

การพัฒนาระบบบริหารการจัดการความปลอดภัยของข้อมูลสารสนเทศ  
โดยวิธี BS 7799-2: 2002 และ ISO/IEC 17799: 2000 สำหรับศูนย์คอมพิวเตอร์ทางวิศวกรรม

นายคง เหงียน ลี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาการจัดการทางวิศวกรรม ศูนย์ระดับภูมิภาคทางวิศวกรรมระบบการผลิต

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2546

ISBN 974-17-4362-9

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

**DEVELOPING AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)  
BASED ON BS 7799-2: 2002 & ISO 17799: 2000  
FOR ENGINEERING COMPUTER CENTER (ECC)**



**Mr. Khuong Le Nguyen**

**A Thesis Submitted in a Partial Fulfillment of the Requirements  
for the Degree of Master of Engineering in Engineering Management  
The Regional Center for Manufacturing System Engineering**

**Chulalongkorn University**

**Academic Year 2003**

**ISBN: 974 – 17 – 4362 – 9**

**Copyright of Chulalongkorn University**

14 ก.พ. 2550

I21601719

Thesis Title            Developing Information Security Management System (ISMS) based on BS  
7799-2: 2002 & ISO/IEC 17799: 2000 for Engineering Computer Center

By                            Khuong Le Nguyen


Field of study            Engineering Management

Advisor                    Assoc. Prof. Damrong Thawesaengkulthai


Co-Advisor                Thongchai Rojkangsadan

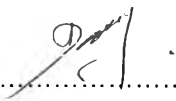
---

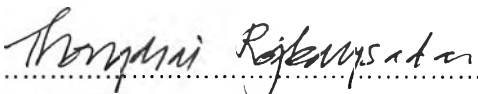
Accepted by the Faculty of Engineering, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree.

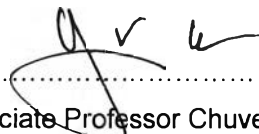
  
.....Dean of the Faculty of Engineering  
(Professor Somsak Panyakeow, D.Eng.)

Thesis Committee

  
.....Chairman  
(Professor Sirichan Thongprasert, Ph.D)

  
.....Thesis Advisor  
(Associate Professor Damrong Thawesaengkulthai, Ph.D)

  
..... Thesis Co-Advisor  
(Thongchai Rojkangsadan, M.Eng)

  
.....Member  
(Associate Professor Chuvej Chansangavej, Ph.D)

KHUONG LE NGUYEN : การพัฒนาระบบบริหารการจัดการความปลอดภัยของข้อมูลสารสนเทศโดยวิธี BS 7799-2: 2002 และ ISO/IEC 17799: 2000 สำหรับศูนย์คอมพิวเตอร์ทางวิศวกรรม. (Developing Information Security Management System Based on BS 7799-2: 2002 & ISO/IEC 17799: 2000 for Engineering Computer Center) อ. ที่ปรึกษา: รองศาสตราจารย์ ดำรงค์ ทวีแสงสกุลไทย, อ.ที่ปรึกษาร่วม : อาจารย์ ธงชัย ไรจน์กั้งสดาล 302 หน้า. ISBN .

นับเป็นเวลามากกว่า 1 ทศวรรษ ที่โมเดลของระบบบริหารจัดการคุณภาพ (Quality Management System: QMS) ได้พิสูจน์ถึงประสิทธิผลในการปรับปรุงคุณภาพของการบริการและสินค้าขององค์กรธุรกิจทั่วโลก ในอีกมุมมองหนึ่งขององค์ความรู้ทางเศรษฐกิจ การเจริญเติบโตหรือการอยู่รอดขององค์กรนั้นไม่ได้ขึ้นอยู่กับประกันคุณภาพเพียงอย่างเดียว แต่ยังขึ้นอยู่กับการรักษาความปลอดภัยของสารสนเทศนั้นๆ อีกด้วย ซึ่งเมื่อทำการจัดลำดับความสำคัญของทรัพยากรในองค์กรแล้ว จะพบว่า ทรัพยากรบุคคลนั้นมาเป็นอันดับแรก ตามด้วยสินทรัพย์ และอีกสิ่งหนึ่งที่มีความสำคัญมากที่สุด ก็คือ สารสนเทศ ซึ่งเปรียบเสมือนเส้นเลือดหลักขององค์กรแต่ละองค์กร นอกจากนั้นได้มีเหตุการณ์ที่ระบบในการรักษาความปลอดภัยของสารสนเทศล้มเหลว ส่งผลให้เกิดความเสียหายอย่างรุนแรงในการดำเนินธุรกิจ ในปัจจุบัน ระบบ BS 7799-2: 2002 & ISO/IEC 17799: 2000 นับเป็นระบบบริหารการจัดการความปลอดภัยของข้อมูลสารสนเทศที่เหมาะสม และเอื้อต่อระบบบริหารจัดการมากที่สุด ซึ่งระบบ ISMS ที่มีประสิทธิภาพได้ช่วยรักษาความปลอดภัยของสารสนเทศในองค์กร รวมถึงการรักษาเสถียรภาพของธุรกรรมทั้งภายใน และภายนอก และความเชื่อถือของผู้บริโภคได้เป็นอย่างดี

การประยุกต์เอาระบบ BS 7799-2: 2002 & ISO/IEC 17799: 2000 มาใช้ในประเทศไทย เหมือนอย่างที่ได้มีการประยุกต์ใช้ในหลายประเทศ เป็นเทคนิคที่ค่อนข้างใหม่ เนื่องจากข้อเท็จจริง 2 ประการ ได้แก่ 1) นโยบายในการรักษาความปลอดภัยของสารสนเทศของผู้บริหารระดับสูงภายในประเทศยังไม่ชัดเจน 2) ความเข้าใจผิดในการนำระบบบริหารจัดการแบบใหม่มาใช้ว่าจะมีความซับซ้อน เสียเวลา และงบประมาณเป็นจำนวนมาก สิ่งต่างๆ เหล่านี้จึงเป็นแรงผลักดันให้ทำการศึกษา ISMS โดยวิธี BS 7799-2: 2002 และ ISO/IEC 17799: 2000 ในการศึกษาถึงคุณลักษณะต่างๆ ของระบบ ISMS และพัฒนารูปแบบทางทฤษฎี โดยนำมาประยุกต์ใช้กับการดำเนินงานของศูนย์คอมพิวเตอร์ทางวิศวกรรม คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

การวิจัยนี้ให้ผลการดำเนินการเป็น 2 ลักษณะ ได้แก่ วิธี OCTAVE<sup>SM</sup> ซึ่งเป็นการประเมินความเสี่ยงของระบบการรักษาความปลอดภัยของสารสนเทศที่มีประสิทธิภาพมากที่สุด ในการนำมาประเมินความเสี่ยงที่จะเกิดขึ้นจากการดำเนินงานของ ECC และผลสรุปการประเมินข้างต้นด้วยระบบ ISMS โดยวิธี BS 7799-2: 2002 และ ISO/IEC 17799: 2000

ภาควิชา ....RCMSE.....ลายมือชื่อผู้รับผิดชอบ.....  
สาขาวิชา ...การบริหารจัดการทางวิศวกรรม...ลายมือชื่ออาจารย์ที่ปรึกษา.....  
ปีการศึกษา...2547.....ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....

##4570699821: MAJOR ENGINEERING MANAGEMENT

KEYWORDS: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)/ BS 7799-2: 2002/ ISO 17799: 2000/ INFORMATION SECURITY RISK ASSESSMENT/ OCTAVE<sup>SM</sup> METHOD.

KHUONG LE NGUYEN: DEVELOPING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) BASED ON BS 7799-2: 2002 & ISO/IEC 17799: 2000 FOR ENGINEERING COMPUTER CENTER. THESIS ADVISOR: ASSOCIATE PROFESSOR DAMRONG THAWESAENGSKULTHAI. THESIS CO- ADVISOR: LECTURER THONGCHAI ROJKANGSADAN. PP. 302.

The model of Quality Management System (QMS), for over a decade, has proven its effectiveness of enhancing the quality of service and product of worldwide enterprises. Yet, in this knowledge economy, the growth or survival of the organization is not only limited to ensuring the quality but also extended to protecting information. Indeed, if we wish to rank the assets, next to personnel – the most valuable one – is unarguably the information, which is considered the lifeblood of each organization. Numerous information security breaches and incidents as well as their associated consequences overwhelm mass media, heavily striking the enterprises' operation. Given that context, the timely release of BS 7799-2: 2002 and ISO 17799: 2000 – an Information Security Management System (ISMS) – is an appropriate, crucial supplementation for existing management systems. An efficient ISMS maintains the organization's information security posture, thereby keeping the stability of internal and external business activities and most significantly, the customers' credit.

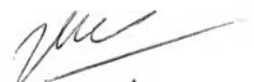
Implementation of BS 7799 and ISO 17799 in Thailand as well as in many other countries is quite fresh. This fact claims for two reasons. First, senior management's awareness of information security is fairly low. More and equally important is the thought that understanding and deploying a new management system would be complicated, time-consuming and costly. These drove me to study the ISMS based on BS 7799 and ISO 17799 to know which are the characteristics and contents of an ISMS and then develop a theoretical model based on a specific case study of the Engineering Computer Center (ECC) of the Faculty of Engineering, Chulalongkorn University.

This study aims at producing two results. First, the OCTAVE<sup>SM</sup> method – the most effective and yet unknown information security risk assessment will be intensively explored in order to conduct a complete risk assessment on the operation of ECC. Next, according to such evaluation results, an ISMS will be fully established by using the BS 7799-2: 2002 and ISO 17799: 2000.

Lastly, in near future, exploring this ISMS and the like would enable Thai authorities to establish their own standards like the ones generated by India, Japan, Germany, Australia and New Zealand.

Department: The Regional Center for Manufacturing  
System Engineering (RCMSE)  
Field of Study: Engineering Management  
Academic year: 2003

Student's signature:



Advisor's signature:



Co-Advisor's signature:



## ACKNOWLEDGEMENTS

My special thanks go to lecturer Thongchai, who directed me to one of the hottest fields of IT - information security, which inspires me much throughout this thesis work. Hardly can I have such a wonderful opportunity to discover the OCTAVE<sup>SM</sup> – the most effective and yet unknown information security risk assessment method – without his recommendation to access to CERT's website and especially his department's financial support to buy expensive documents regarding the OCTAVE<sup>SM</sup> method.

I wish to extend my deepest gratitude to Associate Professor Damrong for his precious advice during writing this tough thesis work. Indeed, it is such a great enthusiasm and kindness of him that remarkably enables me to obtain the BS 7799-2: 2002 and ISO 17799: 2000 documents, which are still extremely scarce in Thailand, and most importantly to raise a passion for doing research in me.

My best wishes go to the "HUT-TODAI" program – a long term educational project co-operated between Hochiminh city University of Technology (HCMUT - Vietnam) and the University of Tokyo (TOU – Japan) where I was given a chance to pursue this dual-master degree to enhance my knowledge.

I am very grateful to the Engineering Computer Center (ECC), International School of Engineering (ISE), Mrs. Potchanaporn from Logic Company, Mr. Eralp Gullep PricewaterhouseCoopers Thailand (PwC), Dr. Komain from ThaiCERT, Dr. Thaweesak from NECTEC, Mr. Karnjana from Bangkok Post - Database for giving me important documents and advices.

My family and Thanh Truc was a huge motivation for me in this thesis work.

I am pleased to thank the committee members: Professor Sirichan and Associate Professor Chuvej for their important comments to improve the quality of this thesis work.

Lastly, I really appreciate the warm support of friends – Christ, Mr. Quoc Huy, Mr. Trung, Mr. Tien, Mr. Tan and especially Anchukorn Jaronsiri.

## CONTENTS

	PAGE
THAI ABSTRACT.....	iv
ENGLISH ABSTRACT.....	v
ACKNOWLEDGEMENT.....	vi
CONTENTS.....	vii
LIST OF TABLES.....	xi
LIST OF FIGURES.....	xii
ABBREVIATIONS.....	xiii
<b>CHAPTER 1 INTRODUCTION</b>	<b>1</b>
1. BACKGROUND OF THE STUDY.....	1
2. RATIONALE OF THE STUDY.....	4
3. THESIS OBJECTIVE & RESEARCH QUESTIONS.....	8
4. SCOPE.....	9
5. METHODOLOGY.....	10
6. EXPECTED RESULTS.....	10
7. AN OUTLINE OF THIS THESIS WORK.....	11
<b>CHAPTER 2 INFORMATION SECURITY RISK ASSESSMENT</b>	<b>13</b>
1. RISK, INFORMATION & INFORMATION SECURITY REQUIREMENTS.....	14
2. INFORMATION SECURITY RISK ASSESSMENT.....	23
2.1 The Importance of Information Security Risk Assessment.....	23
2.2 Strategies for Information Security Risk.....	24
3. CURRENT INFORMATION SECURITY RISK ASSESSMENT APPROACHES..	25
3.1 Quantitative Risk Assessment Methodology.....	25
3.2 Qualitative Risk Assessment Methodology.....	26
4. THE OCTAVE <sup>SM</sup> APPROACH.....	30
4.1 Rationale for Selection of This Method.....	31
4.2 The Octave <sup>SM</sup> Methodology.....	34
4.2.1 The Octave <sup>SM</sup> Structure.....	34
4.2.2 The Octave <sup>SM</sup> Principles & Attributes.....	38
4.2.3 The Outputs of Octave <sup>SM</sup> .....	49
4.2.4 Preparation for Octave <sup>SM</sup> .....	49
5. COMPUTER ASSISSTED-RISK-ASSESSMENT SOFTWARE TOOLS (CARS)	51
6. CONCLUSION.....	53

<b>CHAPTER 3 INFORMATION SECURITY MANAGEMENT SYSTEM</b>	<b>54</b>
1. INTRODUCTION TO INFORMATION SECURITY MANAGEMENT SYSTEM.....	55
2. A GLANCE AT HISTORY OF ISMS.....	56
3. SOME PRACTICAL APPROACHES TO MODERN ISMSs.....	56
3.1 The CERT/CC Model.....	56
3.2 The PricewaterhouseCoopers Model (PWCs Thailand).....	61
3.3 The EWEEK Model.....	64
4. AN INSIGHT INTO ISO/IEC 17799:2000 & BS 7799-2:2002.....	68
4.1 What is ISO/IEC 17799:2000 & BS 7799-2:2002.....	68
4.2 A Condensed History.....	71
4.3 Why to develop an ISMS based on ISO 17799:2000 & BS 7799 2:2002.....	72
4.4 An insight into BS 7799-2:2002 – The structure of ISMS.....	73
4.5 Benefits of ISMS Based on BS 7799/ISO 17799.....	80
5. CONCLUSION.....	81
<b>CHAPTER 4 ISMS - A CASE STUDY OF ECC</b>	<b>82</b>
1. ECC PROFILE.....	83
1.1 An Overview.....	83
1.2 Organizational structure.....	83
1.3 Computing infrastructure.....	84
2. CONDUCTING RISK ASSESSMENT – RESULTS.....	85
2.1 Preparation.....	85
2.2 Start of Phase 1 – Process 1 to 3.....	87
2.3 Process 4 – End of Phase 1.....	92
2.4 Phase 2 – Process 5 to 6.....	100
2.5 Phase 3 – Process 7 to 8.....	102
3. ESTABLISHING ISMS BASED ON BS 7799 & ISO 17799.....	107
3.1 Corporate Information Security Policy.....	107
3.2 Scope of the ISMS.....	110
3.3 Risk Analysis.....	111
3.4 Risk Management.....	112
3.5 Selection of Controls.....	113
3.6 Statement of Applicability.....	131
4. THE DO-CHECK-ACT PHASES.....	132
5. CONCLUSION.....	133



<b>CHAPTER 5 SUMMARY &amp; CONCLUSION</b>	134
1. ANSWERS TO RESEARCH QUESTIONS.....	134
2. LESSONS LEARNED FROM THE STUDY.....	158
2.1 Some Evaluations on Information Security Risk Assessment.....	158
2.2 Some Evaluations on ISMS Based on BS & ISO Standards.....	162
3. SOME COMMENTS AFTER STUDY.....	163
4. SUGGESTION FOR FUTURE STUDY.....	163
5. FINAL CONCLUSION.....	164
<b>REFERENCES</b> .....	165
<b>BIBLIOGRAPHY</b> .....	168
<b>APPENDICES</b>	
<b>APPENDIX A</b>	
A-0 Catalog of Practices.....	169
A-1 Identified Information Assets.....	186
A-2 Identified Areas of Concerns.....	188
A-3 Identified Security Requirements.....	190
A-4 Survey on Security Practices.....	193
A-5 Consolidated Data on Security Practices.....	211
A-6 Mapping Identified Areas of Concerns into Threat Profiles.....	231
A-7 Identified Infrastructure Components.....	245
A-8 Identified Impacts on the Organization.....	246
A-9 Evaluation Criteria.....	256
<b>APPENDIX B</b>	
B-1 Clause 1 - 4.....	257
B-2 Clause 5 - 11.....	260
B-3 Clause 12.....	263
B-4 Clause 13 - 14.....	264
B-5 Clause 15 - 16.....	266
B-6 Clause 17 - 18.....	267
B-7 Clause 19.....	268
B-8 Clause 20 - 21.....	269
B-9 Clause 22 - 23.....	270
B-10 Clause 24 - 27.....	273
B-11 Clause 28 - 29.....	275
B-12 Clause 30 - 34.....	276

**APPENDIX C**

C-1	Users' data - Risk Profile for Human Actors Using Network Access.....	280
C-2	Users' data - Risk Profile for System Problems.....	281
C-3	Users' data - Risk Profile for Other Problems.....	282
C-4	Management data - Risk Profile for Human Actors Using Network Access	283
C-5	Management data - Risk Profile for System Problems.....	284
C-6	UIPS - Risk Profile for Human actors using network access.....	285
C-7	UIPS - Risk Profile for System Problem.....	286
C-8	UIPS - Risk Profile for Other Problems.....	287
C-9	NCs - Risk Profile for Human actors using network access.....	288
C-10	NCs - Risk Profile for Human actors using physical access.....	289
C-11	NCs - Risk Profile for System Problems.....	290
C-12	NCs - Risk Profile for Other Problems.....	291
C-13	PCs - Risk Profile for Human Actors Using Physical Access.....	292
C-14	PCs - Risk Profile for System Problems.....	293
C-15	PCs - Risk Profile for Other Problems.....	294
C-16	Technical team - Risk Profile for Other Problems.....	295

<b>APPENDIX D: GLOSSARY.....</b>	<b>296</b>
----------------------------------	------------

<b>BIOGRAPHY.....</b>	<b>302</b>
-----------------------	------------

## LIST OF TABLES

TABLE 2-1	Mapping OCTAVE <sup>SM</sup> Principles to Attributes.....	45
TABLE 2-2	CARS products.....	54
TABLE 3-1	PDCA adopted for ISMS.....	76
TABLE 4-1	Analysis team members.....	90
TABLE 4-2	Participants in each process.....	91
TABLE 4-3	Processes 1 to 3 activities.....	92
TABLE 4-4	Critical information assets at the center.....	93
TABLE 4-5	Threat Types.....	98
TABLE 4-6	Ratings of Likelihood.....	108
TABLE 4-7	Expected Value Matrix.....	109
TABLE 4-8	Control Risk 1 – Human actors use network to access users’ data.....	118
TABLE 4-9	Control Risk 2 – System problems to threaten users’ data.....	118
TABLE 4-10	Control Risk 3 – Other problems to threaten users’ data.....	120
TABLE 4-11	Control Risk 4 – Human actors use network to access management data.....	121
TABLE 4-12	Control Risk 5 – System problems to threaten management data.....	122
TABLE 4-13	Control Risk 6 – Human actors use network to access UIPS.....	123
TABLE 4-14	Control Risk 7 – System problems to threaten UIPS.....	124
TABLE 4-15	Control Risk 8 – Other problems to threaten UIPS.....	125
TABLE 4-16	Control Risk 9 – Human actors use network to access NCs.....	126
TABLE 4-17	Control Risk 10 – Human actors physically access to NCs.....	127
TABLE 4-18	Control Risk 11 – System problems to threaten NCs.....	128
TABLE 4-19	Control Risk 12 – Other problems to threaten NCs.....	130
TABLE 4-20	Control Risk 13 – Human actors physically access to PCs.....	131
TABLE 4-21	Control Risk 14 – System problems to threaten PCs.....	132
TABLE 4-22	Control Risk 15 – Other problems to threaten PCs.....	133
TABLE 4-23	Control Risk 16 – Other problems to technical team.....	134
TABLE 4-24	Additional Controls.....	135

## LIST OF FIGURES

FIGURE 1-1	The number of incidents from 2000 to present (North America).....	3
FIGURE 1-2	The number of incidents in Thailand from 2000 to present.....	7
FIGURE 2-1	Threat – Vulnerability – Consequences – Control.....	18
FIGURE 2-2	Relationship among Confidentiality, Integrity and Availability.....	21
FIGURE 2-3	Information Security Requirements for Information Assets in Organization	24
FIGURE 2-4	The OCTAVE <sup>SM</sup> Approach.....	32
FIGURE 2-5	OCTAVE <sup>SM</sup> balances operational risk, security practices, and technology	34
FIGURE 2-6	The 3 phases and contents of OCTAVE <sup>SM</sup> Approach.....	38
FIGURE 2-7	Phase 2: Identify Technological Vulnerabilities.....	39
FIGURE 2-8	Phase 3: Conduct Risk Analysis.....	39
FIGURE 2-9	Information Security Risk Management Principles.....	40
FIGURE 2-10	OCTAVE <sup>SM</sup> Outputs.....	51
FIGURE 3-1	Information Security Risk Evaluation.....	60
FIGURE 3-2	Operations & Tasks of the Information Security Management Framework	61
FIGURE 3-3	Information Security Management Framework.....	65
FIGURE 3-4	5-STEPS TO ENTERPRISE SECURITY - Security Step 1: Assessment	67
FIGURE 3-5	5-STEPS TO ENTERPRISE SECURITY - Security Step 2: Prevention	68
FIGURE 3-6	5-STEPS TO ENTERPRISE SECURITY - Security Step 3: Detection	69
FIGURE 3-7	5-STEPS TO ENTERPRISE SECURITY - Security Step 4: Response	69
FIGURE 3-8	5-STEPS TO ENTERPRISE SECURITY - Security Step 5: Vigilance	70
FIGURE 3-9	PCDA Model suggested by BS 7799-2: 2002.....	77
FIGURE 3-10	Steps in developing ISMS suggested by BS 7799-2: 2002.....	82
FIGURE 4-1	ECC's Organizational Structure.....	88
FIGURE 4-2	ECC's computing infrastructure.....	88
FIGURE 4-3	Participants identify threat sources and outcomes.....	94
FIGURE 4-4	Asset-Based Threat Tree for Human Actors Using Network Access.....	99
FIGURE 4-5	Asset-Based Threat Tree for Human Actors Using Physical Access.....	100
FIGURE 4-6	Asset-Based Threat Tree for System Problems.....	101
FIGURE 4-7	Asset-Based Threat Tree for Other Problems.....	102

## ABBREVIATIONS

- CERT/CC – Computer Emergency Respond Team/Coordination Center
- ECC – Engineering Computer Center
- BSI – British Standard Institute
- BS 7799-2:2002: Information security management: Specifications with guidance for use
- DoS – Denial of Service
- ISMS – Information Security Management System
- ISO – International Standard Organization
- ISO 17799:2000 – Information Technology: Code of Practice for information security management, 1<sup>st</sup> edition
- IT – Information Technology
- OCTAVE<sup>SM</sup> – Operationally Critical Threat, Asset, and Vulnerability Evaluation
- NECTEC – National Electronics Computer Technology Engineering Center
- TCSEC – Technical Criteria of Security
- CUNET – Chulalongkorn Network
- Mtg – Mitigation
- Accpt – Acceptance