available, but they are also in practical use (CSI 2007; Khadraoui and Hermann 2007; Brotby 2009); standards for guiding the implementation of the security protection measures exist (ISO/IEC 2005; BSI 2004); and evaluations of protection benefits, considering protection cost, have been addressed from different angles by different researchers (Gordon and Loeb 2002; Mizzi 2005; Anderson and Choobineh 2008). A gap exists in current research for providing a practical generic model that can be easily used as a common guide toward comprehensive cost-benefit analysis of security protection measures in different enterprises, and under different circumstances. Such a model would be able to accommodate different factors and considerations associated with the applications concerned. It would provide a wise calculating guide to the implementation of the recommendations of information security standards.

#### **6.4 The Proposed Cost-Benefit Model**

The mathematical model presented here provides practical generic tools for the cost–benefit analysis of security challenges versus protection measures. The cost of security challenges can be very high if no protection measures are provided. While such measures support reducing the security challenges and their cost, they obviously do not come without cost of their own. In some cases, where many sophisticated protection measures are used, their cost may out-weigh the savings they cause to the cost of security challenges. This

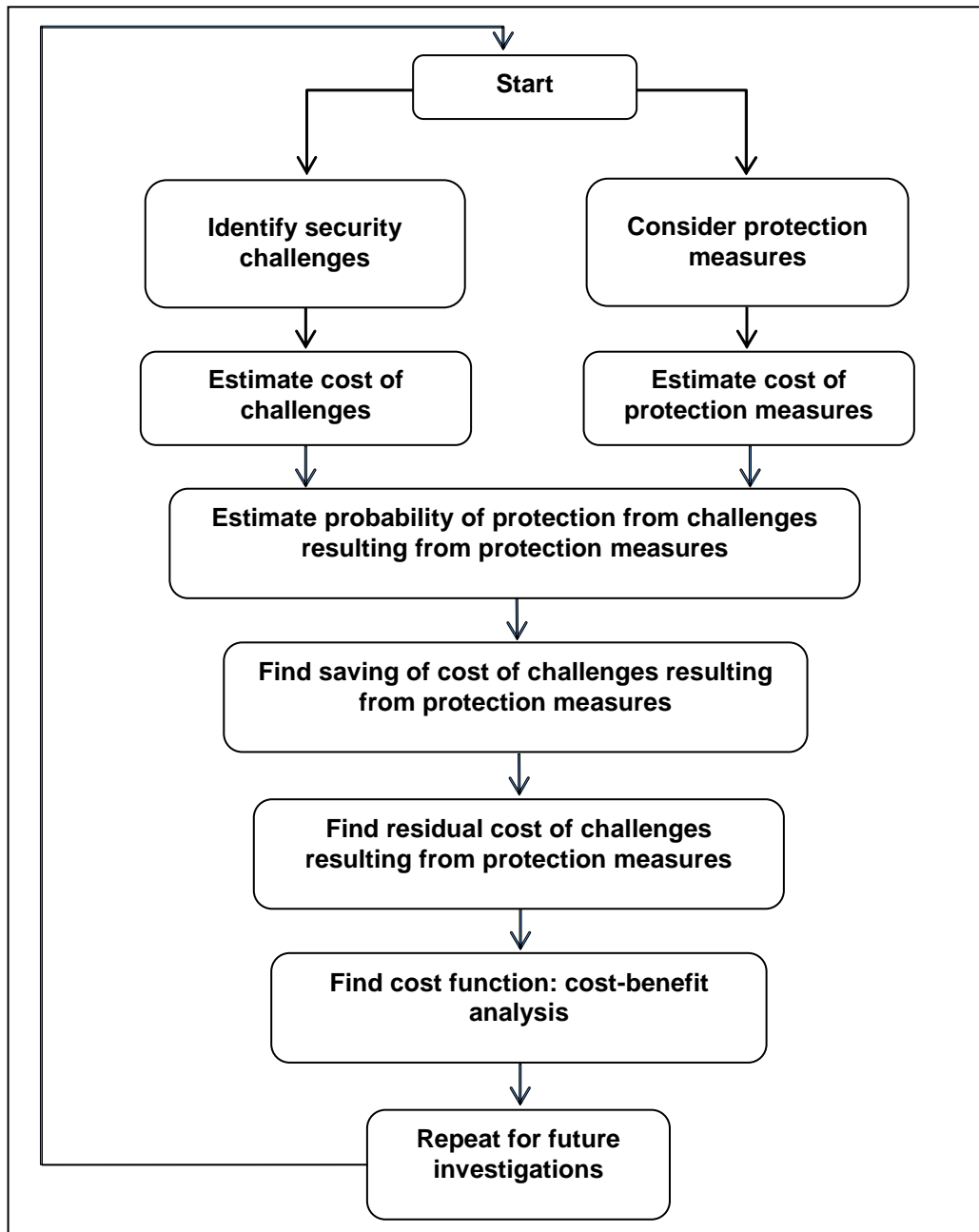
common problem is illustrated in Figure 6-1, and it is the concern of the model presented here.



**Figure 6-1 Protection measures versus security challenges: Cost-benefit analysis**

The model provides analytical tools for dealing with the cost-benefit assessment tasks illustrated in the procedure of Figure 6-2; these tasks include the following:

- Identifying the security challenges that need to be taken into account;
- specifying the protection measures that can be considered;
- estimating the actual protection resulting from the use of the protection measures;
- finding the saved cost of security challenges resulting from the use of the protection measures;
- finding the residual cost of security challenges resulting from the saving caused by the use of the protection measures; and
- finding the cost function that considers the total cost and illustrates the cost-benefit state.



**Figure 6-2 Cost-benefit analysis procedure**

The analytical tools that deal with the above tasks are described in the following sections.

### **6.4.1 Security Challenges**

Table 6-4 identifies the basic factors associated with the security challenges and their inter-relationships. The number of these challenges is considered to be a variable. For each challenge, it gives its estimated cost if it occurs and it

considers its expected annual frequency of occurrence. The same table gives the expected annual cost of each challenge and the annual cost of all challenges.

**Table 6-4 Security challenges and their cost**

Symbol	Description
<b>i</b>	Challenges index.
<b>I</b>	Number of identified challenges.
<b>G[i]</b>	Estimated cost of challenge [i] in case of occurrence.
<b>F[i]</b>	Expected frequency of challenge [i] per year.
<b>g[i]</b>	Expected cost of challenge [i] per year.
	$g[i] = F[i].G[i]$
<b>g</b>	Expected cost of all identified challenges per year.
	$g = \sum_{i=1}^{i=I} g[i]$

### 6.4.2 Protection Measures

Table 6-5 gives the basic factors concerned with the protection measures and their inter-relationships. The number of these protection measures is considered as a variable. For each measure, it addresses its annual cost. The annual total cost of all protection measures is also taken into account.

**Table 6-5 Protection measures and their cost**

Symbol	Description
<b>j</b>	Protection measures index.
<b>J</b>	Number of protection measures considered.
<b>K[j]</b>	Average cost of protection measure [j] per year.
<b>k</b>	Average cost of all identified protection measures per year: "J protection measures".
	$k = \sum_{j=1}^{j=J} K[j]$

A point of clarifications is needed here, that is the distinction between a protection measure and a protection tool. A protection tool, such as those listed in Table 6-3, can be used with different controls leading to different protection measures that result in different protection levels. For example, the anti-virus software tool may be used with or without information back-up security control leading to two different protection measures.



### 6.4.3 Resulting Protection

Of course the use of the protection measures would lead to reducing the effect of the challenges and consequently to saving their cost, partially or fully. Table 6-6 is concerned with estimating the probability of protection provided by the protection measures considered, individually and collectively, that is with regards to each identified challenge.

**Table 6-6 Protection from challenges**

Symbol	Description
$P[i, j]$	Expected probability of protection from challenge [i] due to using protection measure [j].
$p[i]$	Accumulated probability of protection from challenge [i], due to using all protection measures considered: "J protection measures".
	$p[i] = \sum_{j=1}^{j=J} P[i, j] \leq 1$

### 6.4.4 Cost Saving

Achieving a certain level of protection would lead to a certain level of saving of the cost of the challenges and, this is expressed in Table 6-7. The table considers the saving caused by each protection measure and associated with each challenge. The accumulated savings are also taken into account.

**Table 6-7 Saving of challenges cost**

Symbol	Description
$S[i, j]$	Cost saving from cost of challenge [i], due to using protection measure [j].
	$S[i, j] = g[i].p[i, j]$
$s[i]$	Cost saving from cost of challenge [i], due to using all protection measures considered: "J protection measures".
	$s[i] = g[i].p[i]$
$s$	Total cost saving of all identified challenges "I challenges", due to using all protection measures considered: "J protection measures".
	$s = \sum_{i=1}^{i=I} s[i]$

### 6.4.5 Residual Cost

As shown above, protection measures cannot fully eliminate challenges. Therefore, the challenges will keep certain residual cost, and this is addressed in Table 6-8. Various residual costs are given in the same table, both individually and collectively.

**Table 6-8 Residual cost of challenges**

Symbol	Description
R[i,j]	Residual cost of challenge [i], due to using protection measure [j].
	$R[i, j] = g[i].(1 - p[i, j])$
r[i]	Residual cost of challenge [i], due to using all protection measures considered: "J protection measures".
	$r[i] = g[i].(1 - p[i])$
r	Total residual cost of all identified challenges "I challenges", due to using all protection measures considered: "J protection measures".
	$r = \sum_{i=1}^{i=I} r[i]$

### 6.4.6 Cost Function

From the above analysis, cost functions can be developed at different levels. A cost function would combine the cost of the protection measures with the residual cost of the challenges. This can be viewed at each protection measure and challenge level and can also go up to the overall level of all protection measures and challenges, as given in Table 6-9.

The analytical tools given above are of comprehensive nature, and can be applied to a wide variety of case-studies. Their practical application, considering different challenges and protection measures, would provide an insight into the state of cost under different circumstances. Of course minimum value for the overall cost function is desired, but this would also depend on the policy and objectives of the concerned enterprise.

**Table 6-9 Cost functions: challenges with protection**

<b>Symbol</b>	<b>Description</b>
<b>C[i,j]</b>	Cost of protection measure [j], combined with the residual cost of challenge [i], due to using the protection measure.
	$C[i, j] = k[j] + r[i, j]$
<b>c[i]</b>	Cost of all protection measures considered “J protection measures”, combined with the residual cost of challenge [i], due to using these protection measure.
	$c[i] = k + r[i]$
<b>c</b>	Cost of all protection measures considered “J protection measures”, combined with the residual cost of identified challenges “I identified challenges”, due to using these protection measures.
	$c = k + r$

A real illustrative example of the application of the above cost-benefit model that considers the available protection tools and recommendations associated with ISO standards will be presented later in Chapter 7.

## **6.5 Summary**

Chapter 6 aims to develop a practical model for economical analysis of information security investments that enterprises can use as guidance when applying the recommended risk mitigation plans. Chapter 6 presents a review of the standard organisation economical directions. In addition, the economical metrics associated with enterprises information security risk management are also presented. Finally, an approach is then presented based on an economical analytical model that enables the assessment of the necessary investment in the recommended information security. This model would be useful for both information security professionals and researchers in assessing the cost of the security measures versus the benefit of these measures in reducing the identified information security challenges.

**PART IV**  
**APPLICATIONS**

**Chapter 7 EVALUATION CASE STUDIES**

# Chapter 7

## EVALUATION CASE STUDIES

### 7.1 Introduction

In this chapter, evaluation case studies are presented for investigating information security readiness of nine well-established business enterprises working in different fields in the Kingdom of Saudi Arabia (KSA). The main objective is to investigate the information security readiness of these enterprises and consequently validate the developed information security assessment model, therefore providing a valid and reliable tool that can be used by enterprises in numerically assessing their information security readiness with regards to the security requirements of the ISO/IEC 27002 information security management standard. Chapter 7, therefore contributes, in addressing the fifth research question by illustrating the practical use of the developed analytical models in investigating the current state information security readiness of the participated Saudi enterprises, and in evaluating the most economical security solutions.

### 7.2 The Collected Data

This research was supposed to collect data from several Saudi enterprises to have an overall view of the effective use of each of the assigned 283 ISO/IEC 27002 security protection measures presented in Chapter 4. A website was developed and an investigation form was prepared in Chapter 5 and presented in Appendix A for collecting the required data. In addition, the investigation

form was sent by email to more than 100 business enterprises inside Saudi Arabia. Due to the sensitivity of the subject, the response to the website and to the mailed investigation form was very weak. Therefore, the decision was taken to use the triangulation technique (the use of multiple methods) in collecting the required data, and to limit the number of investigated enterprises to nine only.

Using two or more methods for data collection is called triangulation or multi-method approach, which is believed to achieve a greater understanding and grasp of the real world. Denzin (1978) explains that triangulation is an approach in which multiple observers, theoretical properties, sources of data and methodologies are combined. Patton (1990) argues that studies which use only one method are more susceptible to error linked to that particular method. Bryman (1995) claims that each of the qualitative and quantitative data collection methods has several features which can be regarded as advantages or disadvantages and by using triangulation, the validity of conclusions are enhanced.

Considering the number of assigned information security measures (283) and the several visits to each of the nine investigated Saudi enterprises for collecting the required data, so limiting the number of investigated enterprises to nine only satisfies the research objectives at this stage. The main objective of this research was devoted for exploring the applicability of the developed theoretical model for assessing enterprises' information security readiness in real world. In addition, the collected data about the effective use of the assigned 283 ISO/IEC 27002 information security measures would provide a picture of the practical use of the ISO/IEC 27002 information security management standard inside Saudi Arabia. This will help in evaluating the

approach presented in the thesis from one hand, and in recommending means for improving information security management practices inside these enterprises from the other hand.

### **7.2.1 The Concerned Enterprises**

The enterprises considered in this research study include two banks, three governmental enterprises and four private enterprises. The choice of these enterprises was based on the following main requirements:

- Management was willing to discuss in an open manner the information security aspects as a part of this research study;
- management was agreeable to conduct a security review of the enterprise's current practices and procedures by the researcher;
- information security managers, employees and users were agreed by the top management to be interviewed by the researcher;
- management provided all written documentation requested to support the research including policies, procedures, job descriptions, etc..; and
- the selected enterprise was depending mainly on the information systems in conducting its business objectives with a minimum of 100 employees.

It is considered that when an enterprise meets the above requirements, this provide an indication that the investigation of its information security readiness will gain some success.

### **7.2.2 Data Collection**

The information security officer, information technology personnel, head of IT administration, programme management officer, data governance officer, risk and compliance officer, information security consultants, a human resources representative, risk and security personnel, deployment teams, training

department, service managers, service desk/incident managers, a marketing or communication representative, an internal auditor, as well as general computer users were some of the enterprises' employees who took part in responding to the investigation form. Each of these individuals interacts with information security and is being involved in management, implementation, communication and compliance.

A number of interviews with the above stakeholders were carried out to collect the required data. Written material was consulted, including documents, policies and reports. Observation of practices was performed on site for each studied enterprise. In most of the cases, collection of data involved numerous visits to the site and observation of activities on several occasions.

The effectiveness of each 283 information security measures was rated between zero and four (in Likert style), according to how extensively the measure was used effectively by the enterprise according to the scale presented in Table 5-1. A rating of zero indicated that the information security measure was absent or not used, and a rating of four denoted that the measure was implemented effectively, documented, constantly monitored and regularly improved.

The final ratings, assigned for the effective use of information security measures and the occurrence of security problems, were jointly decided by the researcher and the managers at each enterprise. This necessitated discussion and agreement upon appropriate ratings based upon the information gathered. Consistency across cases was also considered by the researcher in the final assignment of ratings.



## **7.3 General Enterprises Information**

In the following, the investigated enterprises are introduced. Then, in order to give a complete picture of the investigated enterprises, a number of general variables about these enterprises are also collected. These variables were categorised in two groups namely, the business profile and the personal profile as discussed before in Chapter 5.

### **7.3.1 The Investigated Enterprises**

In this research study, the decision was taken to not publish the individual enterprises' names so as to protect the confidentiality of the participated enterprises. Therefore, the nine enterprises are ordered from E1 to E9. In addition, these enterprises were arranged into three groups (from group A to group C). Each group has common features and represents a specific type of business as follows:

- Group "A" includes two banks, "E2 and E9". This group is for financial sector and it represents the state of security inside banks.
- Group "B" includes three governmental enterprises, "E4, E7, and E8". This group represents the public sector.
- Group "C" includes four business companies of, "E1, E3, E5, and E6" and it represents the private sector which includes business companies working in different fields.

#### **7.3.1.1 Group "A": Banks**

This group contains two financial enterprises, E2 and E9. The first enterprise, E2, is a bank which commenced business on February 2, 1980. This bank operates through its 113 branches & 12 women sections, plus 1 branch in London, UK since 1991. This bank plays a pivotal role in serving the Saudi

economy, making a steady progress over the past years in different areas of banking. To enrich the customers' experience, the bank offers a variety of innovative new products through an expanded retail network.

The second enterprise E9 has been playing a crucial role in the consolidation and development of the financial system at Saudi Arabia. At the time of its establishment, the country did not have a monetary system exclusively of its own. Foreign currencies circulated in the country as a medium of exchange, along with silver coins. The bank notes had not yet been issued. There were no banks in existence and the banking business was being conducted by foreign bank branches. One of the foremost tasks of this enterprise in its early stage was the development of a national currency. This enterprise also considered the need for promoting the growth of a national banking system. From 1960 to 1972, this enterprise focused on banking regulations against the background of expanding banking business and the country's acceptance of full convertibility of the national currency. From mid 1980s, the enterprise priorities were to introduce financial market reforms. Over the years, with the growth of the economy and expansion of the financial system, the enterprise responsibilities have increased.

#### **7.3.1.2 Group "B": Governmental Enterprises**

This group contains three enterprises E4, E7 and E8. These enterprises will represent the governmental or public sector in this research study. The first enterprise, E4, in this group is considered as a very critical governmental enterprise, supporting IT technology inside Saudi Arabia.

The ruler of the KSA established the general directory of the second enterprise E7 in 1926. Four years later, a royal decree was issued to change this

enterprise to a ministry. It was the first ministry to be announced in the government. Upon the establishment of the general directorate of foreign affairs, there were no diplomatic missions abroad. In 1936, the number of the country diplomatic missions abroad increased to five (three missions in London, Baghdad and Cairo, in addition to two consulates in Swiss and Damascus). In the year 1951, the number of branches of this enterprise increased to 18 in 16 different countries. This expansion in the international relations is in line with the development of this enterprise. This includes the restructuring of the enterprise and its administrative team in order to enable them to fulfil their duties accordingly.

The third enterprise E8 is an independent scientific enterprise of the government, established in 1977. This enterprise is governed by a supreme committee, which is chaired by the Prime Minister and is composed of the ministers of the major ministries to which science and technology are of greatest relevance as follows: to be a world-class research enterprise vital to the country's future and a vital source of science & technology for national societal mission, that combines technology with human needs. From its inception in 1977, it had been carrying out its mission in the promotion of science & technology in the country. This is achieved by coordinating and cooperating with various universities, agencies and institutions concerned with research and technology. It is also concentrated on encouraging experts to undertake research that will help promote the development and evolution of the society.

### **7.3.1.3 Group “C”: Business Companies**

This group contains four enterprises E1, E3, E5 and E6. These enterprises will represent the private sector in this research study. The first enterprise, E1, is a business company that runs a series of restaurants, located in heart of Riyadh, which opened its door in February 1992.

The second enterprise, E3, is a technology company which is one of the leading IT infrastructure solutions providers in the country. It is well positioned to lead the IT service industry in the Middle East by leveraging its strategic partnerships with world class technology vendors, solid service infrastructure and its commitment to the region. This enterprise concentrated on the mission of enabling the best business results through ideas, people and technology. As a total IT infrastructure solutions provider, the company provides a full spectrum of services that includes consulting, design, implementation, integration and a whole host of outsourcing services. In short, this company addresses the entire cycle of a typical IT that include consult, build, deploy and manage. Committed to its full-service proposition, it linked itself with strong alliances of the world's most renowned technology companies including Cisco, HP, Oracle, Veritas, Computer Associates, Microsoft, Symantec, Spirent, Redline Communications, CommScope - to provide the most effective and competitive solutions to their customers. Recognised for its excellent service, quality and business performance, this company has been awarded several local and regional achievement recognitions: from country e-business awards as the best networking solutions company in 2004, from HP as the best enterprise channel in 2003 and from Cisco the gold partner of the year award in 2004 for the region of Russia, Middle East and Africa.

The third enterprise, E5, is a telecommunication company, better known as “network company”. It has offices in the important cities inside and outside the country. This company represents global telecom vendors like Nortel, Tellabs, Polycom, SatComglobal, Nexans, Juniper Networks and many others.

The last investigated enterprise in this group, E6, is an electric company, reformed in 2000. The company helped to establish generating facilities, transmission and distribution systems and substations throughout the country. A long-term goal of this company was to increase the capacity of steam stations and desalination plants to enable them to generate half of the electricity output for the whole country.

In the following, the business profile results of the nine investigated enterprises are first discussed. The personal profile results of the main respondents to the investigation form are then introduced.

### **7.3.2 The Business Profile**

Table 7-1 provides the collected data from the nine Saudi enterprises participated in this study. The table gives full detailed features of each of the investigated enterprises including: type of business, size of enterprise, business experience and existence of information technology department. The business profile results of the participated enterprises, as shown in Table 7-1, are summarised as follows:

- The investigation form has been answered by the following business fields: 22% financial sector, 33% governmental sector and 45% private sector. This shows a good distribution that represents the main business sectors at Saudi Arabia.

**Table 7-1 “Business Profile” results of the participated enterprises**

Group/ Enterprise	Sector	Size: No. Employees	Field	Experience Months	Separate IS Dep.	IT services. Computers	
A	E2	Finance	1001 to 3000	Bank	Over 24	Yes	Over 3000
	E9	Finance	1001 to 3000	Bank	Over 24	Yes	1001 to 3000
B	E4	Public	100 to 500	Government	Over 24	No	100 to 500
	E7	Public	1001 to 3000	Government	Over 24	No	1001 to 3000
	E8	Public	501 to 1000	Government	Over 24	Yes	Less than 100
C	E1	Private	100 to 500	Food	Over 24	No	Less than 100
	E3	Private	100 to 500	IT	Over 24	Yes	100 to 500
	E5	Private	100 to 500	Communication	Over 24	Yes	100 to 500
	E6	Private	Over 3000	Electrical	Over 24	Yes	Over 3000

- All of the investigated enterprises have been in business for more than two years. This indicates that these enterprises are settled in business and have reasonable IT experience.
- 75% of the investigated enterprises have a separate information technology department. This indicates that most of these enterprises are mature and depend mainly on the information technology systems.
- 45% of the investigated enterprises are large companies “from 100 to 3000 employees”. This research study mainly targets the medium and large enterprises.
- 78% of these enterprises are mainly depending on IT services (Number of computers above 100).

The results of the business profile assure that the selected enterprises achieve the main requirements set by the researcher to have a sample that represents different sectors with medium and large enterprises, reasonable IT experience and reliant mainly on IT services.

### **7.3.3 The Personal Profile**

One of the main objectives of this study was to obtain a managerial perspective about the state of information security inside the investigated enterprises. The personal profile of the main respondents to the investigation form by their level in the enterprise reflects this objective. Consequently, clear

majority of the respondents fulfil the objective of the credibility of the collected data. It is also worth to mention here that the investigation form was answered under the direction of the stated person in Table 7-2, and for each TOPE domain, a number of employees according to their expertise in the investigated domain are also involved in answering the sub-questions of the investigation form. This assures the benefit of the categorisation of the information security measures in four specific domains.

Table 7-2 provides the collected personal information of the respondents to the investigation form. It gives full details of the characteristics of the main person responsible for providing the data including: position, nationality, age, degree, field of study, special IS qualifications and experience. The personal profile results of the respondents to the investigation form, as shown in Table 7-2, are summarised as follows:

- 60% of the main respondents are at manager level. Consequently, the majority of respondents fulfil managerial roles in their enterprises.

**Table 7-2 “Personal Profile” of the respondents to the investigation form**

Group/ Enterprise	Position	Nationality	Age: year	Degree	Field of Study	Special Qual.	Experience Months	
A	E2	IT Manager	Saudi	25-40	Bachelor	Business	CISSP CIW	13-18
	E9	IS Manager	Saudi	25-40	Master	Computer Science& Business	N/A	Over 25
B	E4	IT Manager	Saudi	25-40	Master	Computer Science	N/A	Over 25
	E7	Telecom Manager	Saudi	25-40	Master	Engineering	N/A	19-24
	E8	IS Manager	Saudi	25-40	Bachelor	Computer Science	CISSP SANS M5	Over 25
C	E1	IT Manager	Non-Saudi	25-40	Bachelor	Computer Science	N/A	Over 25
	E3	Network Engineer	Saudi	25-40	Bachelor	Engineering	N/A	19-24
	E5	System Engineer	Non-Saudi	25-40	Master	Engineering	N/A	Over 25
	E6	IS Engineer	Saudi	25-40	Bachelor	Engineering	N/A	19-24

- 50% have an engineering background, and the rest have a degree in computer science.
- 80% are Saudi, and their age is between 25 and 40 years.
- 50% of the respondents have a Master degree, and 20% have Special Qualification (SQ) on IT. This indicates that more than 70% of the respondents are IT professionals which reflect on the credibility of the results.
- 50% of the respondents have more than 2 years experience in information security and information technology.
- Most of the respondents have no special information security certificates. This indicates that the interest in information security is still not considered as a major concern in the investigated enterprises.

## **7.4 Data Analysis and Findings**

In the following sections, the collected information security assessment data from the investigated enterprises will be analysed and presented. The obtained results provide important numerical and graphical information which illustrates the strengths and weaknesses of each enterprise with regards to ISO/IEC 27002 security controls, objectives and clauses.

### **7.4.1 Level-1 Assessment Results**

According to the gradual approach presented in Chapter 4, the assessment of the participated enterprises has three levels. Level-1 assessment includes the information security controls which is considered by the ISO/IEC 27002 standard as common and essential for any enterprise. In this regard, the assessment starts with the ISO/IEC 27002 specified essential security controls concerned with legislative issues. This is followed by the investigation of the



security controls considered as common practice for information security (ISO/IEC 27002 2005, pp.x.). In the following sections, the existence of these controls is checked and presented before the numerical assessment that will be presented later in level-2 assessment. The assessment results indicate the awareness degree inside these enterprises about the importance of the priority in applying the ISO/IEC 27002 information security protection controls.

**7.4.1.1 Essential ISO/IEC 27002 Controls**

The investigation results of the controls, considered by the ISO/IEC 27002 standard as essential to an enterprise from a legislative point of view, are given in Table 7-3. An inclusion tick (√) is used to indicate whether the concerned control is applied in the investigated enterprise. These controls apply to most enterprises and any environments as stated by the ISO/IEC 27002 standard.

**Table 7-3 Level-1 assessment results of ISO/IEC 27002 essential controls**

Essential ISO/IEC 27002 Controls		Enterprise								
		A		B			C			
		E2	E9	E4	E7	E8	E1	E3	E5	E6
1	Data protection and privacy according to requirements.	√	√			√		√	√	√
2	Protection of organisational important records.	√				√		√	√	√
3	Implementing technical procedures that ensure compliance.	√	√			√		√		√

**7.4.1.2 Common ISO/IEC 27002 Controls**

The investigation results of the ISO/IEC 27002 controls, which are considered common to all enterprises, are given in Table 7-4. An inclusion tick (√) is also used here to indicate whether the concerned control is applied in the investigated enterprise.

**7.4.1.3 Summary**

Tables 7-3 and 7-4 show that only five of the investigated enterprises E2, E9, E3, E5 and E6 scored more than 90% in the implementation of the 19 security

controls which are considered as essential and common for the success of the implementation of the information security management system inside enterprises. One enterprise E4 achieved 43% of these controls, while both of E7 and E8 scored 56%. Finally, E1 scored only 21% of these controls.

**Table 7-4 Level-1 assessment results of ISO/IEC 27002 common controls**

Common ISO/IEC 27002 Controls		Enterprise								
		A		B			C			
		E2	E9	E4	E7	E8	E1	E3	E5	E6
1	ISP approved by management and published.	√	√		√	√		√	√	√
2	All information security responsibilities should be clearly defined.	√	√	√	√	√		√		√
3	Employees should receive appropriate awareness and training with regular updates.	√	√	√	√	√	√	√		√
4	Input data to applications validated.	√	√	√	√	√		√	√	√
5	Validation checks incorporated into applications.	√	√	√	√	√		√	√	√
6	Message integrity in applications ensured.	√	√	√	√	√		√	√	√
7	Output data from applications validated.		√		√	√		√	√	√
8	Protection against technical vulnerabilities.	√	√	√	√	√		√	√	√
9	Management process addressing information security requirements for business continuity.	√	√					√	√	√
10	Business Impact Analysis carried out to identify the events that can cause interruptions.	√	√					√	√	√
11	Plans to restore operation and information at the required level and in the required time scale developed.	√	√	√				√		√
12	Business continuity plans have a consistent framework addressing security requirements and a priority for testing and maintenance.	√	√			√		√	√	√
13	Regular programme for testing and updating the Business Continuity Process.	√	√				√	√	√	√
14	Quick and effective response procedures.	√	√		√		√	√	√	√
15	Mechanisms to quantify and monitor security incidents: according to type, volume and cost.		√		√		√	√		√
16	Incidents collected, retained and presented on to Jurisdiction.	√						√		√

There is a common problem which appeared in most of the investigated enterprises that according to the ISO/IEC 27002 standard, the 19 security controls appeared in Tables 7-3 and 7-4 are considered essential and common controls for any enterprise of any type, size and scale. Therefore, enterprises should achieve a high score (of 100%) in implementing these security controls

and this is not achieved in most of the investigated enterprises. These results indicate the weaknesses of these enterprises in understanding the main role of the priority in applying the information security protection measures, according to the ISO/IEC 27002 standard.

#### **7.4.2 Level-2 Assessment Results**

In the following, a comparison between three enterprises representing the three groups of the financial, public and private sectors will be introduced. The s-readiness assessment results are then presented with comments on information security weaknesses of each enterprise considering the TOPE domains and their associated ISO/IEC 27002 clauses, objectives, controls and measures. The detailed assessment result of one case study, E9, is presented in Appendix B as an example. The detailed calculations and assessment results of the nine enterprises are presented in Appendix C.

##### **7.4.2.1 Assessment Results Across the Groups**

This section uses the approach presented in Chapter 5 to present practical numerical s-readiness assessment results concerned with three Saudi enterprises participated in this research study. The chosen enterprises, presented in the following, are associated with different sectors. The enterprises considered including a bank, a government enterprise and a private company that represent the identified groups A, B and C respectively. The case studies given below demonstrate the use of the approach presented in the thesis and provide detailed results of the concerned enterprises.

##### **The Enterprises Considered**

The enterprises considered include: a Saudi bank, E9, which represents the financial sector “group A”; a Saudi governmental enterprise, E7, which represents the public sector “group B”; and a Saudi company, E5, which

represents the private sector “group C”. The three enterprises have the following features:

- The employees of the enterprises are in the range from 1000 to 3000;
- each enterprise has a separate IT department; and
- the bank and the government enterprises have been in business for more than 30 years; while the private enterprise has only been in business for around 5 years.

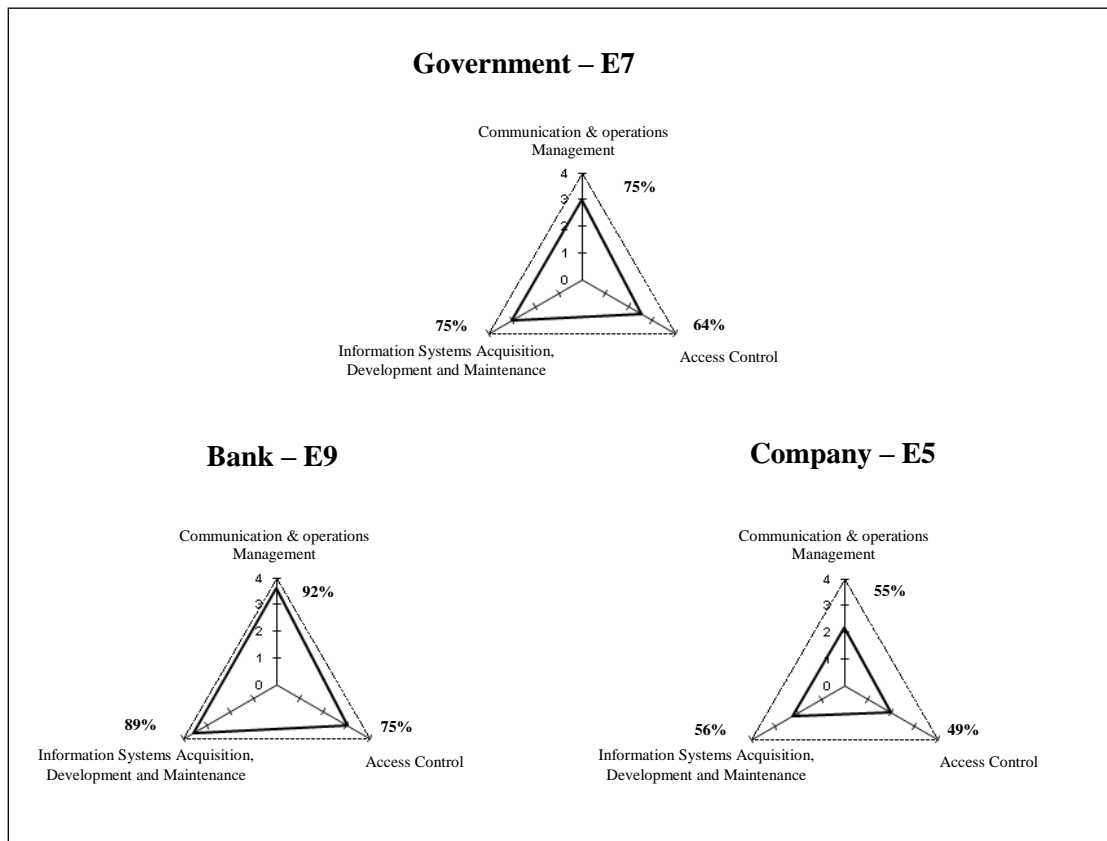
The information security managers of the bank and of the government enterprises have participated in answering the s-readiness assessment investigation form; while the IT manger of the private sector company was the one who participated in answering the investigation form. In the following sections, the information security assessment results for each of the TOPE domains will be presented.

### **The Technology Domain**

Figure 7-1 gives the results obtained for the s-readiness assessment of the ‘technology’ domain.

- The financial enterprise E9 enjoys the highest scores in this domain for the ISO clauses of “communications and operations management”: 92%, “access control”: 75%, and “information systems acquisition development and maintenance” 89%;
- the government enterprise E7 comes second; while
- the private sector enterprise E5 is last.

The overall “technology” domain, non-weighted, scores for the enterprises concerned are: 85% for the financial enterprise E9, 72% for the government enterprise E7 and 53% for the private sector enterprise E5.

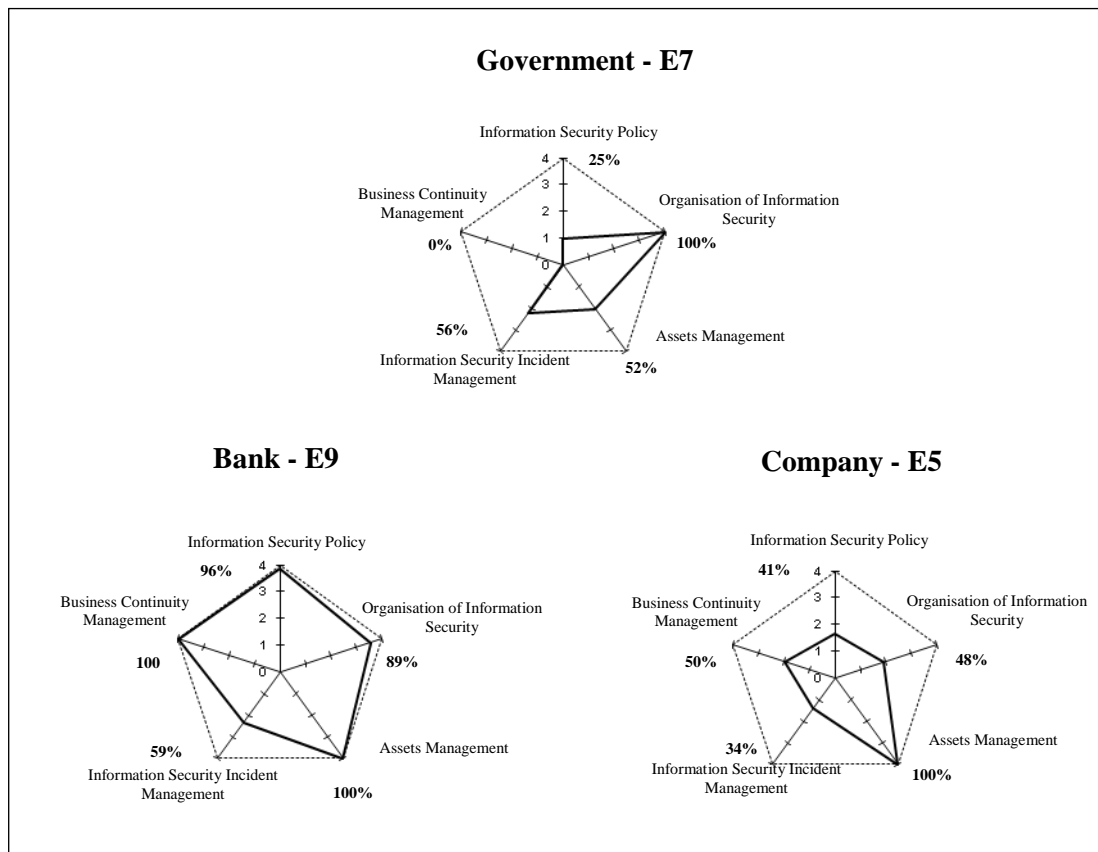


**Figure 7-1 The assessment results of E9, E7 and E5 enterprises concerned with the “Technology” domain**

### The Organisation Domain

Figure 7-2 shows the results concerned with the “organisation” domain. These results illustrate the following:

- The ISO clause of "business continuity" is at its best in the financial enterprise E9, at 100%, and at its worst in the government enterprise E7, at 0%;
- the ISO clause of "organisation of information security" is best in the government enterprise E7, at 100%, and worst in the private enterprise E5, at 48%;
- the ISO clause of "assets management" is at the same score of 100% both in the financial E9 and in the private enterprise E5, but for the government enterprise E7, it is only 52%; and



**Figure 7-2 The assessment results of E9, E7 and E5 enterprises concerned with the “Organisation” domain**

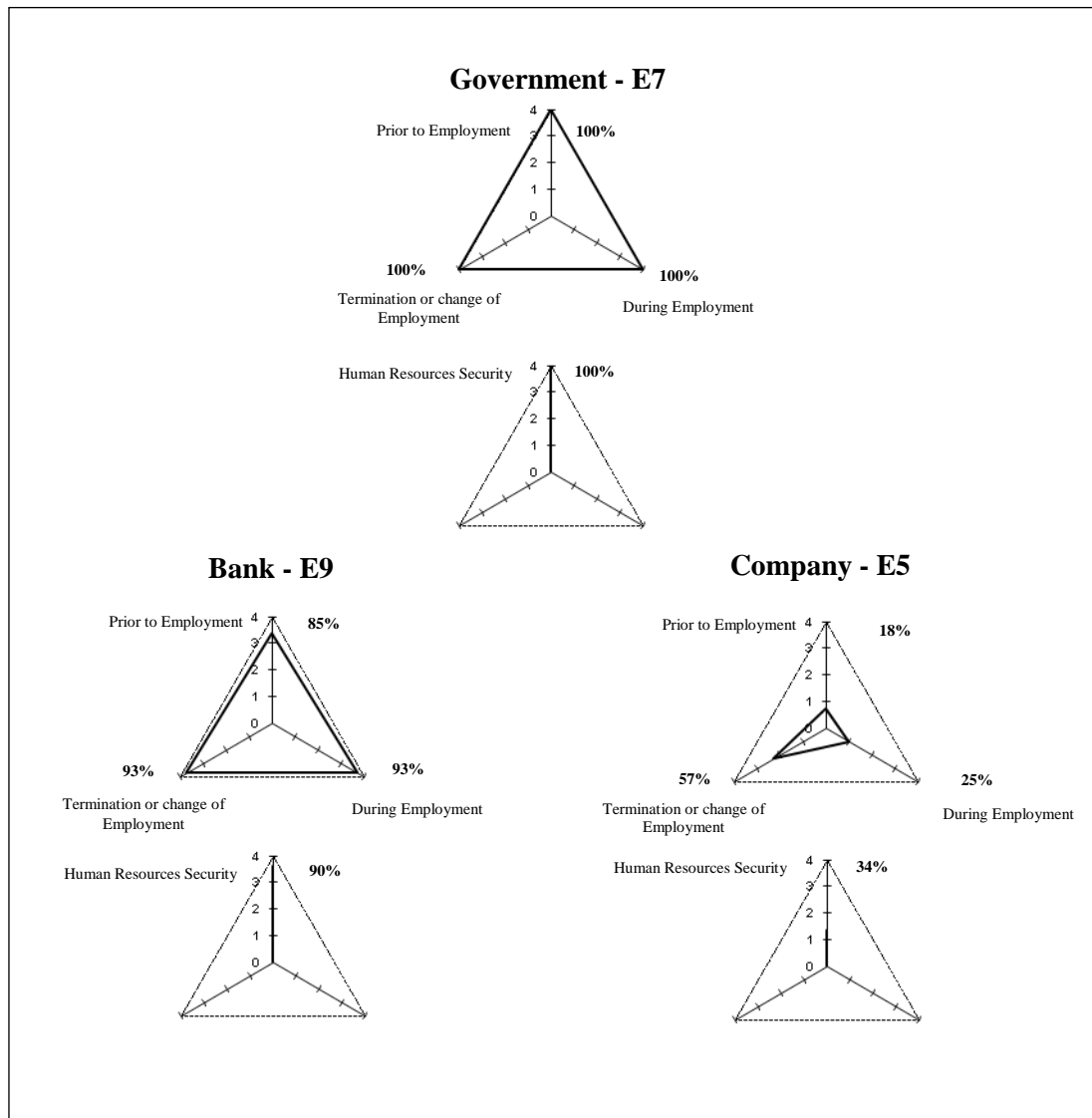
- the ISO clause of "information security incident management" is 59% in the financial enterprise E9, 56% in the government enterprise E7 and in the private enterprise E5, it is 34%.

The overall “organisation” domain, non-weighted, scores for the enterprises concerned are: 90% for the financial enterprise E9, 55% for the government enterprise E7 and 58% for the private enterprise E5.

### The People Domain

Figure 7-3 shows the results of the “people” domain at two levels (level III, and level IV) of the assessment model presented in Chapter 5. In Figure 7-3 the upper graphs illustrate the objectives level “prior to employment”, “during employment”, and “termination of employment”, and the lower graphs illustrate the clause level “human resources security”. It is generally high in financial

enterprise E9 and the governmental enterprise E7 with scores of 90%, and 100% respectively and poor for the private enterprise E5 with a score of 34%.



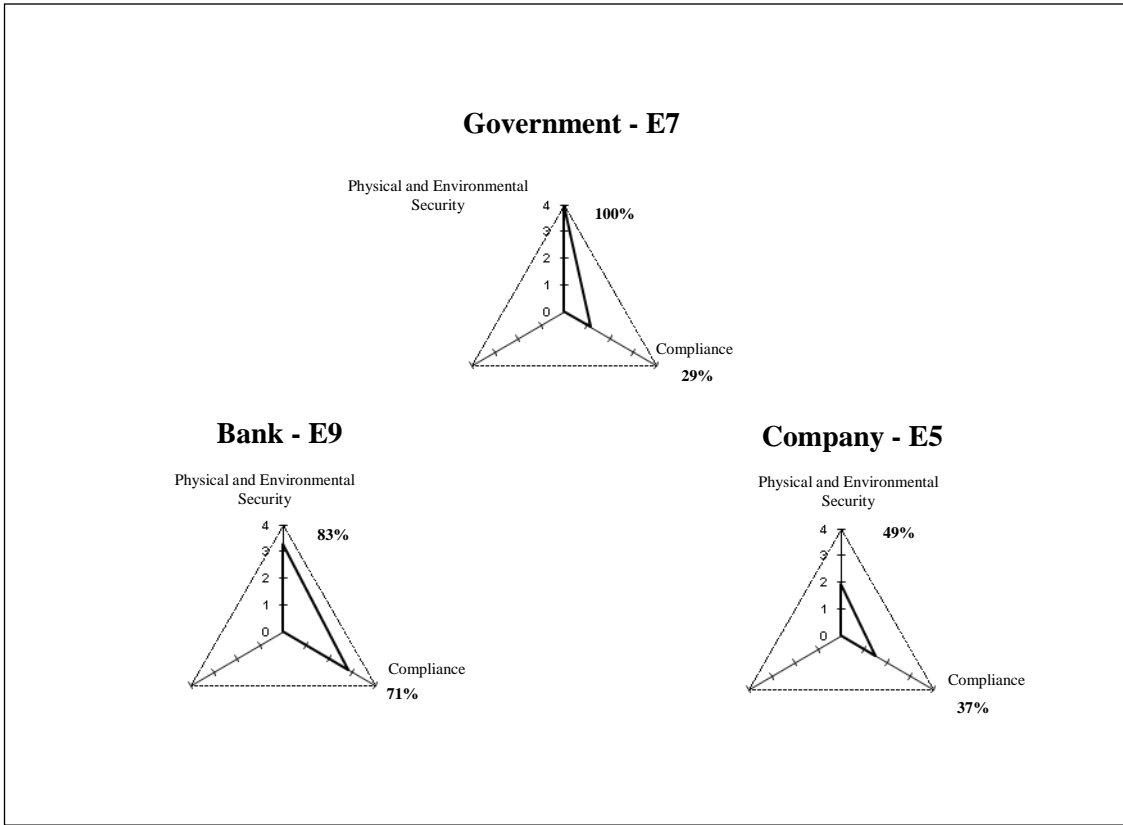
**Figure 7-3 The assessment results of E9, E7 and E5 enterprises concerned with the “People” domain**

### The Environment Domain

Figure 7-4 gives the results of the “environment” domain. The results show the following:

- The ISO clause of “physical and environmental security” reached the highest score of 100% in the government enterprise E7 while this enterprise had the least score of 29% in the ISO “compliance” clause.

The overall “environment” domain, non-weighted scores for the enterprises concerned are: 77% for the financial enterprise E9, 68% for the government enterprise E7 and 43% for the private enterprise E5.



**Figure 7-4 The assessment results of E9, E7 and E5 enterprises concerned with the “Environment” domain**

**Comparison of the Three Enterprises at the Clause Level**

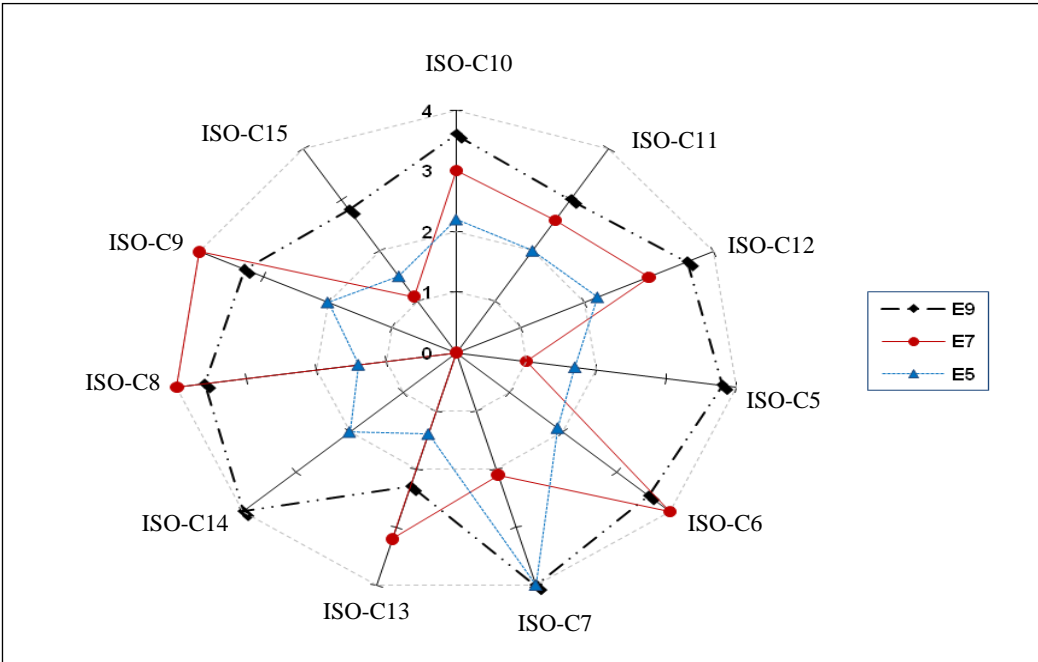
In order to assess the relative strengths and weaknesses of the three enterprises E9, E7 and E5, an analysis of how each enterprise scored on each of the eleven ISO/IEC 27002 clauses was undertaken. The performance score for each enterprise, according to the assessment model presented in Chapter 5, was computed and the results are shown in Table 7-5. The first column lists the code used for each of the eleven ISO/IEC 27002 clauses, and the second column lists the titles of each of the eleven ISO clauses. The columns from three to five list the calculated performance score. The data in Table 7-5 are shown graphically in Figure 7-5 using the radar graph. There is some



significant differences between the three enterprises. The private sector enterprise E5 has the worst scores on the majority of the eleven ISO/IEC 27002 clauses (ISO-C10, ISO-C11, ISO-C12, ISO-C6, ISO-C13, ISO-C8 and ISO-C9). The governmental sector enterprise E7 comes second and achieved the worst scores in the rest of the ISO/IEC clauses (ISO-C5, ISO-C7, ISO-C14 and ISO-C15), while the financial sector enterprise E9 has high scores in the majority of the ISO/IEC 27002 clauses.

**Table 7-5 E9, E7 and E5 scores on the ISO/IEC 27002 eleven clauses**

Code	ISO/IEC 27002 Clauses	Score (of 4)		
		E9	E7	E5
ISO-C10	Communications and Operations Management	3.6	3.0	2.2
ISO-C11	Access Control	3.0	2.6	2.0
ISO-C12	Information Systems Acquisition, Development and Maintenance	3.6	3.0	2.2
ISO-C5	Security Policy	3.8	1.0	1.7
ISO-C6	Organisation of Information Security	3.6	4.0	1.9
ISO-C7	Asset Management	4.0	2.1	4.0
ISO-C13	Information Security Incident Management	2.3	3.2	1.4
ISO-C14	Business Continuity Management	4.0	0.0	2.0
ISO-C8	Human Resources Security	3.6	4.0	1.4
ISO-C9	Physical and Environmental Security	3.3	4.0	2.0
ISO-C15	Compliance	2.8	1.1	1.5



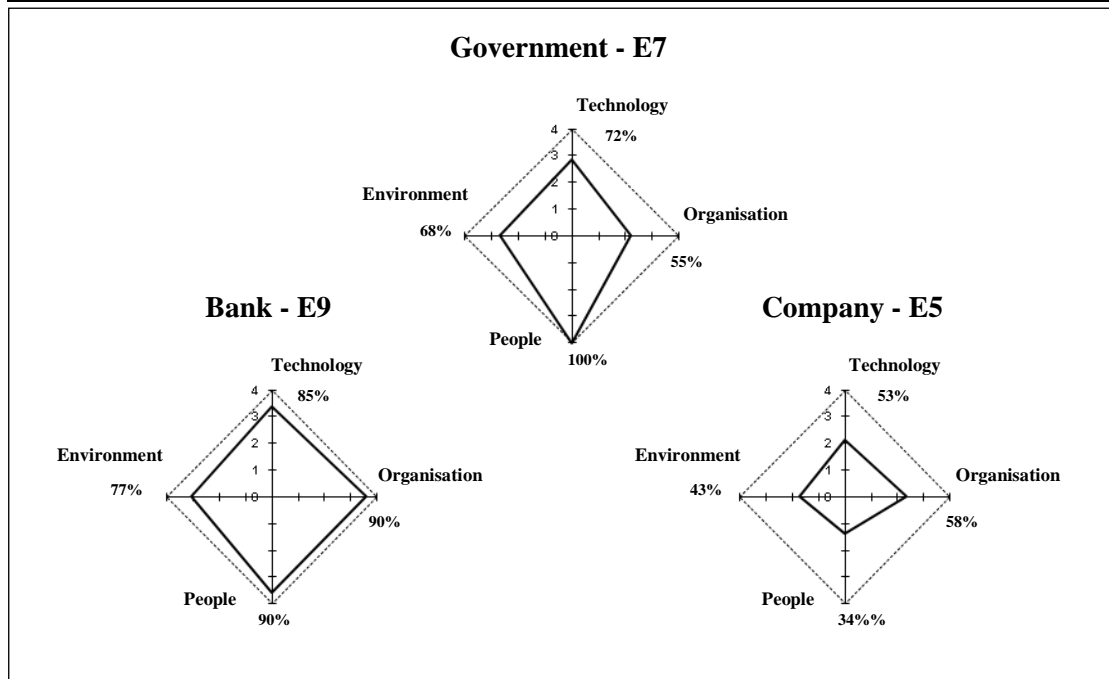
**Figure 7-5 Radar graph of the E2, E5 and E7 performance scores on the ISO/IEC 27002 - clause level**

## The TOPE Indicator

The results obtained above can be presented collectively at the TOPE level, by collecting and weighting the results of each domain. Table 7-6 gives the results concerned with the TOPE overall s-readiness indicators for each enterprise, and these results are illustrated in Figure 7-6. For the financial enterprise E9, the TOPE indicator is (3.4 of 4); for the government enterprise E7, it is (2.8 of 4) and for the private enterprise E5, it is (2 of 4).

**Table 7-6 TOPE weighted indicators**

Domain	Assessment Scores – Domain Level								
	E9			E7			E5		
	D (0-4)	w (of 1)	r (%)	D (0-4)	w (of 1)	r (%)	D (0-4)	w (of 1)	r (%)
<b>T</b>	3.39	0.50	42	2.86	0.50	36	2.13	0.50	27
<b>O</b>	3.61	0.25	23	2.2	0.25	14	2.32	0.25	14
<b>P</b>	3.6	0.10	9	4.0	0.10	10	1.35	0.10	3
<b>E</b>	3.09	0.15	12	2.71	0.15	10	1.73	0.15	6
<b>Indicator</b>	<b>3.4 (86%)</b>			<b>2.8 (70%)</b>			<b>2 (50%)</b>		



**Figure 7-6 Illustration of E9, E7 and E5 assessment results concerned with the TOPE domains**

The presented case studies illustrate the use of the method for practical applications. The results show the weaknesses at all levels, with numerical indicators that help these enterprises to start security improvement programs.

## The Missing Controls

The evaluation results presented above would provide the investigated enterprises with guidelines for future information security improvements. Table 7-7 gives a list of the missing controls for each enterprise. This list could be used to improve the security state in these enterprises. Also, a template of the required security controls could be developed as a result of the e-security experience gained from the comparison of the enterprises working in the same business.

**Table 7-7 A list of the missing controls for each of the investigated enterprises**

D	The Missing Controls for Each of the Investigated Enterprises		
	Bank - E9	Government - E7	Company - E5
Technology	<ul style="list-style-type: none"> <li>-Protection against malicious and mobile code</li> <li>-Mobile computing and tele-working</li> </ul>	<ul style="list-style-type: none"> <li>- Electronic commerce services</li> <li>- Business requirements for access control</li> <li>- Mobile computing and tele-working</li> <li>- Cryptographic controls</li> </ul>	<ul style="list-style-type: none"> <li>- System planning and acceptance</li> <li>- Exchange of information</li> <li>- Business requirements for access control</li> <li>- Mobile computing and tele-working</li> </ul>
Organisation	<ul style="list-style-type: none"> <li>-Reporting information security weaknesses</li> </ul>	<ul style="list-style-type: none"> <li>- Information security policy document.</li> <li>- Information classification</li> <li>- Information security aspects of business continuity management</li> </ul>	<ul style="list-style-type: none"> <li>- change control on information security policy document</li> <li>- security incidents Monitoring</li> <li>- Reporting information security weaknesses</li> <li>- Clear definition of information security responsibilities</li> <li>- Regular reviews by an independent</li> </ul>
People	<ul style="list-style-type: none"> <li>-Contractual security obligations agreed</li> </ul>		<ul style="list-style-type: none"> <li>- Prior to employment</li> <li>- During employment</li> </ul>
Environment	<ul style="list-style-type: none"> <li>-Compliance with security policies and standards</li> </ul>	<ul style="list-style-type: none"> <li>- Compliance with legal requirements</li> <li>- information system audit consideration</li> </ul>	<ul style="list-style-type: none"> <li>- Secure areas</li> <li>- information system audit consideration</li> </ul>

### 7.4.3 The Information Security Assessment Report

An information security assessment report is compiled for each enterprise summarising the achieved scores in the five levels of the TOPE assessment

model, highlighting the key developmental areas and recommending the urgent needed plans as shown in Appendix B. This report was presented to the top management for each enterprise who used the assessment results as a guide in their information security improvement plans, based on the analytical cost-benefit model presented in Chapter 6.

#### 7.4.4 Assessment Results for All Case Studies

In the following sections, the overall average s-readiness assessment results of the nine investigated enterprises are presented at TOPE s-readiness level, the TOPE domains level and the clauses level. In addition, the top ten ranked lowest scores at the objectives, controls and measures levels of the assessment model are also presented.

##### 7.4.4.1 The TOPE-Domains Level

The average s-readiness assessment results of the TOPE domains together with the average overall TOPE indicator of the nine participated enterprises are presented in Table 7-8. The average TOPE indicator of these enterprises is 2.8 of 4 (70%). These enterprises achieved the lowest average score of 2.6 (65%) in the “Technology” domain and had the highest average score of 3.1 of 4 (77.5%) in the “People” domain.

**Table 7-8 The average scores of each of the TOPE domains and the TOPE indicator**

Issue	Assessment Results									
	A		B			C				Avr
	E2	E9	E4	E7	E8	E1	E3	E5	E6	
Technology (of 4)	2.8	3.4	1.5	2.9	3.2	2.2	3.7	2.1	3.9	2.6
Organisation (of 4)	3.5	3.6	1.6	2.2	2.6	0.6	3.9	2.3	3.8	2.7
People (of4)	4.0	3.6	1.3	4.0	4.0	1.8	4.0	1.4	4.0	3.1
Environment (of 4)	2.6	3.1	1.7	2.7	4.0	2.0	4.0	1.7	3.7	2.8
TOPE s-readiness indicator (of 4)	3.0	3.4	1.5	2.8	3.2	1.7	3.8	2.0	3.8	2.8

#### 7.4.4.2 The TOPE-Clauses Level

The average assessment results of the nine investigated enterprises for the eleven ISO/IEC 27002 information security clauses are presented in Table 7-9. The first column lists the TOPE domains, the second column lists the associated ISO/IEC 27002 clauses for each TOPE domain, the third column presents the average score of the nine enterprises in the concerned clause and the fourth column provides the percentage figures of the achieved average score for each of the ISO clauses.

**Table 7-9 The average score of the ISO/IEC 27002 clauses based on the collected data from the nine investigated enterprises**

<b>D</b>	<b>IOS/IEC 27002 Clause</b>		<b>Average Score (of 4)</b>	<b>Percent %</b>
<b>T</b>	10	Communications and Operations Management	2.9	72.5
	11	Access Control	2.9	72.5
	12	Information Systems Acquisition, Development and Maintenance	2.8	70.0
<b>O</b>	5	Security Policy	2.2	55.0
	6	Organisation of Information Security	3.3	82.5
	7	Asset Management	3.0	75.0
	13	Information Security Incident Management	2.3	57.5
	14	Business Continuity Management	3.1	77.5
<b>P</b>	8	Human Resources Security	3.1	77.5
<b>E</b>	9	Physical and Environmental Security	3.1	77.5
	15	Compliance	2.5	62.5

From the results presented in Table 7-9, it is evident that the “information security policy” clause achieved the lowest score of 55%. A recommendation is given for these enterprises to take care of the information security policy using the approach presented in Chapter 5 of the thesis, as will be discussed later in Chapter 8. The ISO/IEC 27002 clause of “information security incident management” achieved 57.5%. The “compliance” clause achieved 62.5%. This

also compiled into general recommendations that will be discussed later in Chapter 8.

#### 7.4.4.3 The TOPE-Objectives Level

According to the assessment results, the ISO/IEC 27002 39 objectives are further investigated, based on the average data collected for the participated enterprises and according to the assessment model presented in Chapter 5, to identify the ten lowest-ranked objectives. The ten lowest-ranked objectives, as shown in Table 7-10, could be used by concerned enterprises inside Saudi Arabia to aid with action plans.

**Table 7-10 The ten lowest-ranked ISO/IEC 27002 objectives based on the analysed data from the nine investigated enterprises**

Rank	The ISO/IEC 27002 Objectives	Average Score	Percent %
1	Electronic commerce services	1.81	45
2	Mobile computing and teleworking	1.87	47
3	Cryptographic controls	2.00	50
4	Management of information security incidents and improvements	2.11	52
5	Information security aspects of business continuity management	2.12	53
6	Information security policy	2.20	55
7	Information systems audit considerations	2.35	59
8	Compliance with legal requirements	2.37	59
9	Business requirements for access control	2.38	60
10	Protection against malicious and mobile code	2.42	61

#### 7.4.4.4 The TOPE-Controls Level

The ten lowest-ranked controls, as shown in Table 7-11, could be used in the development of action plans inside these enterprises. The ten lowest ranked controls are identified as a starting point to address the most critical areas. These controls are addressed to improve the information security practices inside Saudi Arabia and to give a list of recommendations for this purpose.

**Table 7-11 The ten lowest-ranked ISO/IEC 27002 security controls based on the analysed data from the nine investigated enterprises**

Rank	The ISO/IEC 27002 Controls	Average Score	Percent %
1	Collection of evidence	1.22	31
2	Teleworking policy use	1.71	43
3	Protection of organisational records	1.73	43
4	On-line transactions	1.77	44
5	Publicly available information	1.77	44
6	Key management	1.77	44
7	Physical media security	1.77	44
8	Business continuity and risk assessment	1.94	49
9	Reporting security weakness	1.95	49
10	Policy on the use of cryptographic controls	2.00	50

#### 7.4.4.5 The TOPE-Measures Level

The ten lowest-ranked assigned measures are presented in Table 7-12. These measures are identified as a starting point to address the most critical security areas which need improvement.

**Table 7-12 The ten lowest-ranked ISO/IEC 27002 assigned security measures based on the analysed data from the nine investigated enterprises**

Rank	The ISO/IEC 27002 Measures	Average Score	Percent %
1	Do you have mechanism to ensure that no forensics work to be performed on original evidential material?	1.11	28
2	Do you develop internal procedures to be followed in collecting evidence that conform to the rules for evidence laid down in the relevant jurisdiction?	1.22	31
3	Do you develop internal procedures to be followed in presenting evidence that conform to the rules for evidence laid down in the relevant jurisdiction?	1.33	33
4	Do you have control to prevent the execution of unauthorised mobile code?	1.44	36
5	Do you develop and implement procedures, to control teleworking activities?	1.55	39
6	Are the important records protected from loss in accordance with statutory, regulatory, contractual, and business requirements?	1.66	42
7	Do you develop and implement operational plans, to control teleworking activities?	1.67	42
8	Are the important records protected from falsification in accordance with statutory, regulatory, contractual, and business requirements?	1.67	42
9	Do you have formal procedures for safely dispose the media?	1.67	42
10	Do you have a key management policy?	1.77	44

## 7.5 Application of the Cost-Benefit Model

The application of the mathematical model presented in Chapter 6 is illustrated here through a real world example that uses its analytical considerations and procedure. The assessment model of enterprise E2 revealed that a score of 50% is achieved in the ISO/IEC 27002 control concerned with protection against malicious codes. Accordingly, the decision was taken to replace the existing antivirus tool by a newer one that could achieve better performance to protect the enterprise information resources. The example presented in the following is described according to the same sequence through which the model is presented in Chapter 6.

### 7.5.1 Security Challenges

Table 7-13 identifies the challenges that the example takes into account. The estimated cost frequency and cost per year for each challenge are given. In addition, the total cost of all challenges per year is also given. The estimation of these factors is based on common knowledge, expert estimation or models that estimate the expected losses which include the damages to information assets, the cost of repair and restoration, as well as the negative impacts on commercial activity and equity valuation.

**Table 7-13 Challenges considered and their cost**

i	Challenges	Estimated Cost G[i]	Frequency F[i]	Annual Cost g (i)=G[i]*F[i]
1	Virus	2000	6	12000
2	Worm	1000	5	5000
3	Trojan	1000	3	3000
<b>Cost of identified challenges per year</b>		$g = \sum_{i=1}^{i=I} g [i]$		20000

### 7.5.2 Protection Measures

Anti-virus software is widely used for protection against viruses, worms, and trojan horses. According to the annual computer crime and security survey for



the year 2007 (CSI, 2007), anti-virus software has been used by 98% of computer users. The protection obtained by using this software depends on the security controls associated with its application. Considering the technology, organisation, people and environment (TOPE) view of ISO/IEC 27002, as explained before in Chapter 4 (Saleh et al., 2006), the security controls that can be associated with the application of the anti-virus software are given in Table 7-11. Each control is identified and associated with its TOPE domain, its section number within ISO/IEC 27002 standard, its estimated annual cost and its application level (j). Application level-1 represents the essential control of installing the anti-virus. Application level-2 adds another control that is the information back-up control. Subsequent application levels keep adding other controls that can enhance the use of the anti-virus software. Each level would lead to a certain protection probability, and can be viewed as a protection measure against identified challenges.

The above principle of using multi-levels in the application of protection measures has also been used in the empirical study presented in Tanaka et al. (2006). Unlike the above considerations of 12 levels associated with the ISO/IEC 27002 standard, the empirical study of Tanaka et al. considered only three levels and these were associated with: defence measures, security policy and human cultivation. It is important to mention here that the priority given here to each measure, as shown in Table 7-14, will be assigned by an expert in information security. That expert will first choose the most suitable security measures from the list of the ISO/IEC 27002 standard measures. Second, the expert will assign the most effective measure to mitigate the assigned risk to give it higher priority, so the arrangement of these security measures (shown in Table 7-14) will indicate the relative importance of these measures, and

consequently the application level.

**Table 7-14 ISO/IEC 27002 controls associated with application of the antivirus.**

Protection Measures					
ISO/IEC 27002 Ref.	ISO/IEC 27002 Controls	Explanation	Yearly Cost (\$)	j	
T	10.3.1	<b>Capacity management</b>	For the implementation of the antivirus the capacity requirements should be identified to ensure and improve the availability and efficiency of systems.	500	11
	10.3.2	<b>System acceptance</b>	According to the enterprise acceptance criteria and the suitable tests of the system carried out before acceptance.	800	10
	10.4.1	<b>Controls against malicious code</b>	Detection, prevention and recovery controls to protect against malicious code.	2000	1
	10.4.2	<b>Controls against mobile code</b>	Where the use of mobile code is authorised, the configuration should ensure that the authorised mobile code operates.	900	9
	10.5.1	<b>Information back-up</b>	Back-up copies of information and software should be taken prior the installation of the software.	1800	2
	10.10.6	<b>Clock synchronisation</b>	The correct interpretation of the date/time format is important to ensure that the timestamp reflects the reality.	1700	3
	12.1.1	<b>Security requirements analysis and specification</b>	Statements of business requirements for new information systems should be stated	1000	8
O	5.1.2	<b>Review of information security policy</b>	Update the information security policy by adding section for the antivirus software policy.	400	12
	7.1.1	<b>Inventory of assets</b>	All assets should be clearly identified and an inventory of all important assets drawn up.	1500	4
P	8.2.2	<b>Information security awareness, education and training</b>	A programme for awareness training should be prepared .	1300	6
E	15.2.1	<b>Compliance with security policies and standards</b>	All security procedures should be carried out correctly to achieve compliance with security policies and standards.	1200	5
	15.2.2	<b>Technical compliance checking</b>	Information systems should be regularly checked for compliance with security implementation standards.	1100	7

### 7.5.3 Achieved Protection

Table 7-15 is concerned with the protection achieved from each protection level. At no protection, it is apparent that the annual cost is the cost of challenges given in Table 7-14. Each level of protection used is given in the table in terms of the following:

- Its estimated annual cost, accumulated from Table 7-14;
- its estimated protection probability;
- annual saving of challenges' cost;
- annual residual cost; and
- total annual cost.

### 7.5.4 Cost Function

As would be expected, Table 7-15 shows the following:

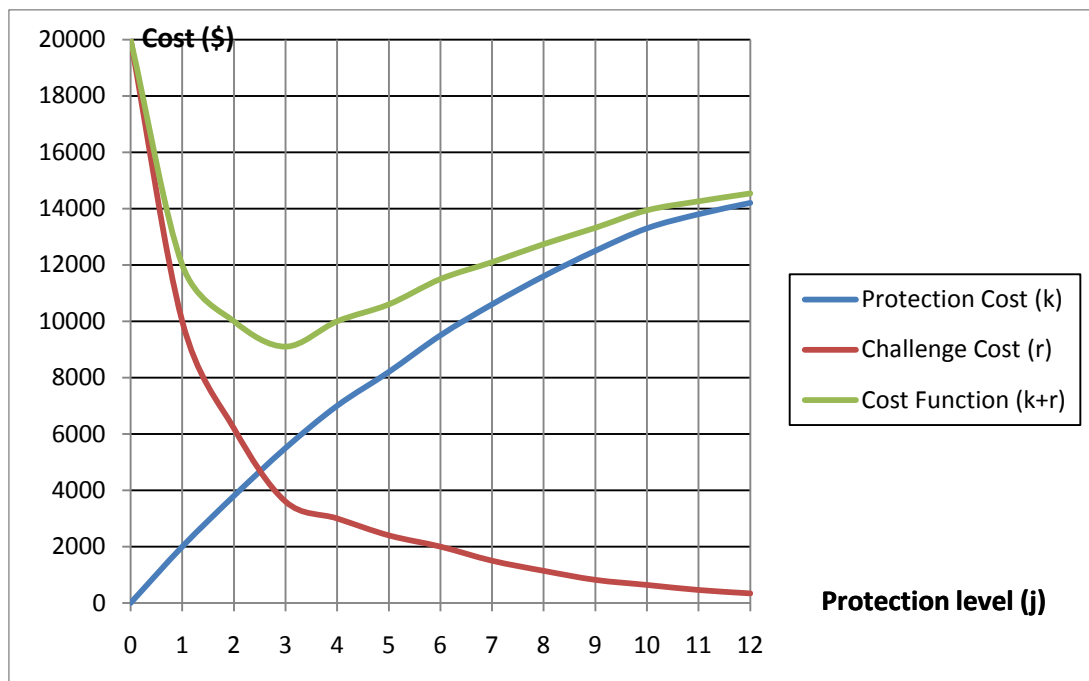
- The estimated value of the cost of protection increases as the level of protection increases;

**Table 7-15 Cost-benefit analysis for twelve protection levels**

Cost of identified challenges per year (Table 7-13)				$g = \sum_{i=1}^{i=I} g[i] = 20000$	
j	Accumulated Cost of protection: k	Probability of protection: p	Saving in challenge cost: g*p	Residual cost: r	Total cost: k + r
0	0	0	0	20000	20000
1	2000	0.5	10000	10000	12000
2	3800	0.19	3800	6200	10000
3	5500	0.13	2600	3600	9100
4	7000	0.03	600	3000	10000
5	8200	0.03	600	2400	10600
6	9500	0.02	400	2000	11500
7	10600	0.025	500	1500	12100
8	11600	0.018	360	1140	12740
9	12500	0.016	320	820	13320
10	13300	0.009	180	640	13940
11	13800	0.009	180	460	14260
12	14200	0.006	120	340	14540

- the residual cost of challenges decreases as the level of protection increases; and
- the estimated total cost changes with both: the increase of the protection cost, and the decrease of the residual challenges cost.

The above cost functions are illustrated in Figure 7-7 based on the calculations of Table 7-15 and with the considerations above, it is shown that minimum total cost is achieved at protection level 3.



**Figure 7-7 The changes of enterprise E2 of : residual cost of challenges (r), cost of protection (k) and total cost (c)**

## 7.6 Summary

The work presented in this chapter presents the achievement of the fifth main objective of this research study, which is concerned with the application of the developed assessment model for investigating information security readiness of nine Saudi enterprises. This assessment is based on the security risk protection controls of ISO/IEC 27002. The results provide indicators associated with the various domains of the TOPE model and with its five levels of details.

These practical results indicate the effectiveness of the approach considered to illustrate the state of the information security inside these enterprises, showing the weaknesses at all levels of the model with numerical indicators that could be used by the directors of the enterprise to assign the priorities and direct the resources to improve the information security. The given results would also help these enterprises in obtaining the ISO/IEC 27001 information security certification that promotes their e-services image. A real example is presented, for applying the cost-benefit model presented in Chapter 6, to investigate the cost versus the benefits of using various protection measures to encounter the expected challenges under their own environment and considering specific circumstances.

**PART V**  
**CONCLUSION**

**Chapter 8 CONCLUSIONS AND FUTURE WORK**

# Chapter 8

## CONCLUSION AND FUTURE WORK

### 8.1 Introduction

There is an increase in the interaction of different enterprises at the internal Intranet, business Extranet and public Internet levels. The need to conduct business or exchange confidential information between these enterprises raises the issues of information security risk management and security readiness assessment. The ultimate aim of this research project is to develop analytical models for enterprise information security readiness assessment and for cost-benefit analysis. These models are incorporated into a developed comprehensive enterprise information security risk management framework that serves as a reference framework for enterprise information security risk management. The developed information security assessment model could be used by enterprises for expressing the assurance level of their information security management system depending on the protection controls of the ISO/IEC 27002 information security management standard. The developed information security cost-benefit model could be used by enterprises for economically adjusting their expenditures on the recommended information security protection measures. Chapter 8, therefore concludes the work presented in this thesis and contributes in addressing the last research question by introducing a number of recommendations to improve the current situation of information security management practices at Saudi enterprises.

## **8.2 Conclusion**

The main objective of this research study was to develop analytical models for numerically assessing the current state enterprise information security readiness and for cost effectively helping in the selection of the recommended protection measures. For this purpose, an enterprise information security risk management framework (EISRM) is developed to integrate the information security risk management approaches in a comprehensive reference framework. The developed EISRM framework consists of four dimensions and depends on well established approaches for its structural and procedural dimensions. The TOPE scope is adopted for achieving the comprehensiveness of the framework while the DMAIC process is used to incorporate the main activities of the key risk management methods. The assessment of the current state information security, which incorporated in the proposed EISRM framework, is based on a multi-level analytical model and uses a developed investigation form for collecting and analysing the required assessment data. The evaluation of the information security assessment model is conducted in nine Saudi enterprises working in different fields. The results proved the effectiveness of the proposed approach in assessing the information security readiness using the ISO/IEC 27002 information security management standard with different levels of detail. The assessment results can be used by enterprises for directing their resources, based on a developed cost-benefit analytical model, to improve their information security readiness to an acceptable level.

### **8.2.1 Study Main Objectives**

To achieve the overall objective of this research study in developing analytical



tools within a comprehensive information security risk management framework for assessing enterprise information security readiness and analysing the investment in protection measures, the research has carried out an extensive investigation of the related literature. Risk management methods, information security management standards and information security economic models have been investigated in detail. Consequently, there are six main objectives of this research study:

- To develop a comprehensive framework for enterprise information security risk management which not only considers technological issues, but also considers organisational, human and environmental issues as well.
- To extract enterprise information security assessment measures based on the ISO/IEC 27002 code of practice for information security management standard.
- To develop an analytical model for enterprise information security readiness assessment that provides integrated multi-level security indicators based on the risk controls of the ISO/IEC 27002 information security management standard.
- To develop a practical analytical model that provides cost-benefit trade-off between enterprise information security risks, and the required protection measures.
- To explore the application of the assessment model in investigating information security readiness of nine Saudi enterprises working in different fields and presenting the assessment results numerically and graphically using a developed computer tool.

- To suggest general recommendations for improving the information security practices at Saudi enterprises.

### **8.2.2 Study Main Contributions**

This study makes several significant contributions towards research and theory of information security risk management. As the theory in the field of information security risk management is still not well developed, this study can be considered as a step towards building of a more robust theory. On the other hand, the study contributes in raising the level of awareness about the essential role of information security management in protecting the rapid development in information technology services at Saudi Arabia. In summary, the main contributions of this research study are as follows:

**The comprehensive enterprise information security risk management (EISRM) framework:** The proposed EISRM framework has two structural dimensions and two procedural dimensions. The structural dimensions include EISRM scope and EISRM assessment criteria, while the procedural dimensions include EISRM process and EISRM assessment tools. The framework uses the comprehensive TOPE (Technology, Organisation, People and Environment) view for the EISRM scope, while its assessment criteria is considered open to various standards. For the procedural dimensions, the framework uses the widely known six-sigma DMAIC (Define, Measure, Analyse, Improve and Control) cycle for the EISRM process, and it considers the use of various assessment tools.

The TOPE scope of the framework enables it to accommodate the wide range of issues associated with EISRM in a well structured and open manner. This does not only integrates the components that have been considered by other

methods, but also permits other or emerging components to be considered. The six-sigma DMAIC process of the framework allows it to accommodate the various processes of other EISRM methods in one unified and widely accepted process.

In addition, the framework responds to the need of using a management criteria and permits various criterion to be taken into account including ISO information security controls, and considering pre-determined benchmarks. Furthermore, the framework considers the use of support tools for performing the various phases of the process efficiently as is the case with other EISRM methods.

The proposed EISRM framework provides enterprises with a comprehensive approach for the effective implementation of information security risk management programme that addresses organisation, people and environment issues as well as the technical issues. The EISRM framework could be considered an open reference for conducting risk management and for improving the security level of information security systems.

**An ISO based information security assessment measures:** The research assigns information security readiness assessment measures, based on the ISO/IEC 27002 code of practice for information security management standard. These measures are structured according to the TOPE domains of technology, organisation, people and environment. The suggested categories serves as a base for developing an investigation form that could be used as an assessment instrument for collecting the required data about the effective use of information security protection measures. In addition, the categorisation technique enables the assessment questions to be answered by different

employees from different departments and with different expertise which leads to achieving better results.

**The multi level analytical information security assessment model:** The developed enterprise information security assessment model is based on the technology, organisation, people and environment (TOPE) scope that provides integrated and well structured view of the various parts and issues of the ISO/IEC 27002 information security management standard. The model has five main levels as follows:

- The first level is associated with the TOPE domains;
- the second level is concerned with the main clauses of the standard. These clauses are organised according to their relationship with each of the TOPE domains;
- the third level is related to the security objectives of the standard;
- the fourth level is associated with the security controls recommended by the standard for the achievement of its objectives; and
- the fifth level is concerned with the measures, which are used for the evaluation of the effective use of the security controls.

The developed mathematical model starts the evaluation of the indicators at the bottom level and moves gradually from one level to another, where the evaluation of each of the higher levels is based on the evaluation of its preceded level. In accumulating the indicators from one level to another, the model assigns weights to the values of the indicators, so that each indicator is valued according to its importance and performance to the information security of the concerned enterprise.

This model provides useful tool for numerically investigating enterprises with the ISO/IEC 27002 information security management standard. The

investigation of real enterprises illustrates the multi-level results concerned with the TOPE domains and the overall higher-level result associated with the TOPE level together with the security readiness indicator for the investigated enterprises.

**The gradual approach for the application of the ISO information security standards:** The proposed gradual approach for the application of the ISO security standards is of incremental nature, and has three levels of assessment, with increasing security controls. The first level considers the 19 ISO/IEC 27002 essential and common security controls, as stated by the standard, which are refined into 45 basic security measures. The second level is concerned with all 133 ISO/IEC 27002 base-line security controls, including those of level one, which are refined into 283 basic security measures. The third level adds to the second level other security controls considered by other standards related to ISO/IEC 27002 or required by various individual enterprises, depending on their business and information security strategies. This approach helps enterprises to move gradually for enhancing their information security, according to the base-line standard protection measures and beyond.

**The practical analytical cost-benefit model:** This practical analytical model is concerned with analysing the cost of threats facing information security in an enterprise versus the benefits of implementing the recommended protection measures that can be used to reduce the effect of these threats. The model is distinguished by its practicality and generic nature, which enables various considerations associated with different case studies to be analysed.

**Case studies:** Case studies are presented for the application of the proposed approach in assessing information security state of nine Saudi enterprises.

The implementation studies have produced important practical numerical results associated with the information security readiness of these enterprises. The practical numerical results illustrate the strengths and weaknesses of the information security at all levels from the ISO/IEC 27002 security controls up to the TOPE domains.

The practical investigation of the participated enterprises includes evaluation of grades and weights for: “283” measures concerned with the use of the protection controls; “133” protection controls associated with the achievement of the security objectives; “39” objectives related to conformance with the clauses of ISO/IEC 27002; “11” ISO clauses concerned with compliance with the TOPE domains; four TOPE domains associated with the s-readiness indicator; and finally, the s-readiness indicator itself. The results of the practical investigations provide enterprises with guidelines for future information security improvements. They would also help them obtain ISO/IEC 27001 information security certification that promotes their e-services’ image. In addition the results presented in Chapter 7 of the thesis can give enterprises a numerical score at different levels that represent an assurance measure of their information security management systems.

**Computer Tool:** The developed computer tool supports the use of the information security assessment model presented in the thesis and graphically presents the results for direct evaluation and comparison of s-readiness indicators at different levels of detail.

### **8.2.3 Study Limitations**

This study, as the case with other research studies, has a number of limitations. These limitations are mainly related to the sensitivity of the subject of this research study, the time constrains, the bias in data collection and the

generalisation of the study. These limitations will be discussed in the following sections.

### **8.2.3.1 Sensitivity of the Subject**

As mentioned before, the information security of any enterprise is a sensitive area and specific to the enterprise stakeholders. It is very difficult to achieve the goals of any study devoted to capture the reality of the information security situation and this was the case with this research study. The researcher faced critical problems in choosing the investigated enterprises, getting the permission and signing official papers for not announcing the real names of participated enterprises. The researcher faces also a major problem in assessing the information security depending mainly on the information security manager, who is responsible for information security, and trying only to pass the assessment exercise safely.

### **8.2.3.2 Time Constraints**

With the use of a case study approach to evaluate the effectiveness of the developed framework and its associated models, more time would allow conducting more than one cycle of information security assessment of the investigated enterprises. This will enable the researcher to benchmark the collected data and identify whether the information security readiness indeed improved after the implementation of the suggested protection measures and how this reflects on the numerical scores at all levels of the model. In addition, more time is needed to investigate a bigger sample for developing a template specific for information security controls of each industry or business. The results in turn could be used to compare the level of information security readiness across different industries.

### **8.2.3.3 Bias in Data Collection**

The possibility of bias in the collection and interpretation of the collected data from interviews, observations and the investigation form are acknowledged. This research, whenever possible, utilised multiple data collection methods (the triangulation method) to increase validity and reliability of the collected data.

### **8.2.3.4 Generalisation of the Study**

The sample, targeted by this study, was hard to reach with a full random selection, so it cannot be considered as a representative of its population. The application of the assessment model to only nine Saudi enterprises limits the generalisation of the findings. However, the main aim of this research was to assess the information security within these enterprises. Further research is needed for applying the model to other enterprises in different industries and in different countries before more global conclusions can be offered. The researcher, to overcome this limitation, developed a website to collect more sample size. The output of this website was very poor during the last ten months.

## **8.2.4 Validation of the Results**

There are no past results that can be used for direct comparison, assessment and rigorous validation of the results obtained here. However, the strength of the approach and the validity of the obtained results stems from the past use of the TOPE scope in various problems associated with ICT use; the extensive use of the six-sigma process in different applications; and the experience behind the development of the ISO/IEC 27002 information security controls. In addition, the investigated enterprises later confirmed that the results from this



study did correspond well to their common feeling of the possible enterprise information security level. Furthermore, the regular publications of the research results in the information security conferences and journals assess the work and get valuable feedback from the reviewers (Saleh et al, 2006, 2007, 2008).

### **8.3 Recommendations for Saudi Enterprises**

This section is devoted to present a number of recommendations revealed as a result from the present study. The following recommendations are concerned with improving the information security situation inside Saudi enterprises based on the assessment results of the nine investigated enterprises.

1. A proactive approach toward managing information security, using preventive rather reactive methods, would improve the information security situation inside Saudi enterprises. The developed EISRM framework in Chapter 3 of the thesis could be used for this purpose. This framework is designed to help enterprises not only in running effective risk management programmes, but also in their decision at early stages about the need for running detailed risk-analysis exercise, or depend only on the best-practice standard security controls. This decision will help in managing enterprise resources in a better way.
2. It is apparent that information security is an enterprise specific issue and should be managed by the employees of enterprise. The developed information security readiness assessment model in Chapter 5 of the thesis could be used for this purpose by Saudi enterprises. The application of the model in different Saudi enterprises proves the effectiveness of the model in assessing information security state according to the ISO/IEC 27002 standard with different levels of detail.

The model could be used for presenting the assessment results numerically and graphically to the top management to assign priorities and direct resources for applying the suggested mitigation plans. This model will increase the trustworthiness of the ISO/IEC 27002 standard and will provide an assurance measure in the enterprise information security management system.

3. Implementing new security measures for the sake of better secured environment can be considered as waste of valuable resources. Saudi enterprises, therefore, need to analyse their information security thoroughly and ensure appropriateness of security controls based on economical analysis before any mitigation plans are undertaken. The cost-benefit analytical model presented in Chapter 6 of the thesis could be used as a base for directing the investment in the recommended information security protection measures. Thus the decision regarding the purchasing of new or additional information security protection measures could be evaluated according to an economical analysis that coincides with enterprise mission and business objectives.
4. It is apparent, from the results of the investigated Saudi enterprises, the absence of the information security standards in managing information security inside these enterprises. This bring to the surface the urgent need to start a mandatory national information security certification programme based on the ISO/IEC 27001 international information security management standard. This will increase the trust between Saudi enterprises and achieve a common secured environment for running their business efficiently.

5. It is clear that the employees of the enterprise, where each has a responsibility towards securing information, should share in protecting enterprise information resources. In this respect, there is an urgent need to create a highly qualified trained security aware workforce from the employees of the enterprise itself that could contribute to improve information security and used to prevent inside as well as outside threats. The structured approach, according to the six-sigma model for assigning information security responsibilities to the employees of the enterprise presented in Chapter 3 of the thesis, could be used by Saudi enterprises for this purpose.
6. The gradual approach presented in Chapter 4 of the thesis could be adopted by Saudi enterprises for moving gradually in three stages to achieve the main requirements by the information security standard parties.

## **8.4 Future Work**

The study achieved the objectives set out for this research, but has certain limitations that call for future research work to supplement and support the current findings. In this respect, future potential studies based on the achievements of this thesis are introduced in the following:

- Further research is possible to find techniques to automate the process of finding the parameters of the assessment model at the lower level. These parameters should automatically receive their values based on the input from real world. This could aid in providing more accurate results, as the failing of the current procedures for assessing information security readiness is because the assessment

process is conducted by human audit at one particular instance in time.

- More practical investigation of the use of the cost-benefit model for improving current approaches in selecting the most economical information security controls. This will help in providing a tool to help the decision makers in their early decisions regarding the investment in the required security controls.
- An important study would be concerned with using the TOPE view presented in this thesis for the development of evaluation bases for information security management in specified business fields, such as banking, health care, education and other fields. Such specific evaluation bases can start from the general common base, given in this thesis, and move on to the required specific bases through field studies that investigate the important issues associated with each specific business field and assign importance levels to these issues. Such investigations will help in drawing a map on the strengths and weaknesses of information security management in enterprises. This approach will help enterprises learning from one another's issues of differences and working together in issues of common problems.
- A second information security assessment should be conducted in the investigated enterprises. The results of the assessment conducted in this research study should serve as benchmark data that could be used to compare the second assessment. This will provide insight into whether the recommendations that were implemented as a result of the information security readiness

assessment model had a positive influence on the information security inside these enterprises.

- The methodology presented in the thesis for numerically assessing enterprise information security readiness can be used by researchers to extend the developed model to integrate different information security standards. Such standards may include other IT security standards, like the BSI Germany standard, the SOGP standard and other related standards. This will help in improving the results by providing more detailed view of the enterprises information security state at lower levels that could be used as an input to the assessment model presented in Chapter 5 of the thesis.
- Human assessments contain some degree of subjectivity that often cannot be expressed in pure numeric scales and requires linguistic expressions. The research in assessing the security measures at the lower level of the information security assessment model used the categorical method in assessing these measures according to the “lickert scale”. The main problem with this method is that the subjectivity and imprecision associated with perceptions are lost by forcing the assessor to use numeric scales. In addition, this method is largely intuitive, heavily dependent on personal judgement of the assessor and all the criteria are assumed to have equal importance. The subjectivity of human assessments and beliefs can best be expressed in linguistic terms without the limitation of the numeric scales’ boundaries. Fuzzy logic techniques that allow the assessors to express their opinions in linguistic terms could be used to

enhance the developed assessment model in capturing this subjectivity.

- Bayesian Belief Network (BBN) could be used in calculating the value of risk depending on the TOPE domains and considering the causes of the threats with different levels of inference on the enterprise assets. This will help in building probabilistic tables that could be used and reused to assess the risks to the enterprises main information resources. The BBN could also be used to illustrate the relationships between enterprise information security risks and its causes from the combined factors resulted from different levels of technical, organisational, people and environmental factors.

**PART VI**  
**REFERENCES**

## REFERENCES

### A

- Alberts, C. and Dorofee, A. (2003) *Managing Information Security Risks: The OCTAVE Approach*. Boston: Addison Wesley.
- Allen, J. (2001) *The CERT Guide to System and Network Security Practices*. Boston: Addison Wesley.
- Anderson, E. and Choobineh, J. (2008) Enterprise information security strategies. *Computer & Security*, 27(1-2), pp. 22-29.
- Anderson, R. and Moore, T. (2006) The economics of information security. *Science*, 314(5799), pp. 610-613.
- Australia Standards NewZealand (2004) AS/NZS 4360:2004. *Risk management third edition standards*. Sydney: Australia, Wellington, NewZealand: Australia Standards NewZealand.
- Australian Computer Crime and Security Survey (ACCSS) (2007)*. [online]. Available from: <http://www.auscert.org.au/ACCSS2007.pdf>. [Accessed: 6th April 2008].
- Axelord, R. (2003) *Risk in network information systems*, Gerald Ford School of Public Policy, University of Michigan, Ann Arbor: Research Report.

### B

- Bagozzi, R. (1994) *Principles of marketing research*. London: Basil Blackwell Ltd.
- Bakry, S. H. (2003a) Development of security policies for private networks. *International Journal of Network Management*, 13(3), pp. 203-210.
- Bakry, S. H. (2003b) Toward the development of a standard e-readiness assessment policy. *International Journal of Network Management*, 13(2), pp. 129-137.
- Bellone, J. (2008) Reaching escape velocity: a practiced approach to information security management system implementation. *Information Management & Computer Security*, 16(1), pp. 49-57.
- Bernard, R. (2007) Information lifecycle security risk assessment: a tool for closing security gaps. *Computer & Security*, 26(1), pp. 26-30.
- BERR, Department for Business Enterprise and Regulatory Reform (2008), *Information Security Breaches: 2008 Survey*, Department for Business Enterprise and Regulatory Reform, UK.
- Beznosov, K. and Beznosova, O. (2007) On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security*, 15(5), pp. 420-431.
- Bodin, L. D., Gordon, L. A. and Loeb, M. P. (2008) Information security and risk management. *Communications of the ACM*, 51(4), pp. 64-68.
- Boehmer, W. (2008) Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. *Proceedings of the Second International Conference on Emerging Security Information Systems and Technologies*. Cap Esterel, France, 25-31th August 2008, IEEE Computer Society, pp.224-231.



- Boehmer, W. (2009) Cost-benefit trad-off analysis of an ISMS based on ISO 27001. *International Conferencem on Availability, Reliability and Security* . Japan, 16-19 th March 2009, IEEE computer society, pp. 392-399.
- Bojanc, R. and Jerman-Blazic, B. (2008) An economic modeling approach to information security risk management. *International Journal of Information Management*, 28(5), pp. 413
- Borodin, L. D., Gordon, L. A. and Loeb, M. P. (2005) Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2), pp. 79-83.
- Bott, T. F. and Eisenhawer, S. W. (2002) Risk analysis using a hybrid Bayesian-approximate reasoning methodology. *Proceedings Annual Reliability and Maintainability Symposium*. Seattle,WA,USA, 28-31th January 2002, IEEE, pp. 127-133.
- Boynton, B. C. (2007) Identification of process improvement methodologies with application in information security. *Information Security CurriculumDevelopment Conference 07*. Georgia, 28-29th September 2007, ACM .
- Braber, F., Hogganvik, I., Lund, M., Stolen, K., and Vraalsen, F. (2007) Model-based security analysis in seven steps – a guide tour to the CORAS method. Vol. 25 (1) of BT Technology Journal, pp. 101-117, Springer Verlag.
- Brace, L. (2004) *Questionnaire design: how to plan, structure and write survey material for effective market research*. Great Britain: Kogan Page Limited.
- British Standards Institution (2005) BS 7799 :2005. *Information technology security techniques. Code of practice for information security management*. London: British Standards Institution.
- Broodryk, J. (2005) *Enterprise Risk Assessment-A New Approach for a Tough Environment*. [online]. Available from: <http://www.ictworls.co.za/EditorialEdit.asp?EditorialID=25209andArchive=1>. [Accessed : 28th June 2007].
- Brotby, K. (2009) *Information Security Governance: A Practical Development and Implementation Approach*. New Jersey: John Wiley and Sons, INC.
- Bryman, A. (1995) *Quantity and quality in social research*. London: Unwin Hyman.
- Bundesamt Fur Sicherheit in der Informationstechnik (2004) BSI Standard. *IT Baseline Protection Manual, Federal Office for Information Security*. Germany: Bundesmt Fur Sicherheit id der Informationostechnik.
- Bundesamt Fur Sicherheit in der Informationstechnik (2005) BSI Standard 100-3:2005. *Risk Analysis based on IT- Grundschutz- Version 2.0, Federal Office for Information Security*. Germany: Bundesmt Fur Sicherteit id der Informationstechnik. [online]. Available from: [www.bsi.bund.de/grundschutz](http://www.bsi.bund.de/grundschutz) [Accessed: 8th March 2008].
- Burgess, T. F. (2001) *A general introduction to the design of questionnaires for survey research*. UK: University of Leeds.
- Butler, S. A. (2002) Security attribute evaluation method: A cost-benefit approach. *Proceedings of the 24th International Conference on Software Engineering –ICSE*. Orlando, Florida, 19-25 May 2002, pp. 232-240.

## C

- Campbell, R. P. (1997) A modular approach to computer security risk management. *In AFIPS Conference Proceedings*. AFIPS Press. pp.293-304.
- Carroll, J. M. (1996) *Computer Security*. 3rd edn., Oxford: Butterworth Heinemann.
- Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2004b) Economics of IT security management: four improvements to current security practices. *Communications of the Association for Information Systems*, 14(3), pp.65-75.
- Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004a) A model for evaluating IT security investments. *Communications of the ACM*, 47(7), pp. 87-92.
- CERT Computer Emergency Response Team web site (2009) [online]. available from:  
<http://www.cert.org/> [Accessed: 21st February 2010]
- Chang, S. E. and Ho, C. B. (2006) Organizational factors to the effectiveness on implementing information security management. *Journal of Industrial Management & Data Systems*, 106(3), pp. 345-361.
- Christopher, A. and Audrey, D. (2003) *Managing Information Security Risks: The OCTAVE Approach*. Boston: Addison Wesley.
- Computer Security Institute CSI (2007), *Computer Crime and Security: 2007 Survey*, Computer Security Institute, USA.
- Control objectives for information and related technologies (COBIT) (2000) COBIT: 2000. *IT Governance Institute (ITGI) and Information Systems Audit and Control Association (ISACA)*.
- Cooper, D. and Emory, C. (1995) *Business Research Methods*. Chicago: Irwin.
- CORAS (2003) [online]. Available from:  
<http://coras.sourceforge.net/>. [Accessed : 24th October 2005].
- CRAMM user guide (2001) *Risk Analysis and Management Method*. United Kingdom: Central Computer and Telecommunication Agency (CCTA).

## D

- Davidson, R. A. and Lambertm, S. C. (2004) Applying the Australian and New Zealand risk management standard to information systems in SMEs. *Australian Journal of Information Systems AJIS*, 12(1), pp. 4-17.
- Denzin, N. K. (1978) *Sociological Methods: A Sourecbook*. London: McGraw-Hill.
- DTI Department for Trade and Industry (2002), *Information Security Breaches: 2002 Survey*, Department for Trade and Industry, London.

## E

- EBIOS – Expression of Needs and Identification of Security Objectives, France (May, 2004) [online]. Available from:  
<http://www.ssi.gouv.fr/en/confidence/ebiospresentation> [Accessed: 8th December 2008].
- Ekelhart, A. Fenz, S. Goluch, G. Steinkellner, M. and Weippl, E. (2009) XML Security – A Comparative Literature Review. *Journal of Systems and Software*, 81(10), pp. 1715-1724.

- Eloff, J. and Eloff, M. (2003) Information security management: a new paradigm. *Proceeding of the Annual Research conference of the South African Institute of Computer Scientists and Information Technologists SAICSIT*. Sandton, South Africa, Institute of Computer Scientists and Information Technologists, pp. 130-136.
- Eloff, J. and Eloff, M. (2005) Integrated Information Security Architecture, *Computer Fraud and Security*, (11) pp. 10-16.
- Eloff, M. M. and Von Solms, S. H. (2000a) Information security management: a hierarchical framework for various approaches. *Computer & Security*, 19(3), pp. 243-256.
- Eloff, M. M. and Von Solms, S. H. (2000b) Information security management: an approach to combine process certification and product evaluation. *Computer & Security*, 19(8), pp. 698-709.
- European Commission EC (2009) *Enterprise and Industry Definitions*. [online]. Available from:  
<http://ec.europa.eu/enterprise/entrepreneurship/in> [Accessed: 6th September 2009].
- European Summit in Lisbon, Portugal (March, 2000) [online]. Available from:  
[http://ec.europa.eu/index\\_en.htm](http://ec.europa.eu/index_en.htm) [Accessed: 8th December 2005].
- F**
- Federal Computer Incident Response Center FedCIRC (2007) United States Department of Homeland Security. [online] Available from:  
<http://www.us-cert.gov/federal/> [Accessed: 25th January 2008].
- Fenz, S., Pruchner, T. and Manutscheri, A. (2009) Ontological Mapping of Information Security Best-Practice Guidelines. BIS 2009, LNBIP 21, pp. 49-60.
- FIPS PUB 65, National Bureau of Standards (1997). *Guidelines of Automatic Data Processing Risk Analysis*. USA: Washington D.C., General Printing Office.
- FISMA Federal Information Security Management Act (2002). [online] Available from:  
<http://csrc.nist.gov/groups/SMA/fisma/index.html>
- Fredriksen, R.; Kristiansen, M.; Gran, B.; Stolen, K.; Opperud, T.; and Dimitrakow, T. (2002) The CORAS framework for a model-based risk management process in the proceeding of Safecom.
- Fu, Y., Farn, K., Yang, C. (2008) CORAS for the Research of ISAC. International Conference on Convergence and hybrid Information Technology. 28-29 August Daejeon, South Korea, pp. 250-256.
- Fulford, H. and Doherty, N. (2003) The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, 11(3), pp. 106-114.
- Fung, A. R., Farn, K. and Lin, A. (2003) A study on the certification of the information security management systems. *Computer Standards & Interfaces*, 25(5), pp. 447-461.

## G

- G8 Summit in Okinawa, Japan (July 2000) [online]. Available from: <http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm> [Accessed: 25 May 2007].
- G8 Summit in Sea Island (June 2004) [online]. Available from: [www.g8usa.gov](http://www.g8usa.gov) [Accessed: 23rd April 2006].
- Gerber, M. and Von Solms, R. V. (2001) From risk analysis to security requirements. *Computer & Security*, 20(7), pp. 577-584.
- Glass, R. (1995) A structure-based critique of contemporary computing research. *Journal of Systems and Software*, 28(1), pp. 3-7.
- Gordon, L. A. and Loeb, M. P. (2001) Economic aspects of information security. *Security Tech Trends Notes*, 110(4), pp. 8-15.
- Gordon, L. A. and Loeb, M. P. (2002) The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), pp. 438-457.
- Gordon, L. A. and Loeb, M. P. (2006) Budgeting process for information security expenditures. *Communications of the ACM*, 49(1), pp. 121-125.

## H

- Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004) Design science in information systems research. *MIS Quarterly*, 28(1), pp. 75-105.
- Hogganvik, I. and Stolen, K. (2005) Risk analysis terminology for IT-systems does it match intuition? *International Symposium on Empirical Software Engineering (ISESE)* pp.13-22.
- Hong, K. S., Chi, Y. P., Chao, L. R. and Tan, J. H. (2002) An integrated system theory of information security management. *Information Management & Compute Security*, 11(5), pp. 243-248.
- Hoo, K. J. (2000) *How much is enough? A risk management approach to computer security*. Consortium for Research on Information Security and Policy (CRISP), working paper.

## I

- Information Security Breaches Survey *ISBS (2008)* Department of Business, Enterprise & Regulatory Reform (BERR), UK. [online] Available from: [http://www.pwc.co.uk/eng/publications/berr\\_information\\_security\\_breaches\\_survey\\_2008.html](http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html)
- Information Security Forum ISF (2007) *The standard of good practice for information security*. Switzerland: Information Security Forum.
- Information Systems Audit and Control Association ISACA (2006) [online]. Available from: <http://www.isaca.org> [Accessed : 8 June 2007].
- Insight Consulting (2003) CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0. SIEMENS.
- International Standards Organization (1989) ISO/IEC 7498-2: 1989. *Information processing system-open systems interconnection-basic reference model-Part 2: Security architecture*. Geneva, Switzerland: International Standards Organization.

- International Standards Organization (1998) ISO/IEC TR 13335-3: 1998. *Information technology-guidelines for the management of IT security: Part 3*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2000) ISO/IEC 13335-4: 2000. *Information technology-guidelines for the management of IT security*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (1999) ISO/IEC Guide 51: 1999. *Safety aspects – Guidelines for their inclusion in standards*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2002) ISO/IEC Guide 73: 2002. *Risk management-vocabulary-guidelines for use in standards*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2004) ISO/IEC 13335-1: 2004. *Information technology-security techniques–management of information and communications technology security*. Geneva, Switzerland: International Standards Organization.
- International Standards organization (2005) ISO/IEC 27001: 2005. *Information technology-security techniques-information security management systems-requirements*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2005) ISO/IEC 27002: 2005. *Information technology-security techniques-code of practice for information security management*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2008) ISO/IEC 27005: 2008. *Information technology-security techniques-information security risk management*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2009) ISO/IEC 27000: 2009. *Information technology-security techniques-Information security management systems – overview and vocabulary*. Geneva, Switzerland: International Standards Organization.
- International Standards Organization (2009) ISO/IEC 27004: 2009. *Information technology-security techniques-information security management Measurement*. Geneva, Switzerland: International Standards Organization.
- ISO (2005) The Website of the International Organization of Standardization, [online]. Available from: <http://www.iso.org> [Accessed: 9th Novembre 2008].

## J

- Janczewski, L. and Xinli Shi, F. (2002) Development of information security baselines for healthcare information systems in NewZeland. *Computer & Security*, 21(2), pp. 172-192.
- Johansson, E. and Johnson, P. (2005) Assessment of enterprise information security – the importance of prioritization. *Proceedings of the Ninth IEEE International Enterprise Computing Conference -EDOC'05*. Enschede, The Netherlands, 19-23th Sept. 2005, IEEE, pp. 207-218.
- Johansson, E., Ekstedt, M. and Johnson, P. (2006) Assessment of enterprise information security: the importance of information search cost. *Proceedings of the 39<sup>th</sup> Hawaii International Conference on System Sciences-2006*. Hawaii, USA, 4-7 th January 2006, IEEE Computer Society, pp. 219a-219a .

Johnson, M. and Whitman, L. (1998) Enterprise engineering: a discipline for integrating people, processes and technologies in knowledge ear. *Proceedings of the Business Process and Knowledge Management Conference 1998*. Orlando, FL.

## K

Kailay, M. P. and Jarratt, P. (1995) RAMEX: a prototype expert system for computer security risk analysis and management. *Computer & Security*, 14(5), pp. 449-463.

Karabacak, B. and Sogukpinar, I. (2005) ISRAM: Information security risk analysis method. *Computer & Security*, 24(2), pp.147-159.

Karabacak, B. and Sogukpinar, I. (2006) A quantitative method for ISO 17799 gap analysis. *Computer & Security*, 25(6), pp. 413-419.

Khadraoui, D. and Hermann, F. (2007) *Advances in Enterprise Information Technology Security*. New York: Information Science Reference.

King, G. Keohane, R. O. and Verba, S. (1994) *Designing Social Inquiry*. Princeton University Press.

Kraemer, S., Carayon, P. and Clem, J. (2009) Human and organizational factors in computer and information security: pathways to vulnerabilities. *Computer and Security*, pp. 1-12.

## L

Lanz, J. (2002) Prioritising aspect of technology risk assessment and mitigation. *Bank Accounting & Finance*, 16(1), pp. 19-26.

Lech, J. & Frank, X. (2002) Development of information security baselines for healthcare information system. *Computer & Security*, 21(2), pp. 172-192.

Lee, W., Fan, W., Miller, M., Stolfo, S., and Zadok, E. (2002) Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, 10(1/2), pp. 5-22.

Liu, F. H. (2007) Constructing enterprise information network security risk management mechanism by using Ontology. *21th International Conference on Advanced Information Networking and Applications Workshop -AINAW'07*. Niagara Falls, Ontario, Canada, 21-23th May2007, IEEE computer society.

Liu, W., Tanaka, H. and Matsuura, K. (2006) An empirical analysis of security investment in countermeasures based on and enterprise survey in Japan. *Workshop on the Economics of Information Security 2006:WEIS 2006*. University of Cambridge, Cambridge, UK, June 2006.

## M

March, S. T. and Smith, G. F. (1995) Design and natural science research on information technology. *Decision Support Systems, Elsevier Science*, 15 (4), pp. 251-266.

Matulevicius, R. Nicolas, M. Haralambos, M. Eric, D. Patrick, H. and Nicolas, G. (2008) Adapting Secure Tropos for Security Risk Management during Early Phases of the Information Systems Development. *Springer Verlag, LNCS (5074)* pp. 541-555.

- Mayer, N., Dubois, E., Matulevicius, R., and Heymans, P. (2008) Towards a Measurement Framework for Security Risk Management. In *Modeling Security Workshop, in conjunction with the 11<sup>th</sup> International Conference on Model Driven Engineering Languages and Systems*. Toulouse, France.
- Mccarthy, M. P. and Campbell, S. (2001) *Security transformation*. New York: McGraw-Hill.
- McGrath, J. E. (1984) *Groups: Interaction and Performance*. Englewood- Cliffs, NJ: Prentice-Hall.
- Mehari (2007). Overview, Club de la Securite de l'Information Francais (CLUSIF).
- Mercuri, R. T. (2003) Analyzing security costs. *Communications of the ACM*, 46(6), pp. 15-18.
- Merriam – Webster Dictionary (2010) [online] Available from: <http://www.merriam-webster.com/>.
- Microsoft (2006) *The Security Risk Management Guide, Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence*. USA: Microsoft Corporation.
- Mizzi, A. (2005) Return on information security investment. Are you spending enough? Are you spending too much? *ACM IT Security Toolbox*.

## **N**

- National Infrastructure Protection Center NIPC. (2007) *Department of Justice*. USA: Federal Bureau of Investigation. [online] Available from: <http://www.nicp.gov/> [Accessed: 8th March 2008]
- National Institute of Standards and Technology (2001) NIST special publication 800-26:2001. *Security self-assessment guide for information technology systems*. USA: National Institute of Standards and Technology.
- National Institute of Standards and Technology (2002) NIST SP800-30: 2002. *Risk management guide for information technology systems*. USA: National Institute of Standards and Technology.
- National Institute of Standards and Technology (2006) NIST special publication 800-53:2006. *Recommended security controls for federal information systems*. USA: National Institute of Standards and Technology.
- National Institute of Standards and Technology (2008) NIST special publication 800-55:2008. *Performance Measurement Guide for Information Security*. USA: National Institute of Standards and Technology.
- NIST web site (2008) [online]. available from: <http://www.nist.gov/> [Accessed: 21st February 2009]

## **O**

- OCTAVE, (2005) Managing information security risk, Carnegie Mellon, USA.
- Office of Inspector General OIG (2007) *Department of Health and Human Services*. [online]. Available from: <http://oig.hhs.gov/> [Accessed: 26th May 2008]

## P

- Parasurman, A. (1986) *Marketing Research*. Addison-Wesley.
- Passori, A. (2004) *Selecting the Risk Assessment Method of Choice*. [online]. Available from:  
[http://searchcio.techtarget.com/originalContent/0,289142,sid19\\_gci994851\\_oo.html](http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci994851_oo.html) [Accessed: 6th August 2005].
- Patton, M. (1990) *Qualitative evaluation and research methods*. London: Sage Publications.
- Peffer, K., Tuunanen, T., Rothenberger, M. and Chatterjee, S. (2008) A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), pp. 45-77.
- Ponemon Institute (2009) *Annual Study: Enterprise Encryption Trends: 2009 Survey*, Ponemon Institute, UK.
- Purser, S. A. (2004) Improving the ROI of the security management process. *Computer & Security*, (23), pp. 542-546.
- Pyzdek, T. (2003) *The Six Sigma Handbook*. New York: McGraw-Hill.

## R

- Raptis, D., Dimitrakos, T., et al. (2002) The COARS approach for model-based risk analysis applied to the e-commerce domain. *In Proc. Communication and Multimedia Security –DMS*. Kluwer, pp.169-181.
- Raval, V. (2004) Guidelines for compliance with Sarbanes-Oxley EDPACS 31(7): 14-20.
- Robert, C. and Rolf, M. (2003) Operationalizing IT risk management. *Computer & Security*, 22(6), pp. 487-493.
- Roper C. A. (1999) *Risk Management for Security Professionals* Butterworth-Heinemann.
- Ryan, J. C. H. and Ryan, D. J. (2006) Expected benefits of information security investments. *Computer & Security*, 25(8), pp. 579-588.

## S

- Saleh, M.S. and Bakry, S.H. (2008) An overview of key IT risk management methods. *Saudi Computer Journal*, 6(2), pp. 61-70.
- Saleh, M.S., Alfantookh, A., Mellor, J.E. and Bakry, S.H. (2008) An open reference framework for enterprise information security risk management using the STOPE scope and the six-sigma process. *Proceedings of the Fourteenth Americas Conference on Information Systems*. Toronto, Canada, 14-17 th August 2008.
- Saleh, M.S., Alrabiah, A. and Bakry, S.H. (2006) Using ISO 17799-2005 security management standard: A STOPE view with six-sigma approach. *International Journal of Network Management*, Wiley, 17(1), pp. 85-97.
- Saleh, M.S., Alrabiah, A. and Bakry, S.H. (2007) A STOPE model for the investigation of compliance with ISO 17799-2005. *Information Management & Computer Security, Emerald*, 15(4), pp. 283-294.
- Saunders, M. Lewis, P. and Thornhill, A. (2007) *Research Methods for Business Students*. Prentice Hall.
- Schrecher, S. E. (2004) Toward econometric models of the security risk from remote attacks. *3rd Workshop on Economics and Information Security*. Las Vegas, Nevada, 13-14th May 2004, pp. 87-92.



- Simon, H. A. (1997) *The Sciences of the Artificial*. 3rd edn., Cambridge,MA: The MIT Press.
- Siponen, M. (2000) A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), pp.31-41.
- Smith, E. and Eloff, J.H.P. (2002) A prototype for assessing information technology risks in health care. *Computer & Security*, 21(3), pp.266-284.
- Solms, B. (2005) Information security governance: COBIT or ISO 17799 or both?. *Computer & Security*, 24(2), pp. 99-104.
- Solms, B. (2006) Information security—the fourth wave. *Computer & Security*, 25(3), pp. 165-168.
- Solms, B. and Von Solms, R. (2001) Incremental information security certification . *Computer & Security*, 20(4), pp. 308 – 310.
- Solms, E. and Eloff, J. H. P. (2002) *Information Security Development Trends*. Technical Report:2002. [Online]. Available from: <http://www.tarrani.net/InfoSecDevelopmentTrends.pdf> [Accessed: 26 th November 2006].
- Solms, R. (1999) Information security management: why standards are important. *Information Management & Computer Security*, 7(1), pp. 50-57.
- Sonnenreich, W., Albanese, J. and Stout, B. (2006) Return on security investment (ROSI) – a practical quantitative model. *Journal of Research and Practice in Information Technology*, 38(1), pp. 55-66.
- Stephenson, P. (2004) Risk and incident management – getting started. *Computer Fraud and Security*, (11), pp 17-19.
- Stolen, K. and Solheim, I. (2006) *Technology research explained*. SINTEF ICT Technical Report: 2006- A313.

## T

- Tanaka, H., Liu, W. and Matsuura, K. (2006) An empirical analysis of security investment in countermeasures based on an enterprise survey in Japan. *The Fifth Workshop on the Economics of Information Security (WEIS '06)*. University of Cambridge, UK., McGraw Hill.
- Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and information security investment:an impirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, 24(1), pp. 37-59.
- Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005) *The Insider Threat to Information Systems and the Effectiveness of ISO17799*. Elsevier: 2005.05.002.
- Tipton, H. and Krause, M. (2008) *Information Security Management Handbook*. 6th edn., New York : Auerbach Publications. Taylor and Francis Group.
- Tipton, H. and Krause, M. (2010) *Information Security Management Handbook*. Auerbach Publications, New York: Taylor and Francis Group.
- Tong, C. K. S., Fung, K. H., Huang, H. Y. H. and Chan, K. K. (2003) Implementation of ISO17799 and BS7799 in Picture Archiving and Communication System: Local Experience in Implementation of BS7799 Standard. *International Congress Series*, 1256, pp. 311-318.
- Tsiakis, T. and Stephanides, G. (2005) The economic approach of information security. *Computer & Security*, 24(2), pp. 105-108.

Tsoumas, V. and Tryfonas, T. (2004) From risk analysis to effective security management: towards an automated approach. *Information Management & Computer Security*, 12(1) pp. 91-101.

## U

UN Millennium Development Goals (2000) [online] Available from: [www.developmentgoals.org](http://www.developmentgoals.org) [Accessed: 28 th July 2006]

## V

Vennaro, N. (2005) *Enterprise Risk Assessment Overview*. [online]. Available from: <http://www.AegisSecurityWorks.com> [Accessed: 6 th August 2008].

Venter, H. S. and Eloff, J. H. P. (2003) A taxonomy of information security technologies. *Computer and Security*, 22(4), pp. 299-307.

Vraalsen, F., Braber, F., Lund, M., and Stolen, K. (2005) The CORAS Tool for Security Risk Analysis. LNCS 3477, pp. 402-405.

## W

Wang, A. (2005) Information Security Models and Metrics. In Proceedings of the 43<sup>rd</sup> annual Southeast regional conference.

Warren, M. and Hutchinson, W. (2003) A security risk management approach for e-commerce. *Information Management & Computer Security*, 11(5), pp. 238-242.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), pp. 4-19.

Whitman, M. E. and Mattord, H. J. (2004) *Management of Information Security Course Technology*. ISBN 978-1-4239-0130-3 Boston: MA.

Wiander, T. (2007) Positive and Negative Findings of the ISO/IEC 17799 Framework. *18<sup>th</sup> Australian Conference on Information Systems 5-7 Dec 2007, Toowooba*.

## X

Xie, N. and Mead, N. R. (2004) SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies. US department of defense.

## Y

Yin, R. K. (1996) *Case Study Research: Design and Methods*. 2nd edn., London: Sage Publications.

**PART VII**  
**APPENDIXES**

# Appendix A

## THE INVESTIGATION FORM

### **Enterprise Information Security Readiness Assessment Questionnaire**

This investigation form is associated with a research project which is concerned with the assessment of the effective use of the ISO/IEC 27002 information security management standard by different enterprises. The assessment is based on a developed multi level structure analytical model that presents the results numerically and graphically at different levels of the model, according to the ISO/IEC 27002 standard.

Your response and comments will be treated with utmost confidentiality. The information collected will neither be used to identify individuals or individual enterprises, nor will it be publicly disseminated. Space is also provided for open-ended responses. We encourage you to share with us anything you think might be useful in terms of supporting IT security efforts.

Please complete the enclosed questionnaire. Your candid and thoughtful reply will help in providing reliable results that can be useful for the future improvement of information security.

The following is a detailed list of information security measures associated with assessment questions. Please answer the questions and give your view of the performance of using these measures for assessing information security inside your respectable enterprise. Five levels of performance grades are given, as explained in the following Table.

### Performance

0	1	2	3	4
None	Poor	Good	Very good	Excellent

Domain 1 :Technology		Performance				
<b>Clause 1:Communication and operations management</b>						
<b>Objective 1:Operational procedures and responsibilities</b>						
<b>Control 1:Documented operating procedures</b>						
1	Do you have documented procedures for system activities?	0	1	2	3	4
2	Does management authorise the changes in operating procedures?	0	1	2	3	4
3	Are operating procedures documents available to the right users?	0	1	2	3	4
<b>Control 2:Change management</b>						
4	Do you formally control the changes to information processing facilities?	0	1	2	3	4
5	Do you have audit logs for the changes in processing facilities?	0	1	2	3	4
<b>Control 3:Segregation of duties</b>						
6	Do you segregate duties to reduce unauthorised modification of assets?	0	1	2	3	4
7	Do you segregate areas of responsibility to reduce misuse of assets?	0	1	2	3	4
<b>Control 4:Separation of development, test and operational facilities</b>						
8	Do you separate development, test and operational facilities?	0	1	2	3	4
<b>Objective 2:Third party service delivery management</b>						
<b>Control 5:Service delivery</b>						
9	Do you ensure the implementation of the third party service delivery agreement?	0	1	2	3	4
10	Do you ensure third party service delivery agreement services operation?	0	1	2	3	4
11	Do you maintain the included services in third party service delivery agreement?	0	1	2	3	4
<b>Control 6:Monitoring and review of third party services</b>						
12	Do you regularly monitor services, reports and records provided by the third party?	0	1	2	3	4
13	Do you regularly review service, reports and records provided by the third party?	0	1	2	3	4
14	Do you regularly audit services, reports and records provided by the third party?	0	1	2	3	4
<b>Control 7:Managing changes to third party services</b>						
15	Do you manage changes to the provision of services provided by third party?	0	1	2	3	4
16	Do you consider the criticality of business systems and process in managing changes to the provision of services provided by the third party?	0	1	2	3	4
<b>Objective 3:System planning and acceptance</b>						
<b>Control 8:Capacity management</b>						
17	Do you monitor resources use to ensure the required system performance?	0	1	2	3	4
18	Do you tune resources use to ensure the required system performance?	0	1	2	3	4
19	Do you project future capacity requirements to ensure system performance?	0	1	2	3	4
<b>Control 9:System acceptance</b>						
20	Do you establish acceptance criteria for information systems?	0	1	2	3	4
21	Do you have suitable tests for the systems against the acceptance criteria?	0	1	2	3	4
<b>Objective 4:Protection against malicious and mobile code</b>						
<b>Control 10:Controls against malicious code</b>						
22	Do you have controls for detections of malicious code?	0	1	2	3	4
23	Do you have controls for prevention of malicious code?	0	1	2	3	4
24	Do you have controls for recovery from malicious code?	0	1	2	3	4
25	Do you implement appropriate user awareness procedures?	0	1	2	3	4
<b>Control 11:Controls against mobile code</b>						
26	Do you have suitable security policy for the operation of mobile codes?	0	1	2	3	4
27	Do you have control to prevent the execution of unauthorised mobile code?	0	1	2	3	4
<b>Objective 5:Back-up</b>						
<b>Control 12:Information back-up</b>						
28	Do you have an agreed backup policy?	0	1	2	3	4
29	Do you have a procedure for regularly taking backup of information and software?	0	1	2	3	4
30	Do you have a procedure for regularly testing backup of information and software?	0	1	2	3	4
<b>Objective 6:Network security management</b>						
<b>Control 13:Network controls</b>						
31	Do you have adequate management procedures to protect the network from threats?	0	1	2	3	4
32	Do you have adequate controls to protect the network from threats?	0	1	2	3	4

<b>Control 14:Security of network services</b>						
33	Do you identify security features, service levels and management requirements of all network services?	0	1	2	3	4
34	Do you include security features, service levels and management requirements of all network services in the in-house network service agreement?	0	1	2	3	4
35	Do you include security features, service levels and management requirements of all network services in the outsource network service agreement?	0	1	2	3	4
<b>Objective 7:Media handling</b>						
<b>Control 15:Management of removable media</b>						
36	Do you have management procedures for the removable media?	0	1	2	3	4
<b>Control 16:Disposal of media</b>						
37	Do you have formal procedures for securely disposing the media?	0	1	2	3	4
38	Do you have formal procedures for safely disposing the media?	0	1	2	3	4
<b>Control 17:Information handling procedures</b>						
39	Do you establish procedures for handling information against unauthorised disclosure or misuse?	0	1	2	3	4
40	Do you establish procedures for the storage of unauthorised disclosure or misuse of information?	0	1	2	3	4
<b>Control 18:Security of system documentation</b>						
41	Do you protect the system documentation from unauthorised access?	0	1	2	3	4
<b>Objective 8:Exchange of information</b>						
<b>Control 19:Information exchange policies and procedures</b>						
42	Do you have formal exchange policies to protect information through the use of all types of communication facilities?	0	1	2	3	4
43	Do you have procedures to protect information through the use of all types of communication facilities?	0	1	2	3	4
44	Do you have controls to protect information through the use of all types of communication facilities?	0	1	2	3	4
<b>Control 20:Exchange agreements</b>						
45	Do you establish an agreement with external parties for the exchange of information?	0	1	2	3	4
46	Do you establish an agreement with external parties for the exchange of software?	0	1	2	3	4
<b>Control 21:Physical media in transit</b>						
47	Do you establish procedures to protect media containing information against unauthorised access, misuse or corruption during transportation?	0	1	2	3	4
<b>Control 22:Electronic messaging</b>						
48	Do you appropriately protect the information included in electronic messages?	0	1	2	3	4
<b>Control 23:Business information systems</b>						
49	Do you develop policies and procedures to protect information associated with the interconnection of business information systems?	0	1	2	3	4
50	Do you implement policies and procedures to protect information associated with the interconnection of business information systems?	0	1	2	3	4
<b>Objective 9:Electronic commerce services</b>						
<b>Control 24:Electronic commerce</b>						
51	Do you have protection measures for information involved in electronic commerce against fraudulent activity, contract dispute and modification?	0	1	2	3	4
<b>Control 25:On-Line transactions</b>						
52	Do you have protection measures for on-line transactions?	0	1	2	3	4
<b>Control 26:Publicly available information</b>						
53	Do you have protection measures to protect the integrity of publicly available information?	0	1	2	3	4
<b>Objective 10:Monitoring</b>						
<b>Control 27:Audit logging</b>						
54	Do you produce audit logs for recording user activities, exceptions and information security events?	0	1	2	3	4
55	Do you keep the audit logs for an agreed period of time to assist in future investigation and access control monitoring?	0	1	2	3	4
<b>Control 28:Monitoring system use</b>						
56	Do you establish procedures for monitoring the use of information processing facilities?	0	1	2	3	4
57	Do you regularly review the results of the monitoring activities?	0	1	2	3	4
<b>Control 29:Protection of log information</b>						
58	Do you protect the logging facilities and the log information against tampering?	0	1	2	3	4
59	Do you protect the logging facilities and the log information against unauthorised access?	0	1	2	3	4
<b>Control 30:Administrator and operator logs</b>						
60	Do you have a log file for system administrator activities?	0	1	2	3	4
61	Do you have a log file for system operator activities?	0	1	2	3	4
<b>Control 31:Fault logging</b>						
62	Do you log the reported faults by users or by system's programs?	0	1	2	3	4
63	Do you analyse the reported faults?	0	1	2	3	4
64	Do you take an appropriate action for the reported faults?	0	1	2	3	4
<b>Control 32:Clock synchronisation</b>						
65	Do you synchronize the clocks of all relevant information processing systems with an agreed accurate time source?	0	1	2	3	4

<b>Clause 2: Access Controls</b>						
<b>Objective 11: Business requirements for access control</b>						
<b>Control 33: Access control policy</b>						
66	Do you establish an access control policy based on business and security requirements?	0	1	2	3	4
67	Do you document the access control policy?	0	1	2	3	4
68	Do you regularly review the access control policy?	0	1	2	3	4
<b>Objective 12: User access management</b>						
<b>Control 34: User registration</b>						
69	Do you have formal user registration procedures for gaining access to all information systems and services?	0	1	2	3	4
70	Do you have formal user de-registration procedures for revoking access to all information systems and services?	0	1	2	3	4
<b>Control 35: Privilege management</b>						
71	Do you restrict the allocation of privileges?	0	1	2	3	4
72	Do you control the use of privileges?	0	1	2	3	4
<b>Control 36: User password management</b>						
73	Do you have formal management process for allocation of passwords?	0	1	2	3	4
<b>Control 37: Review of user access rights</b>						
74	Do you have formal management process for regular review of users' access rights?	0	1	2	3	4
<b>Objective 13: User responsibilities</b>						
<b>Control 38: Password use</b>						
75	Do you advise the users to follow good security practices in the selection of passwords?	0	1	2	3	4
76	Do you advise the users to follow good security practices in the use of their passwords?	0	1	2	3	4
<b>Control 39: Unattended user equipment</b>						
77	Do you have appropriate protection for the unattended equipments?	0	1	2	3	4
<b>Control 40: Clear desk and clear screen policy</b>						
78	Do you adopt a clear desk policy for papers & removable storage media?	0	1	2	3	4
79	Do you adopt a clear screen policy for information processing facilities?	0	1	2	3	4
<b>Objective 14: Network access control</b>						
<b>Control 41: Policy on use of network services</b>						
80	Do you restrict access to services to the authorised users?	0	1	2	3	4
<b>Control 42: User authentication for external connections</b>						
81	Do you have appropriate authentication methods to control access by remote users?	0	1	2	3	4
<b>Control 43: Equipment identification in networks</b>						
82	Do you have an automatic equipment identification to authenticate connections from specific locations and equipments?	0	1	2	3	4
<b>Control 44: Remote diagnostic and configuration port protection</b>						
83	Do you have appropriate controls on physical and logical access to diagnostic ports?	0	1	2	3	4
84	Do you have appropriate controls on physical and logical access to configuration ports?	0	1	2	3	4
<b>Control 45: Segregation in networks</b>						
85	Do you segregate the groups of information services, users and information systems?	0	1	2	3	4
<b>Control 46: Network connection control</b>						
86	Do you restrict the capability of users to connect with the network according to the access control policy?	0	1	2	3	4
87	Do you restrict the capability of users to connect with the network according to the requirements of the business application?	0	1	2	3	4
<b>Control 47: Network routing control</b>						
88	Do routing controls meet the access control policy?	0	1	2	3	4
<b>Objective 15: Operating system access control</b>						
<b>Control 48: Secure log-on procedures</b>						
89	Do you control the access to operation systems by security log-on procedure?	0	1	2	3	4
90	Do you design a procedure for logging into operating system to minimise the opportunity for unauthorised access?	0	1	2	3	4
<b>Control 49: User identification and authentication</b>						
91	Does each user have unique identifier (user ID) for his personal use only?	0	1	2	3	4
92	Do you have authentication technique that substantiates the claimed identity of a user?	0	1	2	3	4
<b>Control 50: Password management system</b>						
93	Do you use interactive password management system?	0	1	2	3	4
94	Does the password management system ensure the quality of passwords?	0	1	2	3	4
<b>Control 51: Use of system utilities</b>						
95	Do you restrict the use of utility programmes that might be capable of overriding system and application controls?	0	1	2	3	4
96	Do you tightly control the use of utility programmes?	0	1	2	3	4
<b>Control 52: Session time-out</b>						
97	Do you have sessions shutdown policy for inactive sessions?	0	1	2	3	4
<b>Control 53: Limitation of connection time</b>						
98	Do you have additional restrictions on connection time limit for high-risk applications?	0	1	2	3	4
<b>Objective 16: Application and information access control</b>						
<b>Control 54: Information access restriction</b>						
99	Do you control the access to information and application system functions by the access control policy?	0	1	2	3	4
100	Do you base the restriction of the access to information and application system functions on individual business application requirements?	0	1	2	3	4

<b>Control 55:Sensitive system isolation</b>						
101	Do you have an isolated environment for sensitive systems?	0	1	2	3	4
<b>Objective 17:Mobile computing and teleworking</b>						
<b>Control 56:Mobile computing and communications</b>						
102	Do you have security policy for protection against the risks of using mobile computing and communication facilities?	0	1	2	3	4
103	Do you have the appropriate security measures against the risks of using mobile computing and communication facilities?	0	1	2	3	4
<b>Control 57:Teleworking policy for use</b>						
104	Do you develop and implement policy for teleworking activities?	0	1	2	3	4
105	Do you develop and implement operational plans to control teleworking activities?	0	1	2	3	4
106	Do you develop and implement procedures to control teleworking activities?	0	1	2	3	4
<b>Clause 3:Information systems acquisition, development and maintenance</b>						
<b>Objective 18:Security requirement of information systems</b>						
<b>Control 58:Security requirements analysis and specification</b>						
107	Do you specify the security controls requirements in the statements of business requirements for new or enhancements to existing information systems?	0	1	2	3	4
108	Do you analysis the controls requirements for new or enhancements to existing information systems?	0	1	2	3	4
<b>Objective 19:Correct processing in applications</b>						
<b>Control 59:Input data validation</b>						
109	Do you validate the input data to applications to ensure its correctness & appropriateness?	0	1	2	3	4
<b>Control 60:Control of internal processing</b>						
110	Do you incorporate validation checks into applications to detect the corruption of information through processing errors or deliberate acts?	0	1	2	3	4
<b>Control 61:Message integrity</b>						
111	Do you identify the requirements for ensuring authenticity and protecting message integrity in applications?	0	1	2	3	4
112	Do you implement the appropriate controls for ensuring authenticity and for protecting message integrity?	0	1	2	3	4
<b>Control 62:Output data validation</b>						
113	Do you validate the output data from an application to ensure that the processing of stored information is correct and appropriate?	0	1	2	3	4
<b>Objective 20:Cryptographic controls</b>						
<b>Control 63:Policy on the use of cryptographic controls</b>						
114	Do you develop a policy for cryptographic controls?	0	1	2	3	4
115	Do you implement the policy for the use of cryptographic controls?	0	1	2	3	4
<b>Control 64:Key management</b>						
116	Do you have a key management policy?	0	1	2	3	4
117	Do you protect all cryptographic keys against modification, loss and destruction?	0	1	2	3	4
<b>Objective 21:Security of system files</b>						
<b>Control 65:Control of operational software</b>						
118	Do you have procedures for controlling the installation of software on operational system?	0	1	2	3	4
<b>Control 66:Protection of system test data</b>						
119	Do you carefully select the test data?	0	1	2	3	4
120	Do you protect and control the test data?	0	1	2	3	4
<b>Control 67:Access control to program source code</b>						
121	Do you restrict access to the programme source code?	0	1	2	3	4
<b>Objective 22:Security in development and support process</b>						
<b>Control 68:Change control procedures</b>						
122	Do you have formal control procedures for controlling the implementation of changes?	0	1	2	3	4
<b>Control 69:Technical review of applications after operating system changes</b>						
123	Do you review the business critical applications after the change of operating systems?	0	1	2	3	4
124	Do you test the business critical applications after the change of operating systems?	0	1	2	3	4
<b>Control 70:Restrictions on changes to software packages</b>						
125	Do you discourage the modifications to software packages?	0	1	2	3	4
126	Do you limit the modifications to software packages?	0	1	2	3	4
127	Do you control the modifications to software packages?	0	1	2	3	4
<b>Control 71:Information leakage</b>						
128	Do you prevent the opportunities for information leakage?	0	1	2	3	4
<b>Control 72:Outsourced software development</b>						
129	Do you supervise the development of outsourced software?	0	1	2	3	4
130	Do you monitor the development of outsourced software?	0	1	2	3	4
<b>Objective 23:Technical vulnerability management</b>						
<b>Control 73:Control of technical vulnerabilities</b>						
131	Do you obtain timely information about technical vulnerabilities?	0	1	2	3	4
132	Do you evaluate the organisation's exposure to the identified vulnerabilities?	0	1	2	3	4
133	Do you take appropriate measures to address the associated risk to the identified vulnerabilities?	0	1	2	3	4



Domain 2: Organisation		Performance				
<b>Clause 1: Security policy</b>						
<b>Objective 1: Information security policy</b>						
<b>Control 1: Information security policy document</b>						
1	Does management approve the information security policy?	0	1	2	3	4
2	Do you publish the information security in the enterprise?	0	1	2	3	4
3	Do employees & external parties have access to the information security policy?	0	1	2	3	4
<b>Control 2: Review of the information security policy</b>						
4	Do you review the information security policy at planned intervals?	0	1	2	3	4
5	Do you review the information security policy when significant changes occur?	0	1	2	3	4
<b>Clause 2: Organisation of information security</b>						
<b>Objective 2: Internal organisation</b>						
<b>Control 3: Management commitment to information security</b>						
6	Does the management have clear direction to support enterprise security?	0	1	2	3	4
7	Does the management demonstrate commitment to support enterprise security?	0	1	2	3	4
8	Does the management have explicit assignment of responsibilities for supporting enterprise security?	0	1	2	3	4
<b>Control 4: Information security co-ordination</b>						
9	Are information security activities co-ordinated by representatives from different parts of the enterprise with relevant roles?	0	1	2	3	4
10	Are information security activities co-ordinated by representatives from different parts of the enterprise with relevant job functions?	0	1	2	3	4
<b>Control 5: Allocation of information security responsibilities</b>						
11	Do you clearly define the information security responsibilities?	0	1	2	3	4
12	Do you document in detail the entity responsible for each asset or security process?	0	1	2	3	4
<b>Control 6: Authorisation process for information processing facilities</b>						
13	Do you identify a management authorisation process for new information processing facilities?	0	1	2	3	4
14	Do you implement the management authorisation process for new information processing facilities?	0	1	2	3	4
<b>Control 7: Confidentiality agreements</b>						
15	Do you identify a confidentiality agreement that reflects enterprise's needs for the protection of information?	0	1	2	3	4
16	Do you regularly review the confidentiality agreement to make sure that it covers the new requirements for protecting enterprise information?	0	1	2	3	4
<b>Control 8: Contact with authorities</b>						
17	Do you maintain appropriate contacts with relevant authorities?	0	1	2	3	4
18	Do you have procedures that specify when and by whom relevant authorities should be contacted?	0	1	2	3	4
<b>Control 9: Contact with special interest groups</b>						
19	Do you maintain appropriate contacts with special interest groups?	0	1	2	3	4
20	Do you maintain appropriate contacts with special security forums?	0	1	2	3	4
21	Do you maintain appropriate contacts with professional associations?	0	1	2	3	4
<b>Control 10: Independent review of information security</b>						
22	Do you review independently at planned intervals the enterprise's approach for managing information security?	0	1	2	3	4
23	Do you review the enterprise's approach for managing information when significant changes occur?	0	1	2	3	4
<b>Objective 3: External parties</b>						
<b>Control 11: Identification of risks related to external parties</b>						
24	Do you identify risks to the enterprise's information processing facilities from business processes involving external parties before granting access?	0	1	2	3	4
25	Do you implement appropriate controls to the enterprise's information processing facilities before granting access to external parties?	0	1	2	3	4
<b>Control 12: Addressing security when dealing with customers</b>						
26	Are the security requirements addressed before giving customers access to the enterprise's information?	0	1	2	3	4
27	Are the security requirements addressed before giving customers access to the enterprise's assets?	0	1	2	3	4
<b>Control 13: Addressing security in third party agreements</b>						
28	Are the agreements with the third parties involving all relevant security requirements in accessing information processing facilities?	0	1	2	3	4
29	Are the agreements with the third parties involving all relevant security requirements in processing information processing facilities?	0	1	2	3	4
30	Are the agreements with the third parties involving all relevant security requirements in communicating information processing facilities?	0	1	2	3	4
<b>Clause 3: Asset management</b>						
<b>Objective 4: Responsibility of assets</b>						
<b>Control 14: Inventory of assets</b>						
31	Do you clearly identify all the enterprise's assets?	0	1	2	3	4
32	Do you have inventory of all important assets?	0	1	2	3	4
33	Do you have a procedure to maintain the inventory of all important assets?	0	1	2	3	4

<b>Control 15:Ownership of assets</b>					
34	Do you classify information and assets associated with information processing facilities?	0	1	2	3 4
35	Do you assign relevant owners to the enterprise information and assets associated with information processing facilities?	0	1	2	3 4
<b>Control 16:Acceptable use of assets</b>					
36	Do you identify rules that define the acceptable use of information and assets associated with information processing facilities?	0	1	2	3 4
37	Do you document the rules that define the acceptable use of information and assets associated with information processing facilities?	0	1	2	3 4
38	Do you implement rules that define the acceptable use of information and assets associated with information processing facilities?	0	1	2	3 4
<b>Objective 5:Information classification</b>					
<b>Control 17:Classification guidelines</b>					
39	Do you classify information according to its value to the enterprise?	0	1	2	3 4
40	Do you classify information according to the legal requirements?	0	1	2	3 4
41	Do you classify information according to its sensitivity to the enterprise?	0	1	2	3 4
42	Do you classify information according to its criticality to the enterprise?	0	1	2	3 4
<b>Control 18:Information labelling and handling</b>					
43	Do you develop procedures for information labelling and handling?	0	1	2	3 4
44	Do you implement procedures for information labelling and handling?	0	1	2	3 4
<b>Clause 4:Information security incident management</b>					
<b>Objective 6:Reporting information security events and weaknesses</b>					
<b>Control 19:Reporting information security events</b>					
45	Do you have a formal information security event reporting procedure?	0	1	2	3 4
46	Do you have a known point of contact for the reporting of information security events?	0	1	2	3 4
47	Are all employees, contractors and third party users aware of their responsibility to report any information security events as quickly as possible?	0	1	2	3 4
<b>Control 20:Reporting security weakness</b>					
48	Do you have an easily accessible and available reporting mechanism for the security weaknesses in systems and services?	0	1	2	3 4
49	Are employees, contractors and third party users informed to report the security weaknesses in systems and services as quickly as possible?	0	1	2	3 4
<b>Objective 7:Management of information security incidents and improvements</b>					
<b>Control 21:Responsibilities and procedures</b>					
50	Do you establish management responsibilities to ensure quick, effective and orderly response to information security incidents?	0	1	2	3 4
51	Do you establish management procedures to ensure quick, effective and orderly response to information security incidents?	0	1	2	3 4
52	Do you ensure that those responsible for information security incident management understand the enterprise's priorities for handling information security incidents?	0	1	2	3 4
<b>Control 22:Learning from information security incidents</b>					
53	Do you have mechanisms to quantify and monitor security incidents according to their type?	0	1	2	3 4
54	Do you evaluate the information security incidents to identify the recurring incidents?	0	1	2	3 4
55	Do you evaluate the information security incidents to identify the high impact incidents?	0	1	2	3 4
<b>Control 23:Collection of evidence</b>					
56	Do you develop internal procedures to be followed in collecting evidence that conform to the rules for evidence laid down in the relevant jurisdiction?	0	1	2	3 4
57	Do you develop internal procedures to be followed in presenting evidence that conform to the rules for evidence laid down in the relevant jurisdiction?	0	1	2	3 4
58	Do you have mechanism to ensure that no forensics work is performed on original evidential material?	0	1	2	3 4
<b>Clause 5:Business continuity management</b>					
<b>Objective 8:Information security aspects of business continuity management</b>					
<b>Control 24:Including information security in the business continuity management process</b>					
59	Do you develop a management process for addressing information security requirements of business continuity?	0	1	2	3 4
60	Do you maintain the management process which addresses information security requirements for business continuity?	0	1	2	3 4
<b>Control 25:Business continuity and risk assessment</b>					
61	Do you identify events that can cause interruptions to business processes?	0	1	2	3 4
62	Do you identify the impact of the interruptions to business processes?	0	1	2	3 4
<b>Control 26:Developing and implementing continuity plans including information security</b>					
63	Do you develop plans to maintain operations and ensure availability of information?	0	1	2	3 4
64	Do you implement plans to maintain operations and ensure availability of information?	0	1	2	3 4
<b>Control 27:Business continuity planning framework</b>					
65	Do you have a single framework of business continuity plans?	0	1	2	3 4
66	Does the business continuity framework address the information security requirements?	0	1	2	3 4
67	Do you assign specific owners for each plan that is responsible for emergency procedures, manual fallback plans and resumption plans?	0	1	2	3 4
<b>Control 28:Testing, maintaining and re-assessing business continuity plans</b>					
68	Do you test the business continuity plans to ensure that all members of the recovery team and other relevant staff are aware of these plans?	0	1	2	3 4
69	Do you regularly update business continuity plans to ensure they are up to date & effective?	0	1	2	3 4

Domain 3: People		Performance				
<b>Clause 1: Human resources security</b>						
<b>Objective 1: Prior to employment</b>						
<b>Control 1: Roles and responsibilities</b>						
1	Do you define and document roles and responsibilities of employees, contractors and third party users?	0	1	2	3	4
2	Are the security roles and responsibilities of employees, contractors and third party users clearly communicated before job assignment?	0	1	2	3	4
3	Are the security roles and responsibilities of employees, contractors and third party users comply with the enterprise information security policy?	0	1	2	3	4
<b>Control 2: Screening</b>						
4	Do you have background verification checks on all users (candidates for employment, contractors and third party) in accordance with relevant laws, regulations and ethics?	0	1	2	3	4
5	Do verification checks take into account all relevant privacy and protection of personal data legislation?	0	1	2	3	4
6	Do you have procedures that define criteria and limitations of verification checks?	0	1	2	3	4
<b>Control 3: Terms and conditions of employment</b>						
7	Do the employees, contractors and third party users agree and sign terms and conditions of their employment contract?	0	1	2	3	4
8	Do you use clear job descriptions to define the security responsibilities for new employees, contractors and third party users?	0	1	2	3	4
9	Are the terms and conditions of employment contract clearly state the actions to be taken if the employee, contractor or third party users disregard the enterprise's security requirements?	0	1	2	3	4
<b>Objective 2: During employment</b>						
<b>Control 4: Management responsibilities</b>						
10	Does management require employees, contractors and third party users to apply security in accordance with the enterprise established policies and procedures?	0	1	2	3	4
11	Does management motivate employees, contractors and third party to fulfil the enterprise security policies?	0	1	2	3	4
12	Does management continue to have personnel with appropriate security skills and qualifications?	0	1	2	3	4
<b>Control 5: Information security awareness, education and training</b>						
13	Do employees, contractors and third party users receive appropriate awareness before access to information or services is granted?	0	1	2	3	4
14	Do employees, contractors and third party users receive ongoing training that includes security requirements, legal responsibilities and business controls?	0	1	2	3	4
15	Does the awareness program include information on known threats, and the contact person for further security advice?	0	1	2	3	4
<b>Control 6: Disciplinary process</b>						
16	Do you have a formal disciplinary process for employees who have committed a security breach?	0	1	2	3	4
17	Does the disciplinary process provide graduated response that takes into consideration the impact of the violation on the business?	0	1	2	3	4
18	Does the disciplinary process allow instant removal of duties, access rights and privileges and immediate escorting out of the site?	0	1	2	3	4
<b>Objective 3: Termination or change of employment</b>						
<b>Control 7: Termination responsibilities</b>						
19	Do you have a clear definition of responsibilities for performing termination of employment?	0	1	2	3	4
20	Do you have a clear definition of responsibilities for performing change of employment?	0	1	2	3	4
<b>Control 8: Return of assets</b>						
21	Does the termination process include formalised procedures for employees, contractors and third party users to return all assets in their possession upon termination of their work?	0	1	2	3	4
22	Does the termination process include formalised procedures to ensure that all relevant information is transferred to the enterprise and securely erased from the outside users' equipments?	0	1	2	3	4
23	Does the termination process include formalised procedures to ensure that important information of ongoing operations of the enterprise possessed by the employees, contractors and third party users are documented and transferred to the enterprise?	0	1	2	3	4
<b>Control 9: Removal of access rights</b>						
24	Are the users' access rights removed upon termination, or adjusted upon change?	0	1	2	3	4
25	Do you have a policy to reduce access rights before the employment termination?	0	1	2	3	4

Domain 4:Environment		Performance				
<b>Clause 1:Physical and environmental security</b>						
<b>Objective 1:Secure areas</b>						
<b>Control 1:Physical security perimeter</b>						
1	Do you clearly define the enterprise security perimeters?	0	1	2	3	4
2	Do you use security perimeters (barriers, walls and card controlled entry gates) to protect areas that contain information processing facilities?	0	1	2	3	4
3	Do you monitor the fire doors on the enterprise security perimeters?	0	1	2	3	4
<b>Control 2:Physical entry controls</b>						
4	Do you protect the secure areas by appropriate entry controls to ensure authorised use?	0	1	2	3	4
5	Do you require employees, contractors, third party users and all visitors to wear some form of visible identifications?	0	1	2	3	4
6	Do you restrict the access to areas where sensitive information is processed or stored to authorised persons only?	0	1	2	3	4
<b>Control 3:Securing offices, rooms and facilities</b>						
7	Do you design and apply physical protection for offices, rooms and facilities?	0	1	2	3	4
8	Do you hide the information about locations of sensitive information security processing facilities from the public?	0	1	2	3	4
<b>Control 4:Protection against external and environmental threats</b>						
9	Do you design and apply proper physical protection against environmental threats?	0	1	2	3	4
10	Do you provide appropriate fire fighting equipment that is placed in suitable places?	0	1	2	3	4
<b>Control 5:Working in secure areas</b>						
11	Do you have guidelines for working in secure areas?	0	1	2	3	4
12	Do you make sure that vacant secure areas are physically locked and checked periodically?	0	1	2	3	4
13	Do you restrict the use of photographic, video and audio equipments in the secure areas?	0	1	2	3	4
<b>Control 6:Public access, delivery and loading areas</b>						
14	Do you isolate the access points, delivery and loading areas, from information processing facilities areas?	0	1	2	3	4
15	Do you secure external doors for delivery and loading when internal doors are opened?	0	1	2	3	4
16	Do you physically segregate incoming and outgoing shipments?	0	1	2	3	4
<b>Objective 2:Equipment security</b>						
<b>Control 7:Equipment sitting and protection</b>						
17	Do you protect enterprise's equipments from environmental threats and hazards?	0	1	2	3	4
18	Do you protect enterprise's equipment from unauthorised access?	0	1	2	3	4
<b>Control 8:Supporting utilities</b>						
19	Do you protect enterprise's equipments from power failures?	0	1	2	3	4
20	Do you protect enterprise's equipments from disruptions caused by failures in supporting utilities?	0	1	2	3	4
<b>Control 9:Cabling security</b>						
21	Are the telecommunication cables carrying data or supporting information services protected from interception?	0	1	2	3	4
22	Do you segregate power cables from communication cables?	0	1	2	3	4
<b>Control 10:Equipment maintenance</b>						
23	Do you maintain equipment according to the supplier's recommendations and specifications?	0	1	2	3	4
24	Do you have records of all suspected or actual faults, and all preventive and corrective maintenance?	0	1	2	3	4
<b>Control 11:Security of equipment off-premises</b>						
25	Does the management have procedure to authorise the use of any information processing equipments outside the enterprise's premises?	0	1	2	3	4
26	Do you have adequate insurance that protects equipments off-site?	0	1	2	3	4
<b>Control 12:Secure disposal or re-use of equipment</b>						
27	Do you check all items of equipments which contain storage media prior to disposal?	0	1	2	3	4
28	Do you overwrite or delete licensed software prior to disposal?	0	1	2	3	4
29	Do you have techniques to make the deleted enterprise sensitive information non-retrievable?	0	1	2	3	4
<b>Control 13:Removal of property</b>						
30	Do you require prior authorisation for off-site moving of equipments?	0	1	2	3	4
31	Do you identify employees, contractors and third party users who have authority to permit off-site removal of assets?	0	1	2	3	4
32	Do you have a process to record the removed off-site equipment and record when returned?	0	1	2	3	4
<b>Clause 2:Compliance</b>						
<b>Objective 3:Compliance with legal requirements</b>						
<b>Control 14:Identification of applicable legislation</b>						
33	Do you explicitly define all relevant statutory, regulatory and contractual requirements for each system?	0	1	2	3	4
34	Do you explicitly document all relevant statutory, regulatory and contractual requirements for each system?	0	1	2	3	4
35	Do you keep all relevant statutory, regulatory and contractual requirements for each system up to date?	0	1	2	3	4

<b>Control 15: Intellectual property rights (IPR)</b>						
36	Do you implement procedures that ensure compliance with legislative requirements for the use of material and software?	0	1	2	3	4
37	Do you implement procedures that ensure compliance with regulatory requirements for the use of material and software?	0	1	2	3	4
38	Do you implement procedures that ensure compliance with contractual requirements for the use of material and software?	0	1	2	3	4
<b>Control 16: Protection of organisational records</b>						
39	Do you protect the important records from loss in accordance with statutory, regulatory, contractual and business requirements?	0	1	2	3	4
40	Do you protect the important records from destruction in accordance with statutory, regulatory, contractual and business requirements?	0	1	2	3	4
41	Do you protect the important records from falsification in accordance with statutory, regulatory, contractual and business requirements?	0	1	2	3	4
<b>Control 17: Data protection and privacy of personal information</b>						
42	Do you insure that data protection and privacy is in accordance with relevant legislation?	0	1	2	3	4
43	Do you insure that data protection and privacy is in accordance with regulations?	0	1	2	3	4
44	Do you insure that data protection and privacy is in accordance with contractual clauses?	0	1	2	3	4
<b>Control 18: Prevention of misuse of information processing facilities</b>						
45	Are the users deterred from unauthorised use of information processing facilities?	0	1	2	3	4
<b>Control 19: Regulation of cryptographic controls</b>						
46	Does the use of the cryptographic controls comply with all relevant agreement?	0	1	2	3	4
47	Does the use of the cryptographic controls comply with all relevant laws?	0	1	2	3	4
48	Does the use of the cryptographic controls comply with all relevant regulations?	0	1	2	3	4
<b>Objective 4: Compliance with security policies, standards and technical compliance</b>						
<b>Control 20: Compliance with security policies and standards</b>						
49	Do managers ensure that all security procedures are carried out correctly to achieve compliance with security policies?	0	1	2	3	4
50	Do managers ensure that all security procedures are carried out correctly to achieve compliance with security standards?	0	1	2	3	4
<b>Control 21: Technical compliance checking</b>						
51	Do you regularly check your information systems for compliance with security standards?	0	1	2	3	4
52	Are technical compliance checks carried out by authorised persons?	0	1	2	3	4
<b>Objective 5: Information systems audit considerations</b>						
<b>Control 22: Information systems audit controls</b>						
53	Do you carefully plan audit requirements and activities to minimise the risk of disruptions to business process?	0	1	2	3	4
54	Are the audit requirements agreed to minimise the risk of disruptions to business process?	0	1	2	3	4
<b>Control 23: Protection of information systems audit tools</b>						
55	Do you protect the access to audit tools to prevent misuse?	0	1	2	3	4
56	Do you protect the access to audit tools to prevent compromise?	0	1	2	3	4

**Other (Free) Comments / Suggestions:**

**For further comments, please add an extra page.**

**Give your views on the questionnaire: Missing Factors / Unnecessary Factors**

**For further views, please add an extra page.**

## **Appendix B**

### **SAMPLE CASE STUDY (E9)**

This organisation has been playing a crucial role in the consolidation and development of the country financial system. At the time of its establishment, there was no monetary system exclusively of the country. Foreign currencies circulated in the country as a medium of exchange, along with country coins. The country bank notes had not yet been issued. There were no banks in existence and the banking business was being conducted by foreign bank branches. One of the foremost tasks of this organisation in its early stage was, therefore, the development of the country currency. This organisation also paid special attention to the need for promoting the growth of a national banking system. From 1960 to 1972, this organisation focused on banking regulations against the background of expanding banking business and the country's acceptance of full convertibility of the currency in March 1961 in accordance with the Article VIII of the Articles of Agreements of the IMF. From 1973 to 1982, this organisation preoccupation was to contain inflationary pressures in the booming economy, expansion of the banking system and manage the massive foreign exchange reserves. From mid 1980s, the organisation priorities have been to introduce financial market reforms.

**Section (I): Technology Domain**  
**ISO/IEC 27002 clause: Communications and operations management**

ISO/IEC 27002 Objectives / Controls of Technology Domain		Results		Illustration of the Results
		c	w	
<b>Objective (1): operational procedures and responsibilities</b>	Documented operating procedures	3.7	.26	
	Change management	3.4	.25	
	Segregation of duties	3.5	.23	
	Separation of development, test and operational facilities	4	.26	
	<i>Indicator of achievement of Technical objective(1)</i> $=3.7*.26+3.4*.25+3.5*.23+4*.26=3.66$			
<b>Objective (2): Third party service delivery management</b>	Service delivery	3.4	.35	
	Monitoring and review of third party services	4	.34	
	Managing changes to third party services	4	.31	
	<i>Indicator of achievement of Technical objective(2)</i> $=3.4*.35+4*.34+4*.31=3.79$			
<b>Objective (3): System planning and acceptance</b>	Capacity management	3.7	.45	
	System acceptance	4	.55	
	<i>Indicator of achievement of Technical objective(3)</i> $=3.7*.45+4*.55=3.87$			
<b>Objective (4): Protection against malicious and mobile code</b>	Control against malicious code	3	.6	
	Control against mobile code	1	.4	
	<i>Indicator of achievement of Technical objective(4)</i> $=3*.6+1*.4=2.2$			
<b>Objective (5): Back-up</b>	Information back-up	3.55	1	
	<i>Indicator of achievement of Technical objective(5)</i> $=3.55*1.0=3.55$			
<b>Objective (6): Network security management</b>	Network controls	4	.55	
	Security of network services	3.8	.45	
	<i>Indicator of achievement of Technical objective(6)</i> $=4*.55+3.8*.45=3.91$			

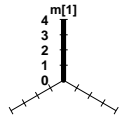
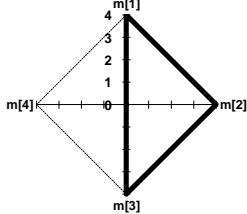
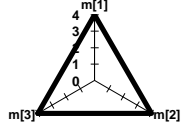
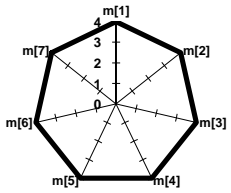
Continue: **Communications and operations management**

ISO/IEC 27002 Objectives / Controls of Technology Domain		Results		Illustration of the Results
		c	w	
<b>Objective (7): Media handling</b>	Management of removable media	4	.25	
	Disposable media	3.5	.24	
	Information handling procedures	3.6	.26	
	Security of system documentation	4	.25	
	<i>Indicator of achievement of Technical objective(7)</i> $=4*.25+3.5*.24+3.6*.26+4*.25=3.78$			
<b>Objective (8): Exchange of information</b>	Information exchange policies and procedures	3.4	.2	
	Exchange agreements	3.5	.19	
	Physical media in transit	4	.2	
	Electronic messaging	4	.22	
	Business information systems	3.5	.19	
	<i>Indicator of achievement of Technical objective(8)</i> $=3.4*.2+3.5*.19+4*.2+4*.22+3.5*.19=3.69$			
<b>Objective (9): Electronic commerce services</b>	Electronic commerce	4	.31	
	On-Line transactions	4	.35	
	Publicly available information	3	.34	
	<i>Indicator of achievement of Technical objective(9)</i> $=4*.31+4*.35+3*.34=3.66$			
<b>Objective (10): Monitoring</b>	Audit logging	4	.16	
	Monitoring of system use	3.5	.16	
	Protection of log information	3.5	.17	
	Administrator and operator logs	3.6	.18	
	Fault logging	3.6	.18	
	Clock synchronisation	4	.15	
	<i>Indicator of achievement of Technical objective(10)</i> $=4*.16+3.5*.16+3.5*.17+3.6*.18*2+4*.15=3.69$			

**Figure B-1a** Sample Case study results concerned with the achievement of the ISO/IEC 27002 technical security objectives of the “communications and operations management” clause



**Section (I): Technology Domain**  
**ISO/IEC 27002 clause: Access control**

ISO/IEC 27002 Objectives / Controls of Technology Domain		Results		Illustration of the Results
		c	w	
<b>Objective (11):</b> Business requirements for access control	Access control policy	3.7	1.0	
	<i>Indicator of achievement of Technical objective(11)</i> $=3.7*1.0=3.7$			
<b>Objective (12):</b> User access management	User registration	3.5	.27	
	Privileges management	3.4	.26	
	User password management	3	.24	
	Review of user access rights	0	.23	
	<i>Indicator of achievement of Technical objective(12)</i> $=3.5*.27+3.4*.26+3*.24+0*.23=2.55$			
<b>Objective (13):</b> User responsibilities	Password use	3.5	.34	
	Unattended user equipment	4	.34	
	Clear desk & Clear screen policy	3.5	.32	
	<i>Indicator of achievement of Technical objective(13)</i> $=3.5*.34+4*.34+3.5*.32=3.67$			
<b>Objective (14):</b> Network access control	Policy on use of network services	4	.15	
	User authentication for external connections	3	.16	
	Equipment identification in networks	4	.14	
	Remote diagnostic and configuration port protection	3.6	.15	
	Segregation in networks	4	.14	
	Network connection control	4	.14	
	Network routing control	4	.12	
	<i>Indicator of achievement of Technical objective(14)</i> $=4*.15+3*.16+4*.14+3.6*.15+4*.14*2+4*.12=3.78$			

Continue: Access control

PROTECTION CONTROLS OF Technical SECURITY		Results		Illustration of the Results
		c	w	
<b>Objective (15): Operating system access control</b>	Secure log-on procedures	3	.18	
	User identification and authentication	3.3	.16	
	Password management system	4	.19	
	User of system utilities	3.6	.17	
	Session time-out	4	.15	
	Limitation of connection time	4	.15	
	<b>Indicator of achievement of Technical objective(15)</b> $=3*.18+3.3*.16+4*.19+3.6*.17+4*.15*2=3.64$			
<b>Objective (16): Application and information access control</b>	Information access restriction	3.5	.52	
	Sensitive system isolation	4	.48	
	<b>Indicator of achievement of Technical objective(16)</b> $=3.5*.52+4*.48=3.74$			
<b>Objective (17): Mobile computing and teleworking</b>	Mobile computing and teleworking	0	.55	
	Teleworking policy for use	0	.45	
	<b>Indicator of achievement of Technical objective(17)</b> $=0*.55+0*.45=0$			

Figure B-1b Sample Case study results concerned with the achievement of the ISO/IEC 27002 technical objectives of the “access control” clause

**Section (I): Technology Domain**  
**ISO/IEC 27002 clause: Information systems acquisition, development and maintenance**

ISO/IEC 27002 Objectives / Controls of Technology Domain		Results		Illustration of the Results
		c	w	
<b>Objective (18):</b> Security requirements of Information systems	Security requirements analysis and specification	4	1	
	<i>Indicator of achievement of Technical objective(18) = 4*1.0=4</i>			
<b>Objective (19):</b> Correct processing in applications	Input data validation	4	.3	
	Control of internal processing	3	.2	
	Message integrity	3.5	.3	
	Output data validation	4	.2	
	<i>Indicator of achievement of Technical objective(19) = 4*.3+3*.2+3.5*.3+4*.2=3.65</i>			
<b>Objective (20):</b> Cryptographic controls	Policy on the use of cryptographic controls	3.6	.5	
	Key management	3.5	.5	
	<i>Indicator of achievement of Technical objective(20) = 3.6*.5+3.5*.5=3.55</i>			
<b>Objective (21):</b> Security of system files	Control of operational software	4	.33	
	Protection of system test data	0	.32	
	Access control to program source code	4	.35	
	<i>Indicator of achievement of Technical objective(21) = 4*.33+0*.32+4*.35=2.72</i>			
<b>Objective (22):</b> Security in development and support processes	Change control procedures	3	.2	
	Technical review of applications after operating system changes	4	.2	
	Restriction on changes to software packages	3.8	.17	
	Information leakage	4	.23	
	Outsourced software development	3.5	.2	
	<i>Indicator of achievement of Technical objective(22) = 3*.2+4*.2+3.8*.17+4*.23+3.5*.2=3.67</i>			
<b>Objective (23):</b> Technical vulnerability management	Control of technical vulnerabilities	3.8	1	
	<i>Indicator of achievement of Technical objective(23) = 4*1=3.8</i>			

**Figure B-1c Sample Case study results concerned with the achievement of the ISO/IEC 27002 technical objectives of the “information systems acquisition, development and maintenance” clause**

ISO/IEC 27002 Clauses / Objectives of Technology Domain		Results		Illustration of the Results
		<i>b</i>	<i>w</i>	
<b>ISO Communications and Operations Management</b>	Operational procedures and responsibilities	3.66	.08	
	Third party service delivery management	3.79	.07	
	System planning and acceptance	3.87	.09	
	Protection against malicious and mobile code	2.20	.08	
	Back-up	3.55	.14	
	Network security management	3.91	.13	
	Media handling	3.78	.1	
	Exchange of information	3.69	.1	
	Electronic commerce services	3.66	.09	
	Monitoring	3.69	.12	
	<b>Indicator of achievement of Technical ISO Part(1)</b> $=3.66*.08+3.79*.07+3.87*.09+2.2*.08+3.55*.14+3.91*.13+3.78*.1+3.69*.1+3.66*.09+3.69*.12=3.68$			
<b>ISO Access Control</b>	Business requirements for access control	3.7	.13	
	User access management	2.55	.15	
	User responsibilities	3.67	.14	
	Network access control	3.78	.15	
	Operating system access control	3.64	.14	
	Application and information access control	3.74	.15	
	Mobile computing and tele-working	0	.14	
<b>Indicator of achievement of Technical ISO Part(2)</b> $=4*.14*5+3.4*.14+0*.14=3.28$				
<b>ISO Information Systems Acquisitions, Development and Maintenance</b>	Security requirements of information systems	4	.18	
	Correct processing in applications	3.65	.16	
	Cryptographic controls	3.55	.19	
	Security of system files	2.72	.17	
	Security in development and support processes	3.67	.15	
	Technical vulnerability management	3.8	.15	
<b>Indicator of achievement of Technical ISO Part(3)</b> $=4*.17*5+2.4*.17=3.81$				

Figure B-1d Sample Case study results concerned with the achievement of the ISO/IEC 27002 technology clauses, considering the results of Figures B-1a, B-1b and B-1c

ISO/IEC 27002 Clauses of Technology Domain		Results		Illustration of the Results
		<i>p</i>	<i>w</i>	
<b>ISO Technical Security</b>	<b>Communications and Operations Management</b>	<b>3.68</b>	<b>0.33</b>	
	<b>Access Control</b>	<b>3.28</b>	<b>0.33</b>	
	<b>Information Systems Acquisition, Development and Maintenance</b>	<b>3.81</b>	<b>0.33</b>	
	<b>Indicator of compliance with ISO Technical security (Technology)</b> $=3.68*.33+3.28*.33+3.81*.33=3.55$			

Figure B-1e Sample Case study results concerned with conformance with the technology domain considering the results of Figure B-1d

**Section (II): Organisation domain**  
**ISO/IEC 27002 clause: Security policy**

ISO/IEC 27002 Objectives / Controls of Organisation Domain		Results		Illustration of the Results
		c	w	
Objective(1): Information Security Policy	Information security policy document	4	.6	
	Review of the information security policy	3.6	.4	
	<i>Indicator of use of Organisation security objective(1) = 4*.6+3.6*.4=3.84</i>			

Figure B-2a Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objective of the “security policy” clause

**Section (II): Organisation Domain**  
**ISO/IEC 27002 clause: Organisation of Information Security**

ISO/IEC 27002 Objectives / Controls of Organisation Domain		Results		Illustration of the Results
		c	w	
Objective (2): Internal organisation	Management commitment to information security	3.8	.14	
	Information security co-ordination	3.5	.12	
	Allocation of information security responsibilities	3.6	.14	
	Authorisation process for information processing facilities	3.5	.1	
	Confidentiality agreements	2	.1	
	Contact with authorities	4	.13	
	Contact with special interest groups	3.7	.15	
	Independent review of information security	3.5	.12	
<i>Indicator of use of Organisation security objective(2) = 3.8*.14+3.5*.12+3.6*.14+3.5*.1+2*.1+4*.13+3.7*.15+3.5*.12=3.49</i>				
Objective (3): External parties	Identification or risks related to external parties	3.6	.35	
	Addressing security when dealing with customers	3.6	.35	
	Addressing security in third party agreements	3.8	.3	
	<i>Indicator of use of Organisation security objective(3) = 3.6*.35*2+3.8*.3=3.66</i>			

Figure B-2b Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “organisation of Information Security” clause

**Section (II): Organisation Domain**  
**ISO/IEC 27002 clause: Assets Management**

ISO/IEC 27002 Objectives / Controls of Organisation Domain		Results		Illustration of the Results
		c	w	
Objective (4): Responsibility for assets	Inventory of assets	4	.35	
	Ownership of assets	4	.35	
	Acceptable use of assets	4	.3	
	<i>Indicator of use of Organisation security</i> $objective(4) = 4 * .35 * 2 + 4 * .3 = 4$			
Objective (5): Information classification	Classification guidelines	4	.55	
	Information labelling and handling	4	.45	
	<i>Indicator of use of Organisation security</i> $objective(5) = 4 * .55 + 4 * .45 = 4$			

**Figure B-2c** Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “assets management” clause

**Section (II): Organisation Domain**  
**ISO/IEC 27002 clause: Information Security incident management**

ISO/IEC 27002 Objectives / Controls of Organisation Domain		Results		Illustration of the Results
		c	w	
Objective (6): Reporting information security events and weaknesses	Reporting information security events	3.7	.6	
	Reporting security weakness	0	.4	
	<i>Indicator of use of Organisation security objective(6) = 3.7*.6+0*.4= 2.22</i>			
Objective (7): Management of information security incidents and improvements	Responsibilities and procedures	3.4	.38	
	Learning from information security incidents	3.8	.35	
	Collection of evidence	0	.27	
	<i>Indicator of use of Organisation security objective(7) = 3.4*.38+3.8*.35+0*.27=2.62</i>			

Figure B-2d Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “information security incident management” clause

**Section (II): Organisation Domain**  
**ISO/IEC 27002 clause: Business Continuity Management**

ISO/IEC 27002 Objectives / Controls of Organisation Domain		Results		Illustration of the Results
		c	w	
Objective (8): Information security aspects of business continuity management	Including information security in the business continuity management process	4	.22	
	Business continuity and risk assessment	4	.25	
	Developing and implementing continuity plans including information security	4	.17	
	Business continuity planning framework	4	.16	
	Testing, maintaining and re-assessing business continuity plans	4	.2	
	<i>Indicator of use of Organisation security objective(8) = 4*.22+4*.25+4*.17+4*.16+4*.2= 4</i>			

Figure B-2e Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation objectives of the “business continuity management” clause

ISO/IEC 27002 Clauses / Objectives of Organisation Domain		Results		Illustration of the Results
		<i>b</i>	<i>w</i>	
ISO Information Security Policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	3.84	1.0	
	<i>Indicator of compliance with ISO security policy (Organisation) = 3.8*1.0 = 3.8</i>			
ISO Organisation of Information Security	Internal organisation	3.49	.65	
	External parties	3.66	.35	
<i>Indicator of achievement of Organisation ISO Clause(1) = 3.4*.5 + 4*.5 = 3.7</i>				
ISO Assets Management	Responsibility of assets	4	.6	
	Information classification	4	.4	
<i>Indicator of achievement of Organisation ISO Clause(2) = 4*.4 + 4*.6 = 4</i>				
ISO Information Security incident management	Information security events and weaknesses	2.22	.7	
	Management of information security incidents and improvements	2.62	.3	
<i>Indicator of achievement of Organisation ISO Clause(3) = 2*.5 + 2.64*.5 = 2.32</i>				
ISO Business continuity management	Information security aspects of business continuity management	4	1	
	<i>Indicator of achievement of Organisation ISO Clause(4) = 4*1 = 4</i>			

Figure B-2f Sample Case study results concerned with the achievement of the ISO/IEC 27002 organisation clauses, considering the results of Figures B-2a, B-2b, B-2c, B-2d and B-2e

ISO/IEC 27002 Clauses of Organisation Domain		Results		Illustration of the Results
		<i>p</i>	<i>w</i>	
ISO Organisation security	Information Security Policy	3.8	0.1	
	Organization of Information Security	3.7	0.2	
	Assets Management	4	0.2	
	Information Security incident management	2.32	0.25	
	Business Continuity Management	4	0.25	
	<i>Indicator of conformance with Organisation domain = 3.8*.1 + 3.7*.2 + 4*.2 + 2.32*.25 + 4*.25 = 3.5</i>			

Figure B-2g Sample Case study results concerned with the achievement of organisation domain, considering the results of Figure B-2f



**Section (III): People Domain**  
**ISO/IEC 27002 clause: Human resources security**

ISO/IEC 27002 Objectives / Controls of People Domain		Results		Illustration of the Results
		c	w	
Objective (1): Prior to employment	Roles and responsibilities	3.7	.36	
	Screening	3.4	.31	
	Terms and conditions of employment	3	.33	
	<i>Indicator of use of Human resources security objective(1) = 3.7*.36+3.4*.31+3*.33 = 3.38</i>			
Objective (2): During employment	Management responsibilities	3.8	.36	
	Information security awareness, education and training	3.9	.32	
	Disciplinary process	3.5	.32	
	<i>Indicator of use of Human resources security objective(2) = 3.8*.36+3.9*.32+3.5*.32=3.72</i>			
Objective (3): Termination or change of employment	Termination responsibilities	3.6	.34	
	Return of assets	3.5	.33	
	Removal of access rights	4	.33	
	<i>Indicator of use of Human resources security objective (3) = 3.6*.34+3.5*.33+4*.33=3.7</i>			

Figure B-3a Sample Case study results concerned with the achievement of the ISO/IEC 27002 people security objectives of the “human resources security” clause

ISO/IEC 27002 Clauses / Objectives of People Domain		Results		Illustration of the Results
		b	w	
ISO Human Resources Security	Prior to employment	3.38	.33	
	During employment	3.72	.32	
	Termination or change of employment	3.70	.35	
	<i>Indicator of achievement of Human resources security objectives = 3.3*.3+4*.35*2=3.79</i>			

Figure B-3b Sample Case study results concerned with the achievement of ISO/IEC 27002 human resources clause, considering the results of Figure B-3a

ISO/IEC 27002 Clauses of People Domain		Results		Illustration of the Results
		p	w	
ISO Human Resources Security	Human Resources Security	3.79	1.	
	<i>Indicator of compliance with ISO Human resources security (people) = 3.79*1.0 = 3.79</i>			

Figure B-3c Sample Case study results concerned with the achievement of people domain, considering the results of Figure B-3b

**Section (IV): Environment Domain**  
**ISO/IEC 27002 clause: Physical and environmental security**

ISO/IEC 27002 Objectives / Controls of Environment Domain		Results		Illustration of the Results
		<i>c</i>	<i>w</i>	
<b>Objective (1): Secure areas</b>	Physical security perimeter	3.5	.19	
	Physical entry controls	3.8	.17	
	Securing offices, rooms and facilities	0	.16	
	Protection against external and environmental threats	3.7	.17	
	Working in secure areas	3.6	.16	
	Public access, delivery and loading areas	3.9	.15	
	<i>Indicator of use of Environmental security objective(1)</i> $=3.5*.19+3.8*.17+0*.16+3.7*.17+3.6*.16+3.9*.15=3.09$			
<b>Objective (2): Equipment security</b>	Equipment sitting and protection	3.5	.14	
	Supporting utilities	3.6	.15	
	Cabling security	4	.15	
	Equipment maintenance	3.5	.14	
	Security of equipment off-premises	4	.15	
	Secure disposal or re-use of equipment	2	.14	
	Removal of property	3.8	.13	
	<i>Indicator of use of Environmental security objective (2)</i> $=3.5*.14+3.6*.15+4*.15+3.5*.14+4*.15+2*.14+3.8*.13=3.48$			

**Figure B-4a Sample Case study results concerned with the achievement of the ISO/IEC 27002 environmental security objectives of the “physical and environmental security” clause**

**Section (IV): Environment Domain**  
**ISO/IEC 27002 clause: Compliance**

ISO/IEC 27002 Objectives / Controls of Environment Domain		Results		Illustration of the Results
		c	w	
<b>Objective (3): Compliance with legal requirements</b>	Identification of applicable legislation	3.8	.17	
	Intellectual property rights	3.8	.17	
	Protection of organisational records	0	.16	
	Data protection and privacy of personal information	3.6	.16	
	Prevention of misuse of information processing facilities	4	.17	
	Regulation of cryptographic controls	4	.17	
	<i>Indicator of use of Environmental security objective(3) = 3.8*.17*2+0*.16+3.6*.16+4*.17*2= 3.19</i>			
<b>Objective (4): Compliance with security policies, standards and technical compliance</b>	Compliance with security policies and standards	0	.6	
	Technical compliance checking	3.5	.4	
	<i>Indicator of use of Environmental security objective (4)=0*.6+3.5*.4=1.75</i>			
<b>Objective (5): information systems audit considerations</b>	Information systems audit controls	3.4	.6	
	Protection of information systems audit tools	4	.4	
	<i>Indicator of use of Environmental security objective (5) = 3.4*.6+4*.4= 3.64</i>			

**Figure B-4b Sample Case study results concerned with the achievement of the ISO/IEC 27002 environmental security objectives of the “compliance” clause**

ISO/IEC 27002 Clauses / Objectives of Environment Domain		Results		Illustration of the Results
		<i>b</i>	<i>w</i>	
ISO Physical and Environmental security	Secure areas	3.09	.47	
	Equipment security	3.48	.53	
	<i>Indicator of achievement of Environmental ISO Part(1)=3.24*.6+3.8*.4=3.46</i>			
ISO Compliance	Compliance with legal requirements	3.19	.33	
	Compliance with security policies and standards	1.75	.35	
	Information system audit consideration	3.64	.32	
	<i>Indicator of achievement of Environmental ISO Part(2)=2.4*.33+1.6*.33+4*.33=2.64</i>			

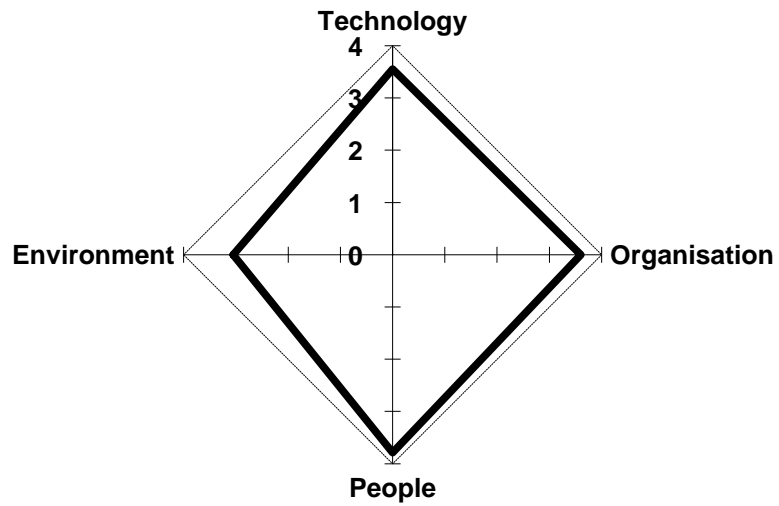
Figure B-4c Sample Case study results concerned with the achievement of the ISO/IEC 27002 environmental security clauses considering the results of Figures B-4a, and B-4b

ISO/IEC 27002 Clauses of Environment Domain		Results		Illustration of the Results
		<i>p</i>	<i>w</i>	
ISO Environmental security	Physical and environmental security	3.46	0.5	
	Compliance	2.64	0.5	
	<i>Indicator of compliance with ISO Environmental security (environment) = 3.46*.5+2.64*.5=3.05</i>			

Figure B-4d Sample Case study results concerned with the achievement of the ISO/IEC 27002 environment domain considering the results of Figure B-4c

Domain	Results			Indicator
	<i>d</i>	<i>w</i>	<i>(d*w)</i>	
Technology	3.55	0.2	.71	Overall TOPE s-readiness indicator: R = 3.55/4
Organisation	3.6	0.2	.70	
People	3.79	0.2	.76	
Environment	3.05	0.2	.61	

**Illustration of the Results**



**Figure B-5 Sample case study results concerned with conformance with TOPE domains**

# **Appendix C**

## **DETAILED ASSESSMENT RESULTS**

**Table C-1 All case studies assessment results concerned with the achievement of the ISO/IEC 27002 security controls**

ISO/IEC 27002 Control		W	Assessment Scores – Controls Level								
			E1	E2	E3	E4	E5	E6	E7	E8	E9
1	Documented operating procedures	.26	4.0	3.7	3.7	1.7	2.7	4.0	3.7	3.7	3.7
2	Change management	.25	4.0	3.2	3.6	2.0	2.6	3.4	3.6	3.6	3.4
3	Segregation of duties	.23	4.0	2.5	2.5	0.0	3.5	4.0	3.5	3.5	3.5
4	Separation of development, test, and operational facilities	.26	3.0	3.0	4.0	0.0	3.0	3.0	4.0	0.0	4.0
5	Service delivery	.35	4.0	2.1	3.7	2.1	3.1	3.7	3.7	3.7	3.4
6	Monitoring and review of third party services	.34	4.0	2.8	4.0	2.3	3.3	4.0	3.5	3.8	4.0
7	Managing changes to third party services	.31	4.0	2.4	4.0	2.4	2.6	4.0	4.0	3.6	4.0
8	Capacity management	.45	4.0	3.0	3.0	3.0	1.4	3.0	0.0	3.7	3.7
9	System acceptance	.55	4.0	2.5	3.0	2.5	2.5	4.0	3.5	3.5	4.0
10	Controls against malicious code	.60	3.0	2.0	3.5	2.5	2.9	3.8	2.0	3.8	3.0
11	Controls against mobile code	.40	0.0	1.0	3.0	2.0	2.2	3.0	2.6	0.0	1.0
12	Information back-up	1.0	4.0	2.2	3.5	2.0	2.8	3.8	3.8	3.8	3.6
13	Network controls	.55	4.0	2.0	4.0	2.0	2.5	4.0	4.0	3.5	4.0
14	Security of network services	.45	0.0	2.8	3.8	0.0	3.4	3.8	3.4	3.8	3.8
15	Management of removable media	.25	0.0	3.0	4.0	2.0	0.0	4.0	4.0	0.0	4.0
16	Disposal of media	.24	0.0	2.0	3.5	2.5	0.0	3.5	3.5	0.0	3.5
17	Information handling procedures	.26	0.0	2.6	3.6	2.4	2.6	4.0	4.0	3.4	3.6
18	Security of system documentation	.25	4.0	2.0	4.0	3.0	3.0	4.0	3.0	4.0	4.0
19	Information exchange policies and procedures	.20	4.0	2.2	3.8	0.0	2.8	3.8	0.0	3.8	3.4
20	Exchange agreements	.19	0.0	2.5	3.5	0.0	0.0	3.5	3.5	3.5	3.5
21	Physical media in transit	.20	0.0	2.0	3.0	0.0	0.0	0.0	3.0	4.0	4.0
22	Electronic messaging	.22	4.0	3.0	4.0	2.0	3.0	4.0	4.0	4.0	4.0
23	Business information systems	.19	0.0	2.0	3.0	0.0	0.0	3.5	3.5	3.5	3.5
24	Electronic commerce	.31	0.0	2.0	4.0	0.0	0.0	4.0	0.0	4.0	4.0
25	On-Line transactions	.35	0.0	1.0	4.0	0.0	3.0	4.0	0.0	0.0	4.0
26	Publicly available information	.34	0.0	0.0	4.0	0.0	3.0	3.0	0.0	3.0	3.0
27	Audit logging	.16	4.0	2.2	4.0	0.0	0.0	3.6	4.0	3.6	4.0
28	Monitoring system use	.16	0.0	2.0	3.5	0.0	0.0	4.0	4.0	3.5	3.5
29	Protection of log information	.17	4.0	2.5	3.5	0.0	2.5	4.0	3.5	3.5	3.5
30	Administrator and operator logs	.18	4.0	2.2	4.0	2.6	3.4	4.0	4.0	3.6	3.6
31	Fault logging	.18	4.0	1.6	3.4	2.6	2.1	3.7	3.7	3.7	3.6
32	Clock synchronization	.15	4.0	2.0	4.0	3.0	0.0	4.0	4.0	3.0	4.0
33	Access control policy	1.0	0.0	4.0	3.7	2.4	0.0	4.0	0.0	3.7	3.7
34	User registration	.27	0.0	4.0	3.5	2.5	2.5	4.0	3.5	3.5	3.5
35	Privilege management	.26	4.0	4.0	3.6	2.4	2.2	4.0	3.6	3.2	3.4
36	User password management	.24	4.0	4.0	3.0	3.0	3.0	4.0	4.0	3.0	3.0
37	Review of user access rights	.23	4.0	4.0	3.0	0.0	3.0	4.0	3.0	2.0	0.0
38	Password use	.34	4.0	4.0	3.5	0.0	2.5	4.0	3.5	3.0	3.5
39	Unattended user equipment	.34	4.0	4.0	4.0	2.0	2.0	4.0	4.0	3.0	4.0
40	Clear desk and clear screen policy	.32	4.0	4.0	3.5	2.5	2.5	4.0	3.5	2.5	3.5
41	Policy on use of network services	.15	4.0	4.0	4.0	2.0	2.0	4.0	3.0	3.0	4.0
42	User authentication for external connections	.16	4.0	4.0	3.0	0.0	3.0	4.0	4.0	3.0	3.0
43	Equipment identification in networks	.14	0.0	4.0	3.0	0.0	0.0	4.0	4.0	0.0	4.0
44	Remote diagnostic and configuration port protection	.15	0.0	4.0	3.4	2.6	2.6	4.0	3.6	3.6	3.6

45	Segregation in networks	.14	4.0	4.0	4.0	2.0	3.0	4.0	4.0	3.0	4.0
46	Network connection control	.14	4.0	4.0	3.0	1.5	3.0	4.0	3.5	3.5	4.0
47	Network routing control	.12	4.0	4.0	3.0	2.0	3.0	4.0	3.0	4.0	4.0
48	Secure log-on procedures	.18	4.0	4.0	4.0	1.4	2.6	4.0	3.4	3.2	3.0
49	User identification and authentication	.16	0.0	4.0	4.0	0.0	1.7	4.0	3.7	3.0	3.3
50	Password management system	.19	0.0	4.0	3.5	0.0	1.5	4.0	4.0	3.5	4.0
51	Use of system utilities	.17	4.0	4.0	4.0	1.6	0.0	4.0	3.4	3.2	3.6
52	Session time-out	.15	4.0	4.0	4.0	0.0	3.0	4.0	3.0	3.0	4.0
53	limitation of connection time	.15	0.0	4.0	4.0	0.0	3.0	4.0	3.0	3.0	4.0
54	Information access restriction	.52	4.0	4.0	4.0	2.5	1.5	4.0	3.5	3.5	3.5
55	Sensitive system isolation	.48	0.0	4.0	4.0	3.0	3.0	4.0	3.0	3.0	4.0
56	Mobile computing and communications	.55	0.0	4.0	3.4	0.0	3.6	4.0	0.0	3.0	0.0
57	Teleworking policy for use	.45	0.0	4.0	3.6	0.0	0.0	4.0	0.0	3.8	0.0
58	Security requirements analysis and specification	1.0	4.0	1.6	4.0	1.6	2.5	4.0	3.6	3.5	4.0
59	Input data validation	.30	0.0	2.0	4.0	2.0	3.0	4.0	4.0	3.0	4.0
60	Control of internal processing	.20	0.0	1.0	4.0	2.0	2.0	4.0	4.0	3.0	3.0
61	Message integrity	.30	0.0	2.5	4.0	1.5	2.5	4.0	3.5	3.5	3.5
62	Output data validation	.20	0.0	0.0	4.0	0.0	2.0	4.0	4.0	3.0	4.0
63	Policy on the use of cryptographic controls	.50	0.0	2.6	4.0	0.0	2.2	4.0	0.0	3.6	3.6
64	Key management	.50	0.0	2.0	4.0	0.0	0.0	4.0	0.0	2.5	3.5
65	Control of operational software	.33	4.0	3.0	4.0	2.0	3.0	4.0	4.0	3.0	4.0
66	Protection of system test data	.32	4.0	0.0	4.0	1.6	2.6	4.0	3.4	3.6	0.0
67	Access control to program source code	.35	4.0	2.0	4.0	0.0	3.0	4.0	4.0	3.0	4.0
68	Change control procedures	.20	3.0	2.0	4.0	2.0	2.0	4.0	4.0	3.0	3.0
69	Review of applications after operating system changes	.20	3.0	2.5	4.0	1.5	3.5	4.0	3.5	3.5	4.0
70	Restrictions on changes to software packages	.17	3.0	1.6	4.0	2.2	2.4	4.0	3.6	3.2	3.8
71	Information leakage	.23	3.0	2.0	4.0	2.0	2.0	4.0	3.0	3.0	4.0
72	Outsourced software development	.20	3.0	2.5	4.0	1.5	2.5	4.0	3.5	3.5	3.5
73	Control of technical vulnerabilities	1.0	0.0	1.8	4.0	2.4	2.2	4.0	3.8	3.2	3.8
74	Information security policy document	.60	0.0	3.0	3.3	0.0	2.8	3.5	1.0	3.3	4.0
75	Review of the information security policy	.40	0.0	2.4	4.0	1.6	0.0	3.0	1.0	3.4	3.6
76	Management commitment to information security	.14	4.0	4.0	4.0	4.0	2.3	3.8	4.0	3.3	3.8
77	Information security co-ordination	.12	0.0	4.0	4.0	4.0	1.5	3.5	4.0	2.5	3.5
78	Allocation of information security responsibilities	.14	0.0	4.0	4.0	4.0	0.0	4.0	4.0	2.6	3.6
79	Authorisation process for information processing facilities	.10	0.0	4.0	4.0	4.0	2.0	4.0	4.0	3.0	3.5
80	Confidentiality agreements	.10	0.0	4.0	4.0	4.0	2.4	3.6	4.0	2.0	2.0
81	Contact with authorities	.13	0.0	4.0	4.0	4.0	2.5	3.5	4.0	3.5	4.0
82	Contact with special interest groups	.15	0.0	4.0	4.0	4.0	2.6	3.9	4.0	2.0	3.7
83	Independent review of information security	.12	0.0	4.0	4.0	4.0	0.0	3.5	4.0	2.0	3.5
84	Identification of risks related to external parties	.35	4.0	4.0	4.0	4.0	2.6	4.0	4.0	2.0	3.6
85	Addressing security when dealing with customers	.35	4.0	4.0	4.0	4.0	2.4	3.6	4.0	2.4	3.6
86	Addressing security in third party agreements	.30	4.0	4.0	4.0	4.0	2.3	2.0	4.0	2.0	3.8
87	Inventory of assets	.35	0.0	4.0	4.0	2.2	4.0	4.0	3.4	3.4	4.0
88	Ownership of assets	.35	0.0	4.0	4.0	1.5	4.0	4.0	3.5	3.5	4.0
89	Acceptable use of assets	.30	0.0	4.0	4.0	2.4	4.0	4.0	3.4	3.4	4.0
90	Classification guidelines	.55	0.0	4.0	4.0	1.4	4.0	4.0	0.0	2.0	4.0
91	Information labelling and handling	.45	0.0	4.0	4.0	0.0	4.0	4.0	0.0	3.5	4.0
92	Reporting information security events	.60	0.0	2.9	4.0	0.0	2.6	4.0	3.7	4.0	3.7
93	Reporting security weakness	.40	0.0	2.6	4.0	0.0	0.0	4.0	3.0	4.0	0.0
94	Responsibilities and procedures	.38	4.0	2.6	4.0	0.0	2.4	4.0	3.8	0.0	3.4



95	Learning from information security incidents	.35	4.0	0.0	4.0	0.0	0.0	4.0	3.8	0.0	3.8
96	Collection of evidence	.27	0.0	3.0	4.0	0.0	0.0	4.0	0.0	0.0	0.0
97	Including IS in the business continuity management process	.22	0.0	4.0	4.0	0.0	2.4	4.0	0.0	0.0	4.0
98	Business continuity and risk assessment	.25	0.0	4.0	4.0	0.0	1.5	4.0	0.0	0.0	4.0
99	Developing and implementing continuity plans including IS	.17	0.0	4.0	4.0	3.5	1.5	4.0	0.0	0.0	4.0
100	Business continuity planning framework	.16	0.0	4.0	4.0	0.0	2.0	4.0	0.0	3.1	4.0
101	Testing, maintaining and assessing business continuity plan	.20	0.0	4.0	4.0	0.0	2.6	4.0	0.0	0.0	4.0
102	Roles and responsibilities	.36	0.0	4.0	4.0	0.0	2.0	4.0	4.0	4.0	3.7
103	Screening	.31	0.0	4.0	4.0	2.4	0.0	4.0	4.0	4.0	3.4
104	Terms and conditions of employment	.33	0.0	4.0	4.0	0.0	0.0	4.0	4.0	4.0	3.0
105	Management responsibilities	.36	3.3	4.0	4.0	1.8	2.8	4.0	4.0	4.0	3.8
106	Information security awareness, education, and training	.32	2.6	4.0	4.0	2.2	0.0	4.0	4.0	4.0	3.9
107	Disciplinary process	.32	0.0	4.0	4.0	2.5	0.0	4.0	4.0	4.0	3.5
108	Termination responsibilities	.34	3.0	4.0	4.0	0.0	2.4	4.0	4.0	4.0	3.6
109	Return of assets	.33	3.0	4.0	4.0	2.0	2.3	4.0	4.0	4.0	3.5
110	Removal of access rights	.33	4.0	4.0	4.0	1.6	2.2	4.0	4.0	4.0	4.0
111	Physical security perimeter	.19	0.0	2.3	4.0	2.0	3.3	3.8	4.0	4.0	3.5
112	Physical entry controls	.17	0.0	2.8	4.0	1.8	3.4	3.8	4.0	4.0	3.8
113	Securing offices, rooms, and facilities	.16	2.0	3.2	4.0	2.4	0.0	3.6	4.0	4.0	0.0
114	Protection against external and environmental threats	.17	4.0	3.3	4.0	2.7	0.0	3.7	4.0	4.0	3.7
115	Working in secure areas	.16	0.0	3.1	4.0	1.9	0.0	3.9	4.0	4.0	3.6
116	Public access, delivery, and loading areas	.15	0.0	2.4	4.0	2.4	0.0	4.0	4.0	4.0	3.9
117	Equipment sitting and protection	.14	4.0	2.5	4.0	1.5	3.5	3.5	4.0	4.0	3.5
118	Supporting utilities	.15	4.0	2.1	4.0	1.5	3.6	3.5	4.0	4.0	3.6
119	Cabling security	.15	4.0	1.4	4.0	2.0	2.6	3.4	4.0	4.0	4.0
120	Equipment maintenance	.14	4.0	3.5	4.0	1.5	2.5	4.0	4.0	4.0	3.5
121	Security of equipment off-premises	.15	4.0	2.0	4.0	0.0	1.6	4.0	4.0	4.0	4.0
122	Secure disposal or re-use of equipment	.14	4.0	3.8	4.0	1.8	2.4	3.8	4.0	4.0	2.0
123	Removal of property	.13	2.0	2.5	4.0	1.8	2.3	3.8	4.0	4.0	3.8
124	Identification of applicable legislation	.17	4.0	3.4	4.0	1.8	2.0	3.6	0.0	3.8	3.8
125	Intellectual property rights (IPR)	.17	0.0	2.8	4.0	0.0	2.5	3.8	0.0	3.5	3.8
126	Protection of organizational records	.16	0.0	2.3	4.0	0.0	2.9	3.3	0.0	3.1	0.0
127	Data protection and privacy of personal information	.16	0.0	3.6	4.0	0.0	0.0	3.9	0.0	3.9	3.6
128	Prevention of misuse of information processing facilities	.17	2.0	3.0	4.0	2.0	3.0	4.0	0.0	3.0	4.0
129	Regulation of cryptographic controls	.17	2.0	3.2	4.0	1.8	2.8	3.8	0.0	0.0	3.8
130	Compliance with security policies and standards	.50	2.0	0.0	4.0	2.0	0.0	3.5	3.0	3.5	0.0
131	Technical compliance checking	.50	4.0	3.0	3.0	2.0	2.5	3.5	3.5	3.5	3.5
132	Information systems audit controls	.60	0.0	3.4	4.0	2.0	0.0	4.0	0.0	3.6	3.4
133	Protection of information systems audit tools	.40	0.0	4.0	4.0	2.0	0.0	4.0	0.0	3.0	4.0

**Table C-2 All case studies assessment results concerned with the achievement of the ISO/IEC 27002 security objectives**

ISO/IEC 27002 Objective		W	Assessment Scores – Objectives Level								
			E1	E2	E3	E4	E5	E6	E7	E8	E9
1	Operational procedures and responsibilities	.08	3.7	3.1	3.5	.90	2.9	3.6	3.7	2.7	3.7
2	Third party service delivery management	.07	4.0	2.4	3.9	2.2	3.0	3.9	3.7	3.7	3.8
3	System planning and acceptance	.09	4.0	2.7	3.0	2.7	2.0	3.6	1.9	3.6	3.9
4	Protection against malicious and mobile code	.08	1.8	1.6	3.3	2.3	2.6	3.5	2.2	2.3	2.2
5	Back-up	.14	4.0	2.2	3.5	2.0	2.8	3.8	3.8	3.8	3.6
6	Network security management	.13	2.2	2.4	3.9	1.1	2.9	3.9	3.7	3.6	3.9
7	Media handling	.10	1.0	2.4	3.8	2.5	1.4	3.9	3.6	1.9	3.8
8	Exchange of information	.10	1.7	2.4	3.5	.40	1.2	3.0	2.8	3.8	3.7
9	Electronic commerce services	.09	0.0	1.0	4.0	0.0	2.1	3.7	0.0	2.3	3.7
10	Monitoring	.12	3.4	2.1	3.7	1.4	1.4	3.9	3.9	3.5	3.7
11	Business requirements for access control	.13	0.0	4.0	3.7	2.4	0.0	4.0	0.0	3.7	3.7
12	User access management	.15	2.9	4.0	3.3	2.0	2.7	4.0	3.5	3.0	2.5
13	User responsibilities	.14	4.0	4.0	3.7	1.5	2.3	4.0	3.7	2.8	3.7
14	Network access control	.15	2.8	4.0	3.4	1.4	2.4	4.0	3.6	2.9	3.8
15	Operating system access control	.14	2.0	4.0	3.9	0.5	1.9	4.0	3.4	3.2	3.6
16	Application and information access control	.15	2.1	4.0	4.0	2.7	2.2	4.0	3.3	3.3	3.7
17	Mobile computing and teleworking	.14	0.0	4.0	3.5	0.0	2.0	4.0	0.0	3.4	0.0
18	Security requirement of information systems	.18	4.0	1.6	4.0	1.6	2.5	4.0	3.6	3.5	4.0
19	Correct processing in applications	.16	0.0	1.6	4.0	1.5	2.5	4.0	3.9	3.2	3.7
20	Cryptographic controls	.19	0.0	2.3	4.0	0.0	1.1	4.0	0.0	3.1	3.6
21	Security of system files	.17	4.0	1.7	4.0	1.2	2.9	4.0	3.8	3.2	2.7
22	Security in development & support processes	.15	3.0	2.1	4.0	1.8	2.5	4.0	3.5	3.2	3.7
23	Technical vulnerability management	.15	0.0	1.8	4.0	2.4	2.2	4.0	3.8	3.2	3.8
24	Information security policy	1.0	0.0	2.8	3.6	0.6	1.7	3.3	1.0	3.2	3.8
25	Internal organisation	.65	0.7	4.0	4.0	4.0	1.7	3.7	4.0	2.6	3.5
26	External parties	.35	4.0	4.0	4.0	4.0	2.4	3.3	4.0	2.1	3.7
27	Responsibility of assets	.60	0.0	4.0	4.0	2.0	4.0	4.0	3.4	3.4	4.0
28	Information classification	.40	0.0	4.0	4.0	0.8	4.0	4.0	0.0	2.7	4.0
29	Reporting information security events and weaknesses	.70	0.0	2.8	4.0	0.0	1.6	4.0	3.4	4.0	2.2
30	Management of information security incidents and improvements	.30	2.9	1.8	4.0	0.0	0.9	4.0	2.8	0.0	2.6
31	Information security aspects of business continuity management	1.0	0.0	4.0	4.0	0.6	2.0	4.0	0.0	0.5	4.0
32	Prior to employment: “Employees, Contractors and Third party users”	.33	0.0	4.0	4.0	0.7	0.7	4.0	4.0	4.0	3.4
33	During employment: “Employees, Contractors and Third party users”	.32	2.0	4.0	4.0	2.1	1.0	4.0	4.0	4.0	3.7
34	Termination or change of employment: “Employees, Contractors and Third party users”	.35	3.3	4.0	4.0	1.2	2.3	4.0	4.0	4.0	3.7
35	Secure areas	.47	1.0	2.8	4.0	2.2	1.2	3.8	4.0	4.0	3.1
36	Equipment security	.53	3.7	2.5	4.0	1.4	2.6	3.7	4.0	4.0	3.5
37	Compliance with legal requirements	.33	1.4	3.0	4.0	1.0	2.2	3.7	0.0	2.9	3.2
38	Compliance with security policies and	.35	3.0	1.5	4.0	2.0	1.3	3.5	3.3	3.5	1.8
39	Information systems audit considerations	.32	0.0	3.3	4.0	2.0	0.9	3.9	0.0	3.5	3.6

**Table C-3 All case studies assessment results concerned with the achievement of the ISO/IEC 27002 security clauses**

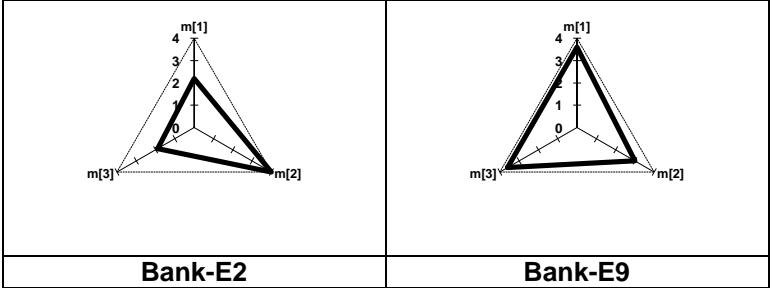
ISO/IEC 27002 Clause			W	Assessment Scores –Clause Level								
				E1	E2	E3	E4	E5	E6	E7	E8	E9
T	10	Communications and Operations Management	.40	2.6	2.2	3.6	1.5	2.2	3.7	3.0	3.2	3.6
	11	Access Control	.35	2.0	4.0	3.6	1.5	2.0	4.0	2.6	3.2	3.0
	12	Information Systems Acquisition, Development and Maintenance	.25	1.9	1.8	4.0	1.4	2.2	4.0	3.0	3.2	3.6
O	5	Security Policy	.20	0.0	2.8	3.6	0.6	1.7	3.3	1.0	3.3	3.8
	6	Organisation of Information Security	.25	1.8	4.0	4.0	4.0	1.9	3.6	4.0	2.5	3.6
	7	Asset Management	.25	0.0	4.0	4.0	1.5	4.0	4.0	2.1	3.1	4.0
	13	Information Security Incident Management	.15	0.9	2.5	4.0	0.0	1.4	4.0	3.2	2.8	2.3
	14	Business Continuity Management	.15	0.0	4.0	4.0	0.6	2.0	4.0	0.0	0.5	4.0
P	8	Human Resources Security	1.0	1.8	4.0	4.0	1.3	1.4	4.0	4.0	4.0	3.6
E	9	Physical and Environmental Security	.55	2.5	2.7	4.0	1.8	2.0	3.7	4.0	4.0	3.3
	15	Compliance	.45	1.5	2.6	4.0	1.7	1.5	3.7	1.1	3.3	2.8

**Table C-4 All case studies assessment results concerned with the achievement of the EISRM TOPE domains**

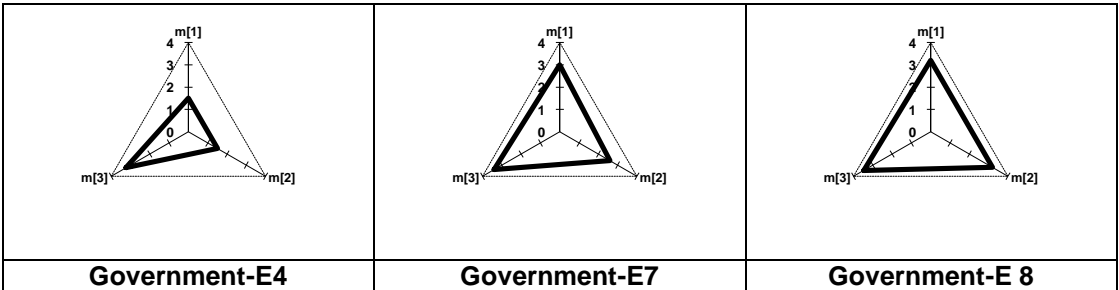
TOPE Domain		W	Assessment Score – domains Level								
			E1	E2	E3	E4	E5	E6	E7	E8	E9
1	Technology	0.50	2.2	2.8	3.7	1.5	2.1	3.9	2.9	3.2	3.4
2	Organisation	0.25	0.6	3.5	3.9	1.6	2.3	3.8	2.2	2.6	3.6
3	People	0.10	1.8	4.0	4.0	1.3	1.4	4.0	4.0	4.0	3.6
4	Environment	0.15	2.0	2.6	4.0	1.7	1.7	3.7	2.7	3.9	3.1
TOPE s-readiness		Of 4	1.7	3.1	3.8	1.5	2.0	3.9	2.8	3.2	3.4
		%	43	78	95	38	50	96	70	80	85
% Achieving Essential Controls			0	100	100	0	67	100	0	100	67
% Achieving Common Controls			25	88	100	44	69	100	63	56	94

**Technology Domain**  
(ISO/IEC 27002 – clause level)

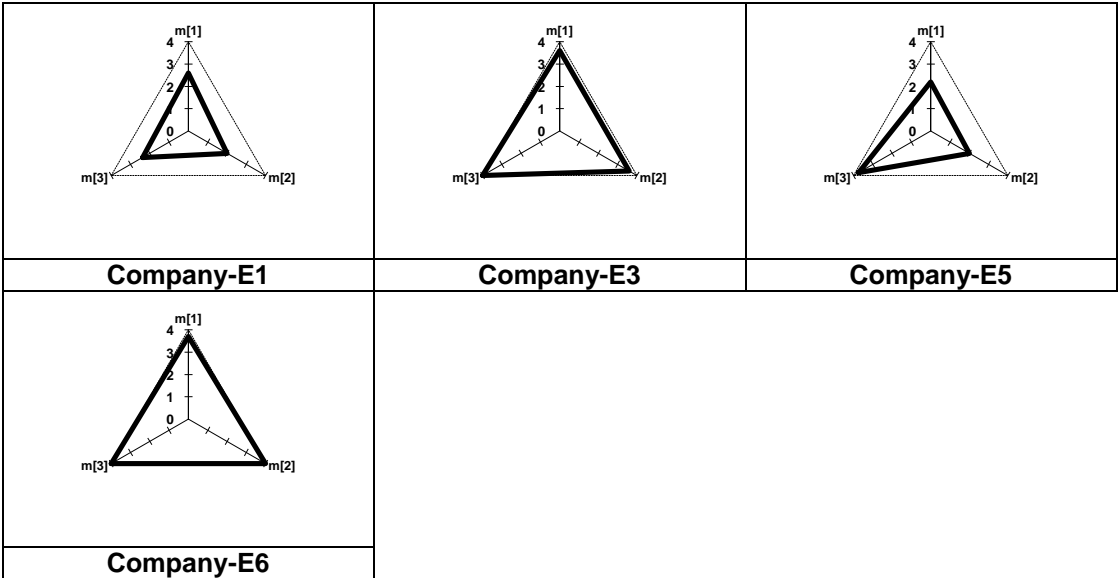
**Group "A" Financial Sector**



**Group "B" Public Sector**



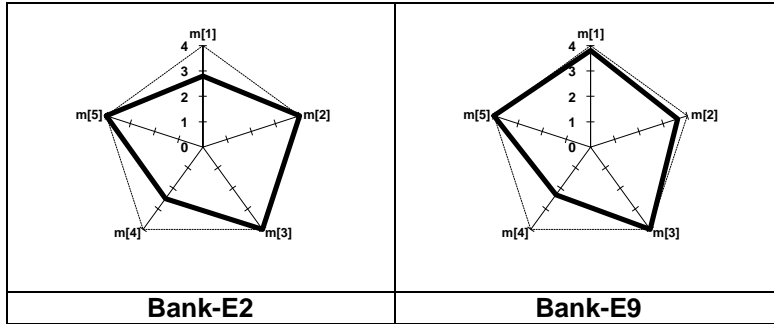
**Group "C" Private Sector**



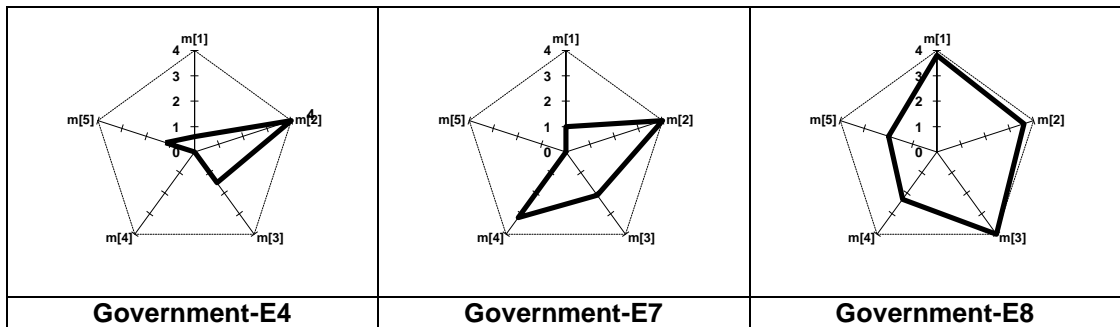
**Figure C-1 All case studies results concerned with the achievement of the ISO/IEC27002 technical security objectives (*Technology Domain*)**

## Organisation Domain (ISO/IEC 27002 – clause level)

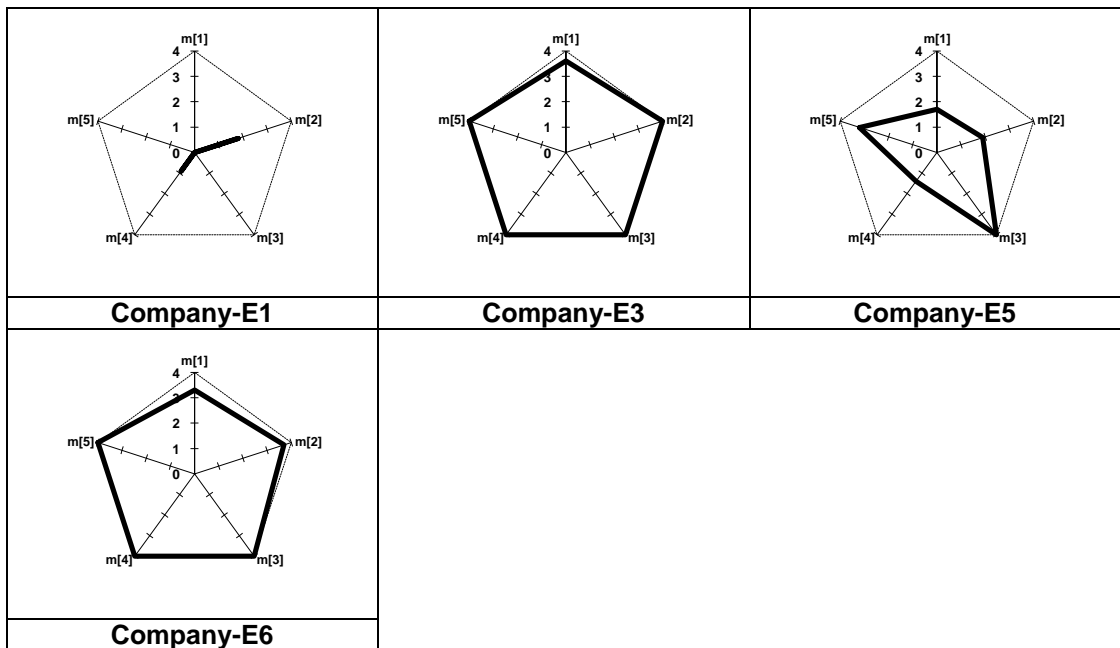
### Group "A" Financial Sector



### Group "B" Public Sector



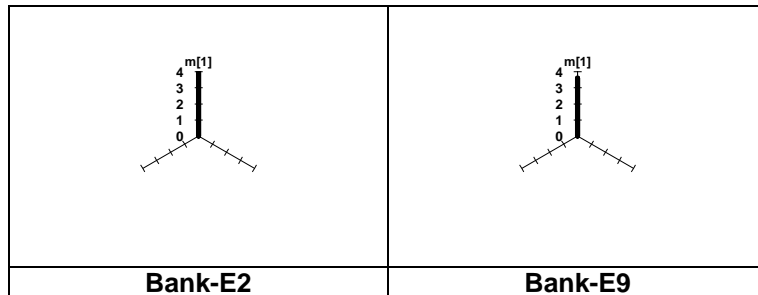
### Group "C" Private Sector



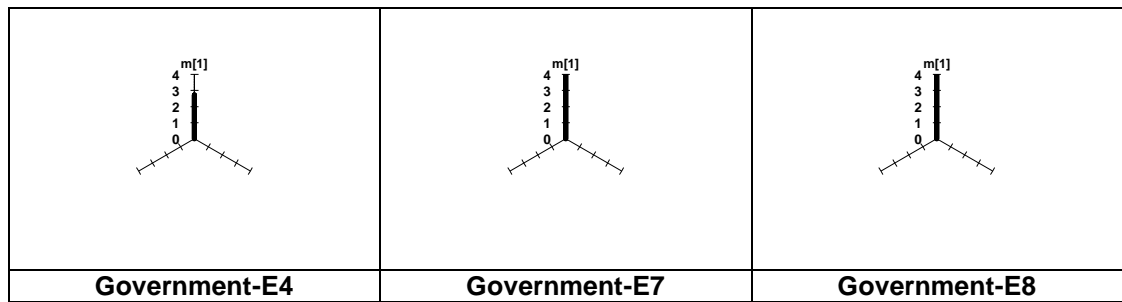
**Figure C-2 All case studies results concerned with the achievement of the ISO/IEC27002 organisation security objective (*Organisation Domain*)**

## People Domain (ISO/IEC 27002 – clause level)

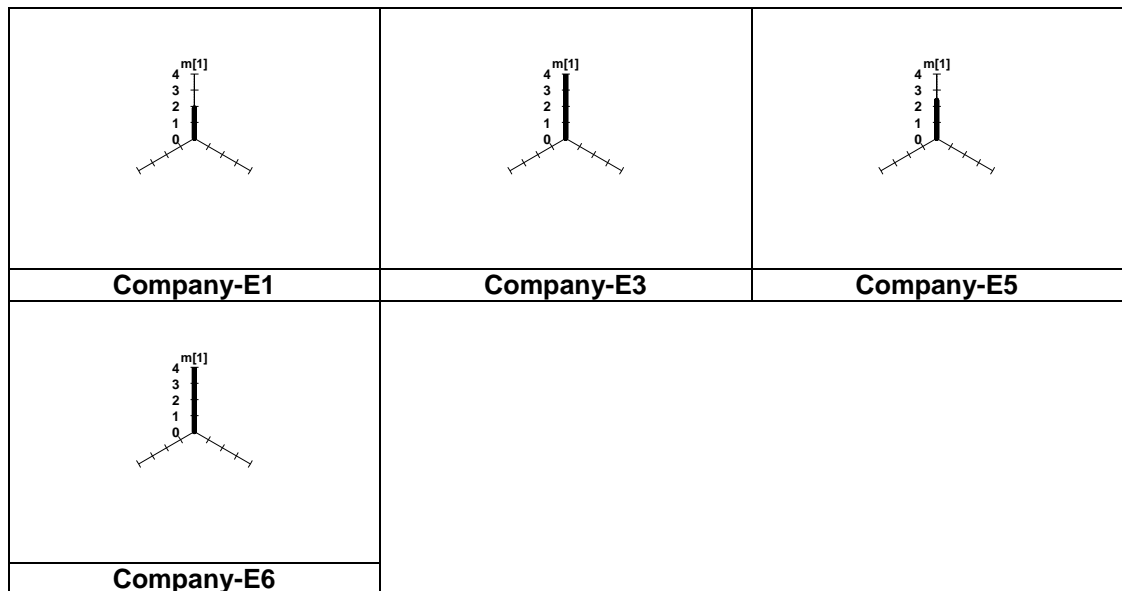
### Group "A" Financial Sector



### Group "B" Public Sector



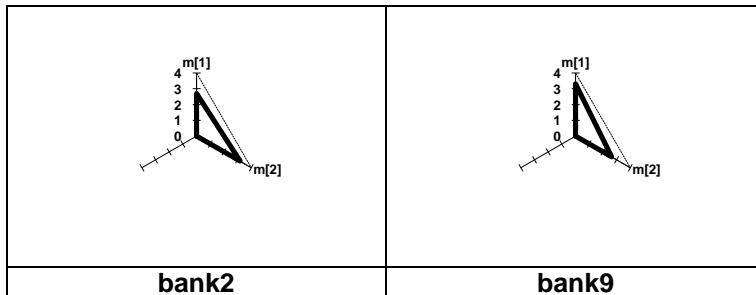
### Group "C" Private Sector



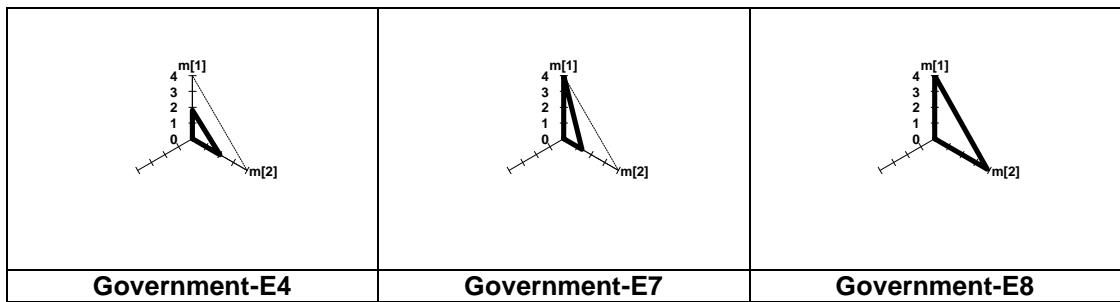
**Figure C-3 All case studies results concerned with the achievement of the ISO/IEC27002 human security objective (*People Domain*)**

## Environment Domain (ISO/IEC 27002 – clause level)

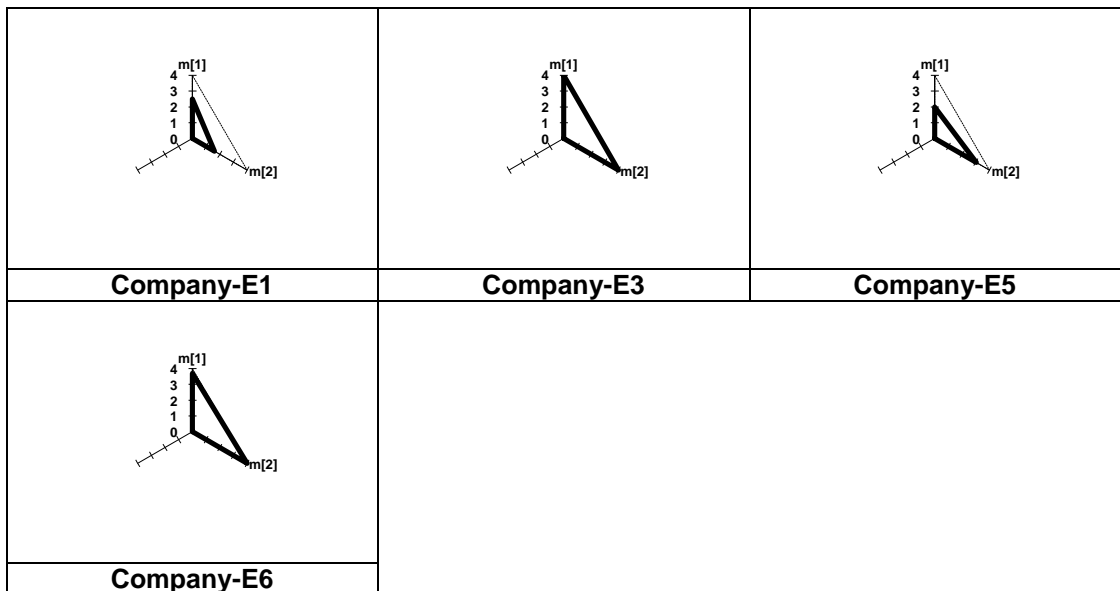
### Group "A" Financial Sector



### Group "B" Public Sector



### Group "C" Private Sector



**Figure C-4 All case studies results concerned with the achievement of the ISO/IEC 27002 environment security objectives (*Environment Domain*)**

# Appendix D

## EISRM ASSESSMENT TOOL

The following tool is developed using “Access Software” and “C #” to help in evaluating enterprises according to the EISRM assessment model presented in the thesis. The tool is still in its early stages and the plan is to enhance this tool in the near future to help enterprises in conducting risk management according to EISRM framework. The tool in its form now is only concerned with the EISRM information security assessment model. The tool is designed to receive the input data from the users and conducts the required calculations.. The tool presents the results in printed reports. This appendix serves as a guide in installing and getting started with the EISRM prototype tool.

### D.1 Installation Requirements

The following minimum system requirements should be met in order to run the EISRM information security assessment prototype tool.

- A Pentium IV 1.4 MHz or better processor.
- 1GB RAM.
- Microsoft Windows 2000/XP/Vista.

### D.2 Installing the EISRM Tool

The EISRM prototype tool is included with the research CD in “ZIP” format. Once the user copies it on his PC he could extract it then start the installation according to the following steps.

- Extracting the EISRM tool.



- Create a temporary folder on the hard drive of your computer and call it, for example, C:\temp.
- Copy the “EISRM Assessment tool” file from the CD to the hard drive of your computer into the C:\temp folder.
- Installing the EISRM tool
  - Double click on the “C:\temp\EISRM Assessment tool” file
  - Click on OK button. The EISRM tool software should open
  - The installation software will automatically create the C:\Document\user\topeCompliance” subfolder on your computer’s hard drive.

The EISRM prototype tool software installation procedure is now completed successfully.

### D.3 Source Code of the EISRM Tool

The EISRM prototype tool is developed using Microsoft Access 2003. The interface for the EISRM prototype tool source code is written in Microsoft “C#”.

The source code is presented in the following

#### D.3.1 Source Code of the Initialization Part

##### 1. Open The Connection

##### 2. Fill The Measure & Importance lists

```
private void Interface_Load(object sender, EventArgs e)
{
    string ConnectionSTR =
"Provider=Microsoft.Jet.OLEDB.4.0;"+ "Data Source= "
+Application.StartupPath + "\\complianceModel.mdb";
objConnection = new OleDbConnection(ConnectionSTR);
try
{
    //Open The Connection
    objConnection.Open();
}
catch
{
    Exception Exp = new Exception();
    MessageBox.Show(Exp.Message);
    this.Close();
    return;
}
}
```

```

        FillCmb();
        pnlNavStrategy_Click(sender,e);
    }

private void FillCmb()
{
    measureArr = new string[5];
    measureArr[0] = "0-None";
    measureArr[1] = "1-Poor";
    measureArr[2] = "2-Average";
    measureArr[3] = "3-Good";
    measureArr[4] = "4-Excellent";
    cmbMeasure.Items.Clear();
    {
        for (int i = 0; i < 5; i++)
            cmbMeasure.Items.Add(measureArr[i]);
    }
    importanceArr = new string[5];
    importanceArr[0] = "1-None";
    importanceArr[1] = "2-Low";
    importanceArr[2] = "3-Moderate";
    importanceArr[3] = "4-Important";
    importanceArr[4] = "5-veryImportant";
    cmbImportance.Items.Clear();
    {
        for (int i = 0; i < 5; i++)
        {
            cmbImportance.Items.Add(importanceArr[i]);
            cmbSImportance.Items.Add(importanceArr[i]);
            cmbTImportance.Items.Add(importanceArr[i]);
            cmbOImportance.Items.Add(importanceArr[i]);
            cmbEImportance.Items.Add(importanceArr[i]);
            cmbPImportance.Items.Add(importanceArr[i]);
        }
    }
}
}

```

### D.3.2 Source Code of the Functions Part

1. Load Parts into the tree view
2. Load parts into the list view
3. Calculate measure of apart from its objectives
4. Flush measure & weight of parts into database

```

private void LoadParts(int DomainID, TreeNode DNode)
{
    int count = 0;
    objPartsCommand = new OleDbCommand();
    objPartsCommand.CommandText = "Usp_SelectParts";
    objPartsCommand.CommandType =
CommandType.StoredProcedure;
    objPartsCommand.Connection = objConnection;
    objPartsCommand.Parameters.Add("@DomainID",
OleDbType.Integer).Value
= DomainID;
    objPartsReader = objPartsCommand.ExecuteReader();
    while (objPartsReader.Read())
    {
        count++;
        // objPartsReader[1] refers to part Name
        DNode.Nodes.Add(objPartsReader[1].ToString());
        int PartID = Convert.ToInt32(objPartsReader[0]);
    }
}

```

```

        DNode.Nodes[count - 1].Tag = PartID;
        LoadObjectives(PartID, DNode.Nodes[count - 1]);
    }
    objPartsReader.Dispose();
    objPartsCommand.Dispose();
}
private void LoadPartsList(int DomainID)
{
    int Count = 0;
    grbParent.Text = tvwPFactors.SelectedNode.Text;
    objPartsCommand = new OleDbCommand();
    objPartsCommand.CommandText = "Usp_SelectParts";
    objPartsCommand.CommandType =
CommandType.StoredProcedure;
    objPartsCommand.Connection = objConnection;
    objPartsCommand.Parameters.Add("@DomainID",
OleDbType.Integer).Value
                                = DomainID;
    objPartsReader = objPartsCommand.ExecuteReader();
    while (objPartsReader.Read())
    {
        Count++;
        // objMeasuresReader[1] refers to Measure Name
        lvwQuestions.Items.Add(objPartsReader[1].ToString());
        int PartID = Convert.ToInt32(objPartsReader["ID"]);
        int Importance =
Convert.ToInt32(objPartsReader["Weight"]);
        int Measure =
Convert.ToInt32(CalculatePartlMeasure(PartID));
        lvwQuestions.Items[Count - 1].Tag =
PartID.ToString();
        lvwQuestions.Items[Count -
1].SubItems.Add(GetMeasure(Measure));
        lvwQuestions.Items[Count -
1].SubItems.Add(GetImportance(Importance));
        lvwQuestions.Items[Count - 1].SubItems.Add("Part" +
Count.ToString());
    }
    lvwQuestions.Items[0].Selected = true;
    lblQuestion.Text = lvwQuestions.Items[0].Text;
    lblQuestion.Tag = lvwQuestions.Items[0].Tag;
    objPartsReader.Dispose();
    objPartsCommand.Dispose();
}
private double CalculatePartlMeasure(int PartID)
{
    int Count = 0;
    double ImportanceSum = 0, MeasureSum = 0;
    objObjectivesCommand = new OleDbCommand();
    objObjectivesCommand.CommandText =
"Usp_SelectObjectives";
    objObjectivesCommand.CommandType =
CommandType.StoredProcedure;
    objObjectivesCommand.Connection = objConnection;
    objObjectivesCommand.Parameters.Add("@PartID",
OleDbType.Integer).Value
                                = PartID;
    objObjectivesReader =
objObjectivesCommand.ExecuteReader();
    while (objObjectivesReader.Read())
    {
        Count++;

```

```

        int Importance =
Convert.ToInt32(objObjectivesReader["Weight"]);
        int Measure =
Convert.ToInt32(objObjectivesReader["Measure"]);
        ImportanceSum += Importance;
        MeasureSum += Measure * Importance;
    }
    double dblMeasure = MeasureSum / ImportanceSum;
    objObjectivesReader.Dispose();
    objObjectivesCommand.Dispose();
    return (Math.Round(dblMeasure));
}
private void FlushParts(int ID, int Measure, int Importance)
{
    objPartsCommand = new OleDbCommand();
    objPartsCommand.CommandText = "Usp_UpdateParts";
    objPartsCommand.CommandType =
CommandType.StoredProcedure;
    objPartsCommand.Connection = objConnection;
    objPartsCommand.Parameters.Add("@Measure",
OleDbType.Integer).Value = Measure;
    objPartsCommand.Parameters.Add("@Weight",
OleDbType.Integer).Value = Importance;
    objPartsCommand.Parameters.Add("@ID",
OleDbType.Integer).Value = ID;
    int rowsAffected = objPartsCommand.ExecuteNonQuery();
    if (rowsAffected != 1)
        MessageBox.Show("");
    objPartsCommand.Dispose();
}

```

### D.3.2.1 Source Code of the Objectives Functions

#### Objectives Functions Part

1. Load Objectives into the tree view
2. Load Objectives into the list view
3. Calculate measure of an Objective from its objectives
4. Flush measure & weight of objectives into database

```

private void LoadObjectives(int PartID, TreeNode PartNode)
{
    int count = 0;
    objObjectivesCommand = new OleDbCommand();
    objObjectivesCommand.CommandText =
"Usp_SelectObjectives";
    objObjectivesCommand.CommandType =
CommandType.StoredProcedure;
    objObjectivesCommand.Connection = objConnection;
    objObjectivesCommand.Parameters.Add("@PartID",
OleDbType.Integer).Value
= PartID;
    objObjectivesReader =
objObjectivesCommand.ExecuteReader();
    while (objObjectivesReader.Read())
    {
        count++;
        // objObjectivesReader[1] refers to Objective Name
PartNode.Nodes.Add(objObjectivesReader[1].ToString());
        int ObjectiveID =
Convert.ToInt32(objObjectivesReader[0]);

```

```

        PartNode.Nodes[count - 1].Tag = ObjectiveID;
        LoadControls(ObjectiveID, PartNode.Nodes[count - 1]);
    }
    objObjectivesReader.Dispose();
    objObjectivesCommand.Dispose();
}
private void LoadObjectivesList(int PartID)
{
    int Count = 0;
    grbParent.Text = tvwPFactors.SelectedNode.Text;
    objObjectivesCommand = new OleDbCommand();
    objObjectivesCommand.CommandText =
"Usp_SelectObjectives";
    objObjectivesCommand.CommandType =
CommandType.StoredProcedure;
    objObjectivesCommand.Connection = objConnection;
    objObjectivesCommand.Parameters.Add("@PartID",
OleDbType.Integer).Value
                                = PartID;
    objObjectivesReader =
objObjectivesCommand.ExecuteReader();
    while (objObjectivesReader.Read())
    {
        Count++;
        // objMeasuresReader[1] refers to Measure Name
lvwQuestions.Items.Add(objObjectivesReader[1].ToString());
        int ObjectiveID =
Convert.ToInt32(objObjectivesReader["ID"]);
        int Importance =
Convert.ToInt32(objObjectivesReader["Weight"]);
        int Measure =
Convert.ToInt32(CalculateObjectivelMeasure(ObjectiveID));
        lvwQuestions.Items[Count - 1].Tag =
ObjectiveID.ToString();
        lvwQuestions.Items[Count -
1].SubItems.Add(GetMeasure(Measure));
        lvwQuestions.Items[Count -
1].SubItems.Add(GetImportance(Importance));
        lvwQuestions.Items[Count - 1].SubItems.Add("Obj" +
Count.ToString());
    }
    lvwQuestions.Items[0].Selected = true;
    lblQuestion.Text = lvwQuestions.Items[0].Text;
    lblQuestion.Tag = lvwQuestions.Items[0].Tag;
    objObjectivesReader.Dispose();
    objObjectivesCommand.Dispose();
}
private double CalculateObjectivelMeasure(int ObjectiveID)
{
    int Count = 0;
    double ImportanceSum = 0, MeasureSum = 0;
    objControlsCommand = new OleDbCommand();
    objControlsCommand.CommandText = "Usp_SelectControls";
    objControlsCommand.CommandType =
CommandType.StoredProcedure;
    objControlsCommand.Connection = objConnection;
    objControlsCommand.Parameters.Add("@ObjectiveID",
OleDbType.Integer).Value
                                = ObjectiveID;
    objControlsReader = objControlsCommand.ExecuteReader();
    while (objControlsReader.Read())

```

```

        {
            Count++;
            int Importance =
Convert.ToInt32(objControlsReader["Weight"]);
            int Measure =
Convert.ToInt32(objControlsReader["Measure"]);
            ImportanceSum += Importance;
            MeasureSum += Measure * Importance;
        }
        double dblMeasure = MeasureSum / ImportanceSum;
        objControlsReader.Dispose();
        objControlsCommand.Dispose();
        return (Math.Round(dblMeasure));
    }
    private void FlushObjectives(int ID, int Measure, int
Importance)
    {
        objObjectivesCommand = new OleDbCommand();
        objObjectivesCommand.CommandText =
"Usp_UpdateObjectives";
        objObjectivesCommand.CommandType =
CommandType.StoredProcedure;
        objObjectivesCommand.Connection = objConnection;
        objObjectivesCommand.Parameters.Add("@Measure",
OleDbType.Integer).Value = Measure;
        objObjectivesCommand.Parameters.Add("@Weight",
OleDbType.Integer).Value = Importance;
        objObjectivesCommand.Parameters.Add("@ID",
OleDbType.Integer).Value = ID;
        int rowsAffected =
objObjectivesCommand.ExecuteNonQuery();
        if (rowsAffected != 1)
            MessageBox.Show("");
        objObjectivesCommand.Dispose();
    }

```

### D.3.2.2 Source Code of the Controls Functions

1. Load Controls into the tree view
2. Load Controls into the list view
3. Calculate measure of a Control from its objectives
4. Flush measure & weight of controls into database

```

private void LoadControls(int ObjectiveID, TreeNode ObjectiveNode)
{
    int count = 0;
    objControlsCommand = new OleDbCommand();
    objControlsCommand.CommandText = "Usp_SelectControls";
    objControlsCommand.CommandType =
CommandType.StoredProcedure;
    objControlsCommand.Connection = objConnection;
    objControlsCommand.Parameters.Add("@ObjectiveID",
OleDbType.Integer).Value
= ObjectiveID;
    objControlsReader = objControlsCommand.ExecuteReader();
    while (objControlsReader.Read())
    {
        count++;
        // objControlsReader[1] refers to Control Name
ObjectiveNode.Nodes.Add(objControlsReader[1].ToString());
        int ControlID =
Convert.ToInt32(objControlsReader[0]);
        ObjectiveNode.Nodes[count - 1].Tag = ControlID;
    }
}

```

```

    }
    if (listpopulated < 1)
    {
        tvwPFactors.SelectedNode = ObjectiveNode.Nodes[0];
        tvwPFactors.SelectedNode.Expand();
    }
    objControlsReader.Dispose();
    objControlsCommand.Dispose();
}
private void LoadControlsList(int ObjectiveID)
{
    int Count = 0;
    grbParent.Text = tvwPFactors.SelectedNode.Text;
    objControlsCommand = new OleDbCommand();
    objControlsCommand.CommandText = "Usp_SelectControls";
    objControlsCommand.CommandType =
CommandType.StoredProcedure;
    objControlsCommand.Connection = objConnection;
    objControlsCommand.Parameters.Add("@ObjectiveID",
OleDbType.Integer).Value
                                = ObjectiveID;
    objControlsReader = objControlsCommand.ExecuteReader();
    while (objControlsReader.Read())
    {
        Count++;
        // objMeasuresReader[1] refers to Measure Name
        lvwQuestions.Items.Add(objControlsReader[1].ToString());
        int ControlID =
Convert.ToInt32(objControlsReader["ID"]);
        int Importance =
Convert.ToInt32(objControlsReader["Weight"]);
        int Measure =
Convert.ToInt32(CalculateControlMeasure(ControlID));
        lvwQuestions.Items[Count - 1].Tag =
ControlID.ToString();
        lvwQuestions.Items[Count -
1].SubItems.Add(GetMeasure(Measure));
        lvwQuestions.Items[Count -
1].SubItems.Add(GetImportance(Importance));
        lvwQuestions.Items[Count - 1].SubItems.Add("C" +
Count.ToString());
    }
    lvwQuestions.Items[0].Selected = true;
    lblQuestion.Text = lvwQuestions.Items[0].Text;
    lblQuestion.Tag = lvwQuestions.Items[0].Tag;
    objControlsReader.Dispose();
    objControlsCommand.Dispose();
}
private void FlushControl(int ID, int Measure, int
Importance)
{
    objControlsCommand = new OleDbCommand();
    objControlsCommand.CommandText = "Usp_UpdateControls";
    objControlsCommand.CommandType =
CommandType.StoredProcedure;
    objControlsCommand.Connection = objConnection;
    objControlsCommand.Parameters.Add("@Measure",
OleDbType.Integer).Value = Measure;
    objControlsCommand.Parameters.Add("@Weight",
OleDbType.Integer).Value = Importance;
    objControlsCommand.Parameters.Add("@ID",
OleDbType.Integer).Value = ID;
}

```

```

        int rowsAffected = objControlsCommand.ExecuteNonQuery();
        if (rowsAffected != 1)
            MessageBox.Show("");
        objControlsCommand.Dispose();
    }
    private double CalculateControlMeasure(int ControlID)
    {
        int Count = 0;
        double ImportanceSum = 0, MeasureSum = 0;
        objMeasuresCommand = new OleDbCommand();
        objMeasuresCommand.CommandText = "Usp_SelectMeasures";
        objMeasuresCommand.CommandType =
CommandType.StoredProcedure;
        objMeasuresCommand.Connection = objConnection;
        objMeasuresCommand.Parameters.Add("@ControlID",
OleDbType.Integer).Value
            = ControlID;
        objMeasuresReader = objMeasuresCommand.ExecuteReader();
        while (objMeasuresReader.Read())
        {
            Count++;
            int Importance =
Convert.ToInt32(objMeasuresReader["Weight"]);
            int Measure =
Convert.ToInt32(objMeasuresReader["Measure"]);
            ImportanceSum += Importance;
            MeasureSum += Measure * Importance;
        }
        double dblMeasure = MeasureSum / ImportanceSum;
        objMeasuresReader.Dispose();
        objMeasuresCommand.Dispose();
        return (Math.Round(dblMeasure));
    }

```

### D.3.2.3 Source Code of the Measures Functions

#### 5. Load Measures into the list view

#### 6. Flush measure & weight of Measures into database

```

private void LoadMeasures(int ControlID, TreeNode ControlNode)
{
    listpopulated++;
    int Count = 0;
    tvwPFactors.SelectedNode = ControlNode;
    tvwPFactors.Focus();
    grbParent.Text = ControlNode.Text;
    objMeasuresCommand = new OleDbCommand();
    objMeasuresCommand.CommandText = "Usp_SelectMeasures";
    objMeasuresCommand.CommandType =
CommandType.StoredProcedure;
    objMeasuresCommand.Connection = objConnection;
    objMeasuresCommand.Parameters.Add("@ControlID",
OleDbType.Integer).Value
        = ControlID;
    objMeasuresReader = objMeasuresCommand.ExecuteReader();
    while (objMeasuresReader.Read())
    {
        Count++;
        // objMeasuresReader[1] refers to Measure Name
        lvwQuestions.Items.Add(objMeasuresReader[1].ToString());
        int MeasureID =
Convert.ToInt32(objMeasuresReader["ID"]);
        int Importance =
Convert.ToInt32(objMeasuresReader["Weight"]);
    }
}

```



```

        int Measure =
Convert.ToInt32(objMeasuresReader["Measure"]);
        lvwQuestions.Items[Count - 1].Tag =
MeasureID.ToString();
        lvwQuestions.Items[Count -
1].SubItems.Add(GetMeasure(Measure));
        lvwQuestions.Items[Count -
1].SubItems.Add(GetImportance(Importance));
        lvwQuestions.Items[Count - 1].SubItems.Add("M" +
Count.ToString());
    }
    lvwQuestions.Items[0].Selected = true;
    lblQuestion.Text = lvwQuestions.Items[0].Text;
    lblQuestion.Tag = lvwQuestions.Items[0].Tag;
    objMeasuresReader.Dispose();
    objMeasuresCommand.Dispose();
}
private void FlushMeasure(int ID, int Measure, int
Importance)
{
    objMeasuresCommand = new OleDbCommand();
    objMeasuresCommand.CommandText = "Usp_UpdateMeasures";
    objMeasuresCommand.CommandType =
CommandType.StoredProcedure;
    objMeasuresCommand.Connection = objConnection;
    objMeasuresCommand.Parameters.Add("@Measure",
OleDbType.Integer).Value = Measure;
    objMeasuresCommand.Parameters.Add("@Weight",
OleDbType.Integer).Value = Importance;
    objMeasuresCommand.Parameters.Add("@ID",
OleDbType.Integer).Value = ID;
    int rowsAffected = objMeasuresCommand.ExecuteNonQuery();
    if (rowsAffected != 1)
        MessageBox.Show("");
    objMeasuresCommand.Dispose();}

```

### D.3.2.4 Source Code of Saving & Navigation Functions

```

private void Save()
{
    int NoOfMeasures = lvwQuestions.Items.Count;
    if (tvwPFactors.SelectedNode.Level == 0)
    {
        for (int i = 0; i < NoOfMeasures; i++)
        {
            int ID =
Convert.ToInt32(lvwQuestions.Items[i].Tag);
            int imp =
GetNumericImportance(lvwQuestions.Items[i].SubItems[2].Text);
            int mea =
GetNumericMeasure(lvwQuestions.Items[i].SubItems[1].Text);
            FlushParts(ID, mea, imp);
        }
        Navigate();
    }
    else if (tvwPFactors.SelectedNode.Level == 1)
    {
        for (int i = 0; i < NoOfMeasures; i++)
        {
            int ID =
Convert.ToInt32(lvwQuestions.Items[i].Tag);

```

```

        int imp =
GetNumericImportance(lvwQuestions.Items[i].SubItems[2].Text);
        int mea =
GetNumericMeasure(lvwQuestions.Items[i].SubItems[1].Text);
        FlushObjectives(ID, mea, imp);
    }
    Navigate();
}
else if (tvwPFactors.SelectedNode.Level == 2)
{
    for (int i = 0; i < NoOfMeasures; i++)
    {
        int ID =
Convert.ToInt32(lvwQuestions.Items[i].Tag);
        int imp =
GetNumericImportance(lvwQuestions.Items[i].SubItems[2].Text);
        int mea =
GetNumericMeasure(lvwQuestions.Items[i].SubItems[1].Text);
        FlushControl(ID, mea, imp);
    }
    Navigate();
}
else if (tvwPFactors.SelectedNode.Level == 3)
{
    for (int i = 0; i < NoOfMeasures; i++)
    {
        int ID =
Convert.ToInt32(lvwQuestions.Items[i].Tag);
        int imp =
GetNumericImportance(lvwQuestions.Items[i].SubItems[2].Text);
        int mea =
GetNumericMeasure(lvwQuestions.Items[i].SubItems[1].Text);
        FlushMeasure(ID, mea, imp);
    }
    Navigate();
}
}
private bool CheckData(int NoOfMeasures)
{
    for (int i = 0; i < NoOfMeasures; i++)
    {
        if (lvwQuestions.Items[i].SubItems[1].Text == "null"
||
        lvwQuestions.Items[i].SubItems[2].Text == "null")
            return false;
    }
    return true;
}
private void Navigate()
{
    TreeNode MyNode;
    tvwPFactors.SelectedNode.ForeColor = Color.Black;
    if (tvwPFactors.SelectedNode.Level == 0)
    {
        MyNode = tvwPFactors.SelectedNode;
        MessageBox.Show("Parts Completed");
    }
    if (tvwPFactors.SelectedNode.Level == 1)
    {
        MyNode = tvwPFactors.SelectedNode;
        if (MyNode == MyNode.Parent.LastNode)
        {

```



```
tvwPFactors.SelectedNode.Checked = true;}
```

### D.3.2.5 Source Code of the Charts

```
private void CreateChart()
{
    // Set the chart type
    chart1.Type = ChartType.Radars;
    // Set the size
    //chart1.Width = 600;
    //chart1.Height = 350;
    // Set the temp directory
    chart1.TempDirectory = "temp";
    // Debug mode. ( Will show generated errors if any )
    chart1.Debug = true;
    chart1.Title = "";

    chart1.TitleBox.Position =
TitleBoxPosition.FullWithLegend;
    chart1.DefaultSeries.Type = SeriesType.Line;
    chart1.DefaultElement.Marker.Size = 10;
    // *DYNAMIC DATA NOTE*
    // This sample uses random data to populate the chart. To
populate
    // a chart with database data see the following
resources:
    // - Classic samples folder
    // - Help File > Data Tutorials
    // - Sample: features/DataEngine.aspx
    SeriesCollection mySC = getMeasureData();
    // Add the random data.
    chart1.SeriesCollection.Clear();
    chart1.SeriesCollection.Add(mySC);
}
SeriesCollection getMeasureData()
{
    SeriesCollection SC = new SeriesCollection();
    Random myR = new Random(1);
    Series s = new Series();
    s.Name = tvwPFactors.SelectedNode.Text;
    for (int b = 0; b < lvwQuestions.Items.Count; b++)
    {
        Element e = new Element();
        e.Name = lvwQuestions.Items[b].SubItems[3].Text;
        e.YValue =
GetNumericMeasure(lvwQuestions.Items[b].SubItems[1].Text);
        s.Elements.Add(e);
    }
    SC.Add(s);
    // Set Different Colors for our Series
    SC[0].DefaultElement.Color = Color.Red;
    //SC[2].DefaultElement.Color = Color.FromArgb(255,99,49);
    //SC[3].DefaultElement.Color = Color.FromArgb(0,156,255);

    return SC;}
}
```

## D.4 Running the EISRM Tool

When the EISRM prototype is loaded, it presents the user with a GUI, as shown in Figure D-1. Input screens for the personal, business, and TOPE/ISO domains are shown in Figures D-2, D-3 and D-4 respectively.

**Figure D-1 EISRM tool - Input screen for the “Personal Profile”**

The screenshot shows a Microsoft Word window displaying a form titled 'Profile'. The form has two tabs: 'Personal Profile' and 'Business Profile'. The 'Personal Profile' tab is active. The form contains the following fields and options:

- What is the type of your organization?  Public  Private
- What is the size of your organization terms of its number of employees? (Dropdown menu)
- What is the field of your organization? (Dropdown menu with options: Less than 100, 100 to 500, 501 to 1000, 1001 to 3000, Over 3000)
- How long has your organization been in business? (Dropdown menu)
- Does your organization have separate Information Security Department?  Yes  No
- Number of computers (either PCs or Workstations) in your organization: (Dropdown menu)

A 'Save' button is located at the bottom of the form. The background shows a Microsoft Word interface with various toolbars and a taskbar at the bottom.

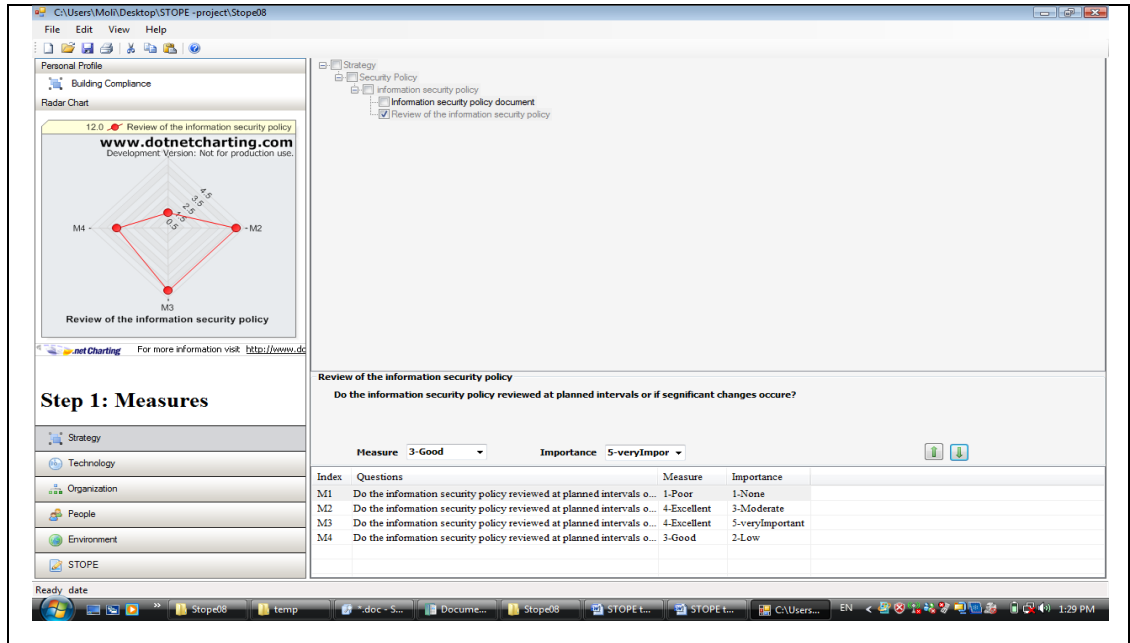
**Figure D-2 EISRM tool - Input screen for the “Business Profile”**

The screenshot shows a Windows Explorer window displaying a form titled 'Profile'. The form has two tabs: 'Personal Profile' and 'Business Profile'. The 'Business Profile' tab is active. The form contains the following fields and options:

- Company Name (Text input)
- Address (Optional) (Text input)
- Nationality?  Local  Non-Local
- Age? (Dropdown menu)
- Academic qualifications: degree(s)? (Dropdown menu)
- Field of study? (Dropdown menu)
- Special qualifications in Information Security?  CIW  CISSP  SANS  MS
- Position? (Dropdown menu)
- How long have you been in IS/IT department of your current employer (organization)? (Dropdown menu)

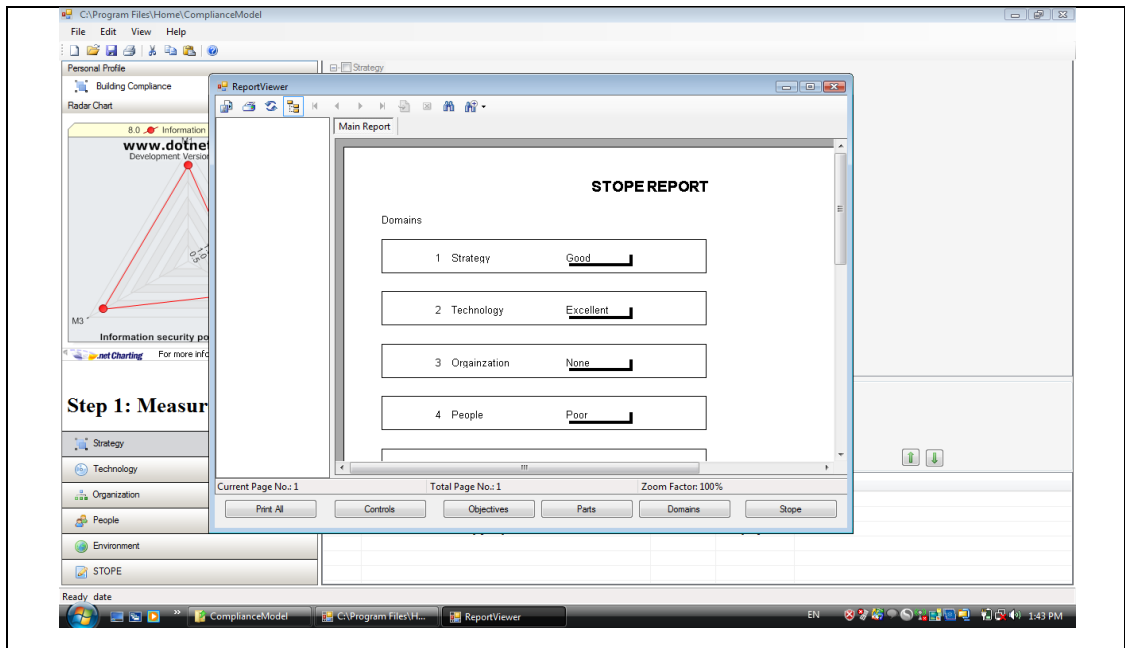
A 'Continue' button is located at the bottom of the form. The background shows a Windows Explorer interface with a sidebar on the left and a taskbar at the bottom.

**Figure D-3 EISRM tool - Input screen for the TOPE domains**



The EISRM prototype tool could be used in printing reports. The user of the tool could use these reports for presenting the results in numerically and graphically. Figure D-4 shows an example for the types of reports.

**Figure D-4 EISRM tool – Example of reports for the TOPE domains**



# Appendix E

## PUBLICATIONS

### A. Conference Contributions:

1. Saleh, M. S., Alrabiah, A., and Bakry, S. H., (2006). "*E-Business Diffusion Requirements: A STOPE View for Easing the Use of ISO 17799 Information Security Management Standard*", Proceeding of the First National Information Technology Symposium (NITS 2006), Riyadh, Saudi Arabia, 6-8 February.
2. Saleh, M. S., Mellor, J. E., Cullen, A. J., and Bakry, S. H., (2006). "*A STOPE approach for the evaluation of compliance of organizations with ISO 17799-2005*", First Conference on Advances in Computer Security and Forensics (ACSF), 13<sup>th</sup> and 14<sup>th</sup> July, Liverpool John Moores University, Liverpool, UK.
3. Saleh, M. S., Mellor, J. E., Cullen, A. J., and Bakry S. H., (2006). "*Structured evaluation of site security using an agent based hierarchical approach to ISO 17799*", Fourth International Conference on Performance Modeling and Evaluation of Heterogeneous networks (HET-NETs '06), Ilkley, West Yorkshire, UK.
4. Saleh, M. S., Alfantookh, A., Mellor, J. E., and Bakry, S. H., (2008). "*An Open Reference Framework For Enterprise Information Security Risk Management Using the STOPE Scope and the Six-Sigma Process*", Proceedings of the Fourteenth Americas Conference on Information Systems, Toronto, Canada, August 14<sup>th</sup>-17<sup>th</sup>.
5. Saleh, M. S., Alfantookh, A., and Bakry S. H., (2008). "*A STOPE-Based Incremental Method for the Assessment of Enterprise Information Security Using ISO 17799 Standard*", Proceedings of the 19<sup>th</sup> National Computer Conference (NCC19) on Digital Economy and ICT industry, Riyadh, Saudi Arabia, November 1<sup>st</sup>-5<sup>th</sup>.

### B. Journal Publications:

1. Saleh, M. S., Alrabiah, A., and Bakry, S. H., (2007). "*ISO Information Security Standards: A Common and Safe Environment for e-Services*", Journal of Applied Computing & Informatics, 6(1): 73-80.
2. Saleh, M.S., Alrabiah, A., and Bakry, S.H., (2006). "*Using ISO 17799-2005 security management standard: A STOPE view with six sigma approach*", International Journal of Network Management, Wiley, 17(1): 85-97.
3. Saleh, M.S., Alrabiah, A., and Bakry, S.H., (2007). "*A STOPE model for the investigation of compliance with ISO 17799-2005*", Information Management & Computer Security, Emerald, 15(4): 283-294.
4. Saleh, M. S., Bakry, S. H., "*An overview of key information technology risk management methods*", Journal of Applied Computing & Informatics, 6(2): 61-70.