

ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

การพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

The Development of Information Security Risk Analysis System

โดย

นายกษพงศ์ เพ็ชรราช

รหัส 45061522



\*H002225\*

อาจารย์ที่ปรึกษา

ผศ.ดร. โชติพัทธ์ ภรณ์วลัย

วัน เดือน ปี.....	0 8 ก.พ. 2550
เลขทะเบียน.....	02225
เลขเรียกหนังสือ.....	อศ. ก 112 ก 2547
"ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล."	

b.11699048

i.12871971

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน  
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2547

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อหัวข้อ	การพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศ
นักศึกษา	นายกชพงศ์ เพ็ชรราช
อาจารย์ที่ปรึกษา	ผศ.ดร. โชติพัทธ์ ภรณ์วลัย
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2547

## บทคัดย่อ

ปัจจุบันความปลอดภัยของสารสนเทศมีความสำคัญต่อการดำเนินงานของบริษัทและองค์กรต่างๆ ดังนั้น การวิเคราะห์และประเมินความเสี่ยงจึงเป็นสิ่งที่ทุกบริษัทหรือองค์กรต่างๆ จำเป็นต้องมี เพื่อค้นหาจุดอ่อนและปัจจัยที่ทำให้เกิดความเสี่ยง แล้วจัดการดำเนินการจัดการเพื่อทำให้ความเสี่ยงเหล่านั้นลดลง แต่ขั้นตอนในการวิเคราะห์ความเสี่ยงมีความซับซ้อนและต้องใช้เวลาค่อนข้างมาก เนื่องจากต้องอาศัยข้อมูลจากบุคคลที่เกี่ยวข้องมากมายและต้องมีการติดต่อสื่อสารกันระหว่างทีมนักวิเคราะห์ ซึ่งการวิเคราะห์ความเสี่ยงในปัจจุบันส่วนใหญ่ต้องพึ่งทีมนักวิเคราะห์เป็นหลักและยังขาดเครื่องมือหรือระบบในการช่วยวิเคราะห์ความเสี่ยง จึงควรมีการพัฒนาระบบวิเคราะห์ความเสี่ยงขึ้นมาเพื่อช่วยให้การวิเคราะห์ความเสี่ยงมีความสะดวกและรวดเร็วยิ่งขึ้น โครงการนี้เป็นการพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศโดยนำแนวคิดของ Cobit มาประยุกต์ใช้ในการออกแบบและพัฒนาระบบ โดยหลักการทำงานของระบบจะเกี่ยวข้องกับการวิเคราะห์ความเสี่ยงของทรัพย์สิน ภัยคุกคามและผลกระทบในองค์กร รวมถึงการวิเคราะห์การควบคุมและจัดการความเสี่ยงที่ได้ทำไปแล้ว

<b>Title</b>	The Development of Information Security Risk Analysis System
<b>Student</b>	Mr. Kochapong Petcharaj
<b>Advisor</b>	Asst.Prof.Dr. Chotipat Pornavalai
<b>Level of Study</b>	Master of Science in Information Technology
<b>Major</b>	Information Science
<b>Academic Year</b>	2004

### Abstract

Recently, Security policy has important to operation of organizations and company. Thus, risk analysis and evaluation are essential to all organizations. It used to identify vulnerabilities and develop security strategy to mitigate them. But process in risk analysis is complex and use a longtime because it need information from many people and communication between analyst team. Today, Most risk analysis depend on analyst team and lack of analysis tool. Thus, the development of risk analysis system for help to improve speed and facility should be done. This project, The Development of Information Security Risk Analysis System, use CobiT approach to design and implement. Principle of work is analyze asset, threat and impact in organization. Including analyze about risk control that have been implement.

# สารบัญ

## หน้า

บทคัดย่อภาษาไทย.....	II
บทคัดย่อภาษาอังกฤษ.....	II
สารบัญ.....	II
สารบัญรูป.....	V
สารบัญตาราง.....	IX
บทที่	
1. บทนำ.....	1
1.1 วัตถุประสงค์ของการพัฒนาระบบ.....	1
1.2 วิธีการในการพัฒนาระบบ.....	1
2. แนวคิดการวิเคราะห์ความเสี่ยงของสารสนเทศ.....	3
2.1 การวิเคราะห์ความเสี่ยงของสารสนเทศ.....	3
2.2 การวิเคราะห์ความเสี่ยงของสารสนเทศโดยใช้แนวคิด OCTAVE.....	5
2.3 การวิเคราะห์ความเสี่ยงของสารสนเทศโดยใช้แนวคิด CobIT.....	15
3. การวิเคราะห์และออกแบบระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	20
3.1 ลักษณะและขอบเขตของระบบ.....	20
3.2 การวิเคราะห์และออกแบบระบบ.....	24
4. การใช้งานระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	60
4.1 การเข้าสู่ระบบ.....	60
4.2 การเปลี่ยนรหัสผ่าน.....	61
4.3 การวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กร.....	62
4.4 การจัดการคำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง.....	79
4.5 การจัดการผู้ใช้ระบบ.....	82
5. การพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	85
5.1 รูปแบบการพัฒนาระบบ.....	85

## สารบัญ (ต่อ)

	หน้า
5.2 โครงสร้างฐานข้อมูล .....	88
6. สรุป.....	95
บรรณานุกรม.....	96
ประวัติผู้เขียน.....	97



# สารบัญรูป

หน้า

## รูปที่

2.1 ความสัมพันธ์ระหว่างการประเมินความเสี่ยงและการจัดการความเสี่ยง .....	4
2.2 วิธีการของ OCTAVE .....	5
2.3 ขั้นตอนที่ 1 สร้างโครงสร้างของภัยคุกคามต่อทรัพย์สิน .....	6
2.4 โครงสร้างภัยคุกคามการเข้าถึงทรัพย์สินผ่านเครือข่าย .....	8
2.5 ขั้นตอนที่ 2 ระบุจุดอ่อนของโครงสร้างพื้นฐาน.....	8
2.6 ความสัมพันธ์ระหว่างโครงสร้างของภัยคุกคามและส่วนประกอบของโครงสร้างพื้นฐาน.....	9
2.7 ขั้นตอนที่ 3 พัฒนากลยุทธ์และแผนการเกี่ยวกับความปลอดภัย.....	11
2.8 โครงสร้างภัยคุกคามการเข้าถึงทรัพย์สินผ่านเครือข่าย .....	13
2.9 กระบวนการทางเทคโนโลยีสารสนเทศของ CobiT ถูกกำหนดไว้ภายใต้ 4 โดเมน .....	16
2.10 โครงสร้างการดำเนินงานของธุรกิจและเทคโนโลยีสารสนเทศ.....	18
2.11 สรุป Control Objectives ของ CobiT .....	19
3.1 Activity Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	21
3.2 Use Case Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	23
3.3 Sequence Diagram : Logon to System .....	26
3.4 Activity Diagram : Logon to System.....	27
3.5 Sequence Diagram : Change Password .....	28
3.6 Activity Diagram : Change Password .....	29
3.7 Sequence Diagram : Display Risk Analysis Result.....	30
3.8 Activity Diagram : Display Risk Analysis Result.....	31
3.9 Sequence Diagram : Manage Project.....	32
3.10 Activity Diagram : Manage Project.....	33
3.11 Sequence Diagram : Manage Analyst Team .....	35
3.12 Activity Diagram : Manage Analyst Team.....	36

## สารบัญรูป (ต่อ)

หน้า

รูปที่

3.13 Sequence Diagram : Analyze Asset.....	38
3.14 Activity Diagram : Analyze Asset.....	39
3.15 Sequence Diagram : Analyze Threat.....	41
3.16 Activity Diagram : Analyze Threat.....	42
3.17 Sequence Diagram : Analyze Impact.....	44
3.18 Activity Diagram : Analyze Impact.....	45
3.19 Sequence Diagram : Analyze Inherent Risk.....	46
3.20 Activity Diagram : Analyze Inherent Risk.....	47
3.21 Sequence Diagram : Analyze Residual Risk.....	48
3.22 Activity Diagram : Analyze Residual Risk.....	49
3.23 Sequence Diagram : Manage Question.....	510
3.24 Activity Diagram : Manage Question.....	52
3.25 Sequence Diagram : Manage User.....	54
3.26 Activity Diagram : Manage User.....	55
3.27 Class Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	57
3.28 ER Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	58
4.1 หน้าจอเข้าสู่ระบบ.....	60
4.2 เข้าสู่ระบบผิดพลาด.....	60
4.3 หน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ.....	61
4.4 หน้าจอเปลี่ยนรหัสผ่าน.....	61
4.5 ข้อความยืนยันรหัสผ่านไม่ถูกต้อง.....	62
4.6 ข้อความเปลี่ยนรหัสผ่านเรียบร้อยแล้ว.....	62
4.7 หน้าจอการจัดการโครงการ.....	63

## สารบัญรูป (ต่อ)

หน้า

รูปที่

4.8 หน้าจอการเพิ่มโครงการใหม่.....	63
4.9 ข้อความยืนยันการลบโครงการ.....	64
4.10 หน้าจอการจัดการทีมนักวิเคราะห์.....	64
4.11 ข้อความเตือนให้ใส่ข้อมูลให้ครบก่อนคลิกปุ่มเพิ่มผู้วิเคราะห์.....	65
4.12 หน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร.....	66
4.13 หน้าจอการเมื่อคลิกปุ่มวิเคราะห์ระดับความสำคัญทรัพย์สิน.....	66
4.14 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญทรัพย์สิน.....	67
4.15 หน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน.....	68
4.16 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์โอกาสที่จะเกิดภัยคุกคาม.....	68
4.17 หน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม.....	69
4.18 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์ผลกระทบจากภัยคุกคาม.....	70
4.19 หน้าจอการช่วยอธิบายความหมายของคำต่างๆที่ใช้.....	70
4.20 ระดับผลกระทบต่อธุรกิจขององค์กร.....	72
4.21 ระดับโอกาสที่จะเกิดภัยคุกคามต่อธุรกิจขององค์กร.....	72
4.22 ตารางกำหนดค่าในการคำนวณหาความเสี่ยง.....	73
4.23 ระดับความเสี่ยงตามลักษณะธุรกิจขององค์กร.....	73
4.24 ตารางความเสี่ยงถาวร.....	74
4.25 หน้าจอรายการโดเมนย่อยของ CobIT.....	74
4.26 หน้าจอการวิเคราะห์การจัดการความเสี่ยง.....	75
4.27 นักวิเคราะห์ตอบคำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง.....	75
4.28 ตารางความเสี่ยงที่เหลืออยู่.....	76
4.29 คำแนะนำในการจัดการความเสี่ยงในโดเมน AI.....	76
4.30 คำแนะนำในการจัดการความเสี่ยงในโดเมน PO.....	77

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## สารบัญญรูป (ต่อ)

หน้า

รูปที่

4.31 ภัยคุกคามที่มีโอกาสเกิดขึ้นมากที่สุด.....	78
4.32 ภัยคุกคามที่ส่งผลกระทบมากที่สุด .....	78
4.33 บทสรุปและคำแนะนำ .....	79
4.34 หน้าจอการจัดการคำถาม .....	80
4.35 หน้าจอรายการคำถามในโดเมนย่อยที่เลือก .....	81
4.36 คำถามและคำตอบต้องการจะแก้ไข .....	81
4.37 ข้อความเตือนเมื่อกรอกคำถามและคำตอบไม่ครบ.....	81
4.38 หน้าจอการจัดการผู้ใช้ระบบ.....	82
4.39 รายละเอียดเกี่ยวกับผู้ใช้ระบบ.....	83
4.40 หน้าจอแสดงสถานะการใช้งานระบบ.....	83

# สารบัญตาราง

หน้า

ตารางที่

2.1 ผลที่ได้จากการทดสอบเบื้องต้น .....	10
2.2 ระดับของจุดบกพร่อง .....	10
2.3 การประเมินความน่าจะเป็นของภัยคุกคามที่จะเกิดขึ้นสำหรับองค์กร .....	12
2.4 เมทริกซ์แสดงค่าระดับความเสี่ยง .....	14
5.1 โครงสร้างของตาราง Analyst .....	88
5.2. โครงสร้างของตาราง Answer .....	89
5.3. โครงสร้างของตาราง Asset .....	90
5.4. โครงสร้างของตาราง Domain .....	91
5.5. โครงสร้างของตาราง Impact .....	91
5.6. โครงสร้างของตาราง Position .....	92
5.7. โครงสร้างของตาราง Question .....	92
5.8. โครงสร้างของตาราง SubDomain .....	93
5.9. โครงสร้างของตาราง Threat .....	93
5.10. โครงสร้างของตาราง Title .....	94
5.11. โครงสร้างของตาราง User .....	94

# บทที่ 1

## บทนำ

### 1.1 วัตถุประสงค์ของการพัฒนาระบบ

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศเป็นระบบที่นำเอาระบบคอมพิวเตอร์เข้ามาช่วยในการวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กร เพื่ออำนวยความสะดวกให้นักวิเคราะห์ความเสี่ยงสามารถวิเคราะห์ความเสี่ยงได้อย่างรวดเร็วและเป็นระบบ วัตถุประสงค์โดยรวมของระบบวิเคราะห์ความเสี่ยงของสารสนเทศมีดังต่อไปนี้

1. เพื่อช่วยวิเคราะห์และประเมินความเสี่ยง ซึ่งผลการวิเคราะห์ความเสี่ยงสามารถนำมาใช้เป็นแนวทางในการแก้ไขความเสี่ยงได้
2. เพื่อช่วยรวบรวมข้อมูลที่จำเป็นในการวิเคราะห์และประเมินความเสี่ยง โดยเป็นลักษณะของการตอบแบบสอบถาม
3. เพื่อช่วยนักวิเคราะห์ความเสี่ยงให้ทำงานได้สะดวกรวดเร็วขึ้น
4. เพื่อช่วยลดขั้นตอนในการวิเคราะห์ความเสี่ยงและใช้เวลาน้อยลง
5. เพื่อแสดงให้นักวิเคราะห์ความเสี่ยงรวมถึงผู้บริหารองค์กร เห็นความเสี่ยงในจุดต่างๆ ขององค์กรได้ชัดเจน โดยแสดงผลการวิเคราะห์ความเสี่ยงในลักษณะตารางและแผนภูมิต่างๆ
6. เพื่อช่วยให้นักวิเคราะห์ความเสี่ยงสามารถดูผลการวิเคราะห์ความเสี่ยงที่เคยทำไปแล้วได้ เพื่อใช้เป็นแนวทางต่อไป
7. เพื่อช่วยให้ผู้ดูแลระบบสามารถ เพิ่ม ลบ แก้ไข ข้อมูลในส่วน of คำถาม ได้อย่างสะดวกรวดเร็ว
8. เพื่อช่วยเก็บข้อมูลของโครงการ ข้อมูลส่วนตัวของนักวิเคราะห์ แบบสอบถาม ผลการวิเคราะห์ความเสี่ยง
9. เพื่อช่วยให้นักวิเคราะห์ความเสี่ยงสามารถพิมพ์รายงานผลการวิเคราะห์ความเสี่ยงได้ เพื่อนำมาใช้ประกอบในการวิเคราะห์ความเสี่ยงต่อไป

### 1.2 วิธีการในการพัฒนาระบบ

โครงการนี้เป็นการพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศโดยมีการศึกษาแนวคิดและวิธีการวิเคราะห์และประเมินความเสี่ยงหลายๆแนวคิดมาใช้เป็นแนวทางในการพัฒนาระบบ เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยแนวคิดต่างๆที่ศึกษาเพื่อนำมาเป็นแนวทางในการพัฒนา ได้แก่ OCTAVE ,CobiT ,FRAP และ BIA ส่วนแนวคิดหลักที่นำมาใช้เป็นมาตรฐานในการพัฒนาระบบ คือ CobiT ซึ่งเป็นแนวคิดและแนวทางการปฏิบัติเพื่อการควบคุมด้านเทคโนโลยีสารสนเทศสำหรับองค์กร โดยโครงสร้างของ CobiT ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศใช้ UML ช่วยในการออกแบบ ซึ่งมีการใช้โมเดลต่างๆมาช่วยอธิบายระบบงานนั้นๆ ทำให้สามารถแสดงภาพรวมของระบบทั้งหมดได้อย่างชัดเจน และช่วยทำให้นักวิเคราะห์ระบบ นักพัฒนาและผู้ใช้ มีมุมมองที่เข้าใจตรงกัน ทำให้การพัฒนา ระบบเป็นไปอย่างรวดเร็ว



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 2

### แนวคิดการวิเคราะห์ความเสี่ยงของสารสนเทศ

#### 2.1 การวิเคราะห์ความเสี่ยงของสารสนเทศ

สารสนเทศหรือทรัพย์สินที่สำคัญขององค์กรควรอยู่ภายใต้การจัดการและระบบรักษาความปลอดภัยที่ดี การทำให้ระบบมีความปลอดภัยสามารถทำได้หลายวิธี ไม่ว่าจะเป็นการหาเครื่องมือต่างๆมาใช้ เช่น ไฟร์วอลล์ ระบบตรวจจับผู้บุกรุก(IDS) ส่วนอีกวิธีหนึ่ง คือ การปรับปรุงระบบคอมพิวเตอร์และเครือข่ายขององค์กร ให้มีการใช้งานในลักษณะที่มีความปลอดภัยมากขึ้น ซึ่งจะขึ้นอยู่กับนโยบายเกี่ยวกับการรักษาความปลอดภัยและการจัดการดำเนินงานในการการลดช่องโหว่และความเสี่ยงให้น้อยลง ความเสี่ยงของสารสนเทศอาจเกิดได้ทั้งจากคนภายในองค์กรหรือบุคคลภายนอก

##### 2.1.1 ความปลอดภัยของสารสนเทศ

ความปลอดภัยของสารสนเทศเป็นมากกว่าการคอนฟิกไฟร์วอลล์ การแก้ไขจุดบกพร่องของระบบหรือโปรแกรมที่ถูกตรวจพบ หรือการตรวจดูว่าเทปที่สำรองข้อมูลยังอยู่ในที่เก็บอย่างครบถ้วน แต่ความปลอดภัยของสารสนเทศจะเป็นการพิจารณาว่าอะไรที่จำเป็นต้องมีการปกป้องทำไมจึงต้องปกป้อง ปกป้องจากอะไรและจะปกป้องสิ่งนั้นอย่างไรตลอดระยะเวลาที่สิ่งนั้นยังคงอยู่

ความปลอดภัยของสารสนเทศต้องทำเป็นระบบและทำอย่างต่อเนื่องไม่มีวันจบ ระบบของเราอาจมีความปลอดภัยที่ดีในวันนี้ อีกเดือนหนึ่งหรืออีกสัปดาห์หนึ่งข้างหน้า ระบบอาจถูกบุกรุกได้ เหตุผลก็คือ ช่องโหว่ของระบบใหม่ๆ เกิดขึ้นแทบทุกวัน สังเกตได้จาก NOS ในตระกูลวินโดวส์ของไมโครซอฟต์นั้น จะมีรายงานช่องโหว่ของระบบทุกเดือน โดยเฉลี่ยเดือนละ 3-5 ช่องโหว่ บางเดือนก็มีถึงกว่า 10 ช่องโหว่ โดยมาจากทั้งตัว Windows 2000 Server เอง ,IIS Web Server ,Microsoft SQL Server หรือแม้กระทั่ง IE 6.0 ตลอดจน Outlook Express เป็นต้น

##### 2.1.2 ความสัมพันธ์ระหว่างการวิเคราะห์และจัดการความเสี่ยงของสารสนเทศ

เราจะรู้ได้อย่างไรว่าระบบคอมพิวเตอร์และเครือข่ายขององค์กรมีความปลอดภัยหรือไม่ หากยังไม่ปลอดภัยจะต้องทำอะไรบ้าง จะต้องใช้ผลิตภัณฑ์ด้านความปลอดภัยอะไร มีขั้นตอนในการดำเนินการอย่างไร ซึ่งไม่มีคำตอบมาตรฐานสำหรับคำถามข้างต้น และไม่มีคำตอบเดียวที่

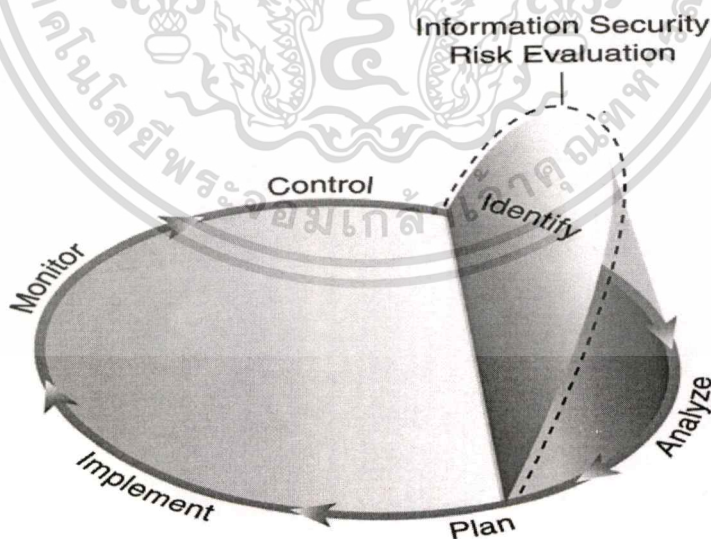
สามารถใช้กับทุกสถานการณ์ได้ แต่เราสามารถประเมินความเสี่ยงและจัดการความเสี่ยงเพื่อให้ระบบมีความเสี่ยงลดลงได้ นั่นคือเพิ่มความปลอดภัยของระบบให้สูงขึ้น

ก่อนที่เราจะสามารถดำเนินการจัดการเพื่อลดความเสี่ยงได้จะต้องมีการประเมินความเสี่ยงก่อน ซึ่งการประเมินความเสี่ยง มีขั้นตอน โดยสรุปคือ

- การระบุสารสนเทศที่มีความเสี่ยง (Identify)
  - การวิเคราะห์ระดับของความเสี่ยง (Analyze)
  - วางแผนเพื่อพัฒนากลยุทธ์ในการป้องกัน (Plan)
- หลังจากการประเมินความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อไปที่ต้องทำมีดังนี้

- วางแผนว่าจะนำกลยุทธ์มาใช้ได้อย่างไร (Plan)
- นำแผนการป้องกันมาใช้ (Implement)
- สังเกตและเฝ้าดูการทำงานและประสิทธิภาพ (Monitor)
- ควบคุมตัวแปรให้เหมาะสมและถูกต้อง (Control)

ขั้นตอนที่กล่าวมาทั้งหมดเป็นการจัดการความเสี่ยง ซึ่งประกอบด้วยขั้นตอนในการประเมินความเสี่ยงร่วมกับขั้นตอนในการนำแผนกลยุทธ์ในการป้องกันมาใช้ นั่นคือ การประเมินความเสี่ยงเป็นส่วนหนึ่งในการจัดการความเสี่ยงนั่นเอง ความสัมพันธ์ระหว่างการประเมินความเสี่ยงและการจัดการความเสี่ยง แสดงในรูปที่ 2.1



รูปที่ 2.1 ความสัมพันธ์ระหว่างการประเมินความเสี่ยงและการจัดการความเสี่ยง

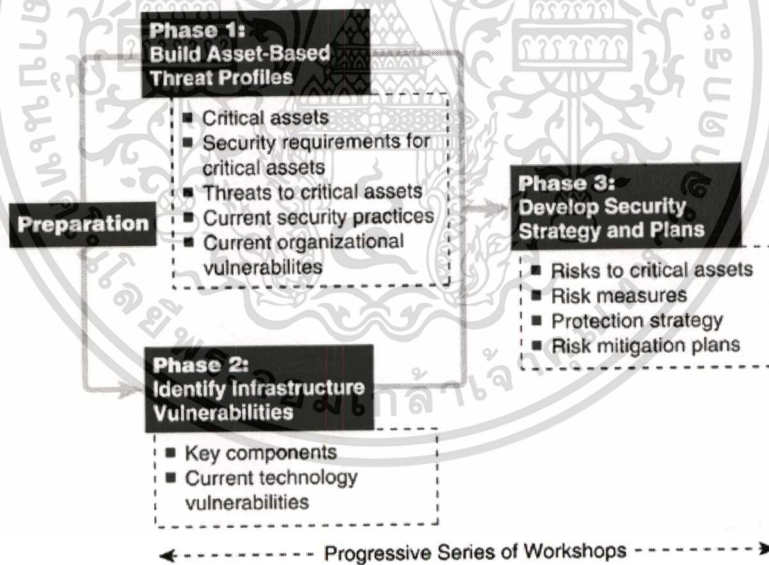
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## 2.2 การวิเคราะห์ความเสี่ยงของสารสนเทศโดยใช้แนวคิด OCTAVE

วิธีการของ OCTAVE มีการแบ่งออกเป็น 3 ขั้นตอน (three-phase) ซึ่งประกอบไปด้วย 8 กระบวนการ ดังนี้

- ขั้นตอนที่ 1 : สร้างโครงร่างของภัยคุกคามต่อทรัพย์สิน ประกอบไปด้วย 4 กระบวนการ คือ กระบวนการที่ 1 ถึง 3 เป็นการสัมภาษณ์พนักงานแต่ละระดับในองค์กร และกระบวนการที่ 4 สร้างโครงร่างของภัยคุกคาม
- ขั้นตอนที่ 2 : ระบุจุดอ่อนของโครงสร้างพื้นฐาน ประกอบไปด้วย 2 กระบวนการ คือ กระบวนการที่ 5 ระบุส่วนประกอบที่สำคัญ และกระบวนการที่ 6 การประเมินส่วนประกอบที่ถูกเลือก
- ขั้นตอนที่ 3 : พัฒนากลยุทธ์และแผนการเกี่ยวกับความปลอดภัย ซึ่งประกอบไปด้วย 2 กระบวนการ คือ กระบวนการที่ 7 การดำเนินการวิเคราะห์ความเสี่ยง และกระบวนการที่ 8 พัฒนากลยุทธ์การป้องกัน

ภาพรวมวิธีการของ OCTAVE แสดงในรูปที่ 2.2

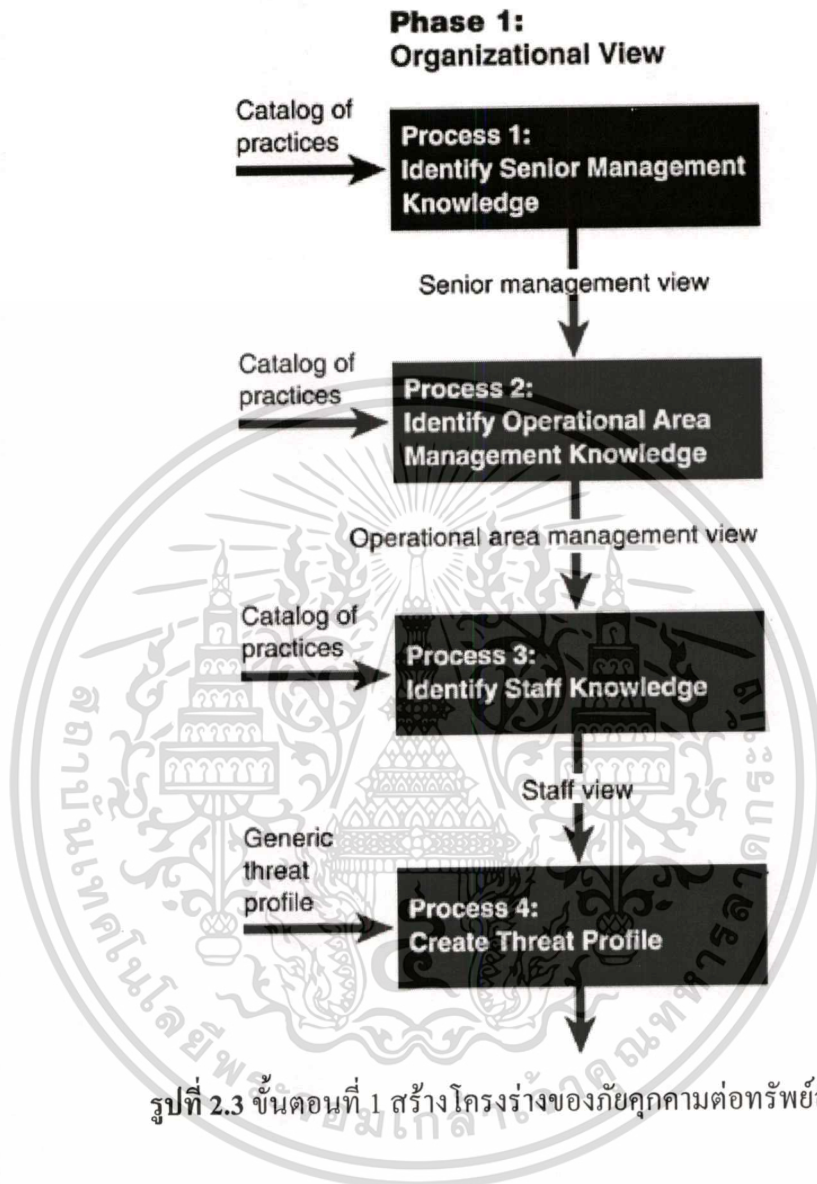


รูปที่ 2.2 วิธีการของ OCTAVE

### 2.2.1 ขั้นตอนที่ 1 : สร้างโครงร่างของภัยคุกคามต่อทรัพย์สิน

ในขั้นตอนที่ 1 เริ่มต้นโดยพิจารณาที่คนในองค์กร เพราะการที่จะเข้าใจได้ว่ามีอะไรเกิดขึ้นบ้างในองค์กรจะต้องถามคนที่ทำงานในองค์กรนั้น โดยจะต้องมีการเก็บรวบรวมข้อมูลของพนักงานในระดับที่แตกต่างกันทั้งจากผู้เชี่ยวชาญด้านธุรกิจและผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ โดยในขั้นตอนที่ 1 ประกอบด้วย 4 กระบวนการ ดังรูปที่ 2.3

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่ออนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



### กระบวนการที่ 1 ถึง 3 (Process 1 to 3)

ทีมนักวิเคราะห์ (Analysis team) จะต้องทำรวบรวมข้อมูลต่างๆ ที่ได้จากการสอบถามพนักงานในองค์กร และนำข้อมูลที่ได้มาวิเคราะห์ว่าทรัพย์สินอะไรที่สำคัญในองค์กรและถูกปกป้องไว้อย่างไร โดยในแต่ละกระบวนการเป็นการสัมภาษณ์พนักงานในแต่ละระดับ ดังนี้

กระบวนการ 1 : ผู้บริหารระดับสูง

กระบวนการ 2 : ผู้บริหารระดับกลาง ผู้จัดการสาขา

กระบวนการ 3 : พนักงานทั่วไป พนักงานสารสนเทศ

กิจกรรมในกระบวนการที่ 1 ถึง 3 มี 4 กิจกรรม ดังนี้

#### ■ ระบุทรัพย์สินและกำหนดระดับความสำคัญ

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ซึ่งการเผยแพร่เพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ระบุขอบเขตของภัยคุกคามที่เกี่ยวข้อง
- ระบุความต้องการความปลอดภัยสำหรับทรัพย์สินที่สำคัญ
- รวบรวมข้อมูลที่ได้จากการสำรวจเกี่ยวกับความปลอดภัยและช่องโหว่ขององค์กร

#### กระบวนการที่ 4 : สร้างโครงสร้างของภัยคุกคาม

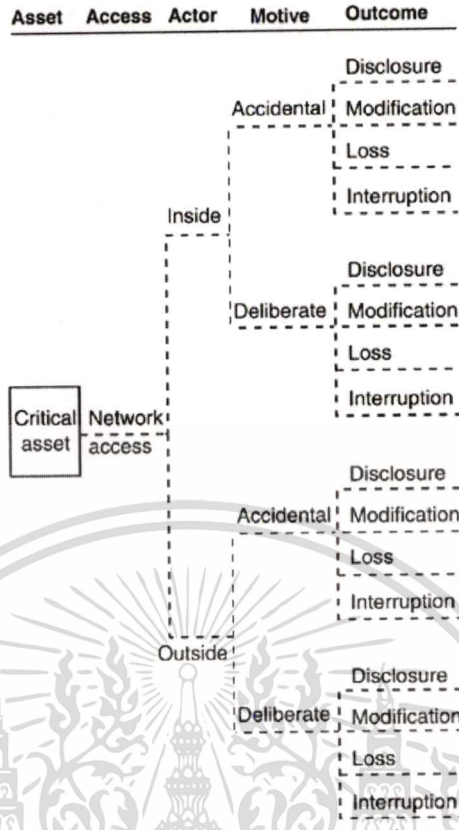
ทีมนักวิเคราะห์ (Analysis team) จะรวบรวมข้อมูลที่ได้จากกระบวนการที่ 1 ถึง 3 มาวิเคราะห์เพื่อหาทรัพย์สินที่สำคัญและมีความเสี่ยง (critical assets) และสร้างโครงสร้างของภัยคุกคาม โดยทีมนักวิเคราะห์ควรมีทักษะและคุณสมบัติต่อไปนี้

- เข้าใจลักษณะและระบบธุรกิจขององค์กร
- เข้าใจเทคโนโลยีสารสนเทศขององค์กร
- มีทักษะในการติดต่อสื่อสาร
- มีทักษะในการวิเคราะห์

โครงสร้างของภัยคุกคามเป็นโครงสร้างที่ใช้แสดงขอบเขตของภัยคุกคามที่มีต่อทรัพย์สินที่สำคัญ โดยจะแสดงในลักษณะโครงสร้างต้นไม้ ซึ่งวิธีการของ OCTAVE ภัยคุกคามจะถูกแสดงในโครงสร้างโดยใช้คุณสมบัติต่อไปนี้

- ทรัพย์สิน (assets) สิ่งใดที่มีค่าต่อองค์กร
- ผู้กระทำ (actor) ใครหรืออะไรก็ตามที่อาจมีการละเมิดความปลอดภัยของทรัพย์สิน
- จุดประสงค์ (motive) ผู้กระทำตั้งใจทำโดยเจตนาหรือเป็นอุบัติเหตุ
- การเข้าถึง (access) ผู้กระทำสามารถเข้าถึงทรัพย์สินได้โดยวิธีใด เช่น ผ่านเครือข่ายหรือทางกายภาพ
- ผลที่ตามมา (outcome) ผลลัพธ์ที่เกิดขึ้นในขณะที่มีการละเมิดความปลอดภัยของทรัพย์สิน

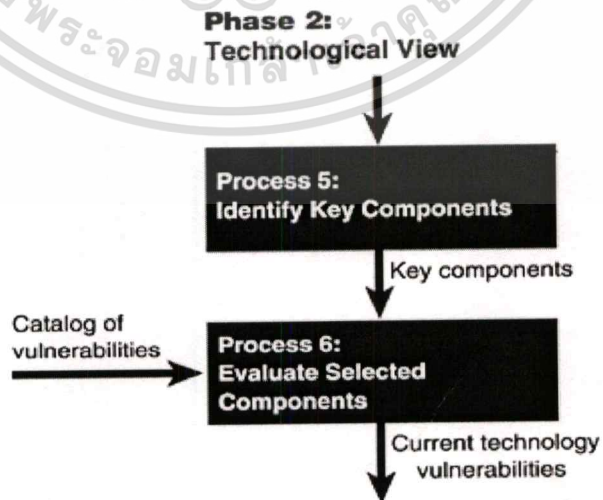
ภัยคุกคามที่เกิดขึ้นมีหลายรูปแบบ เช่น การเข้าถึงทรัพย์สินผ่านเครือข่าย การเข้าถึงทรัพย์สินทางกายภาพ ปัญหาหรือข้อผิดพลาดของระบบทั้งซอฟต์แวร์หรือฮาร์ดแวร์ ภัยธรรมชาติต่างๆ รวมไปถึงอุบัติเหตุที่อาจเกิดขึ้นในองค์กร เป็นต้น จากภัยคุกคามที่ได้กล่าวมา สามารถนำมาสร้างโครงสร้างของภัยคุกคามได้ ดังรูปที่ 2.4



รูปที่ 2.4 โครงร่างภัยคุกคามการเข้าถึงทรัพย์สินผ่านเครือข่าย

### 2.2.2 ขั้นตอนที่ 2 : ระบุจุดอ่อนของโครงสร้างพื้นฐาน

ในขั้นตอนที่ 2 จะเป็นการนำข้อมูลเกี่ยวกับองค์กรที่ได้วิเคราะห์ในขั้นตอนที่ 1 มาพิจารณาเกี่ยวกับเทคโนโลยีและโครงสร้างพื้นฐานขององค์กร เพื่อค้นหาและระบุจุดอ่อนหรือช่องโหว่ที่เกิดขึ้น โดยในขั้นตอนนี้ประกอบด้วย 2 กระบวนการ คือ กระบวนการที่ 5 และ 6 แสดงในรูปที่ 2.5



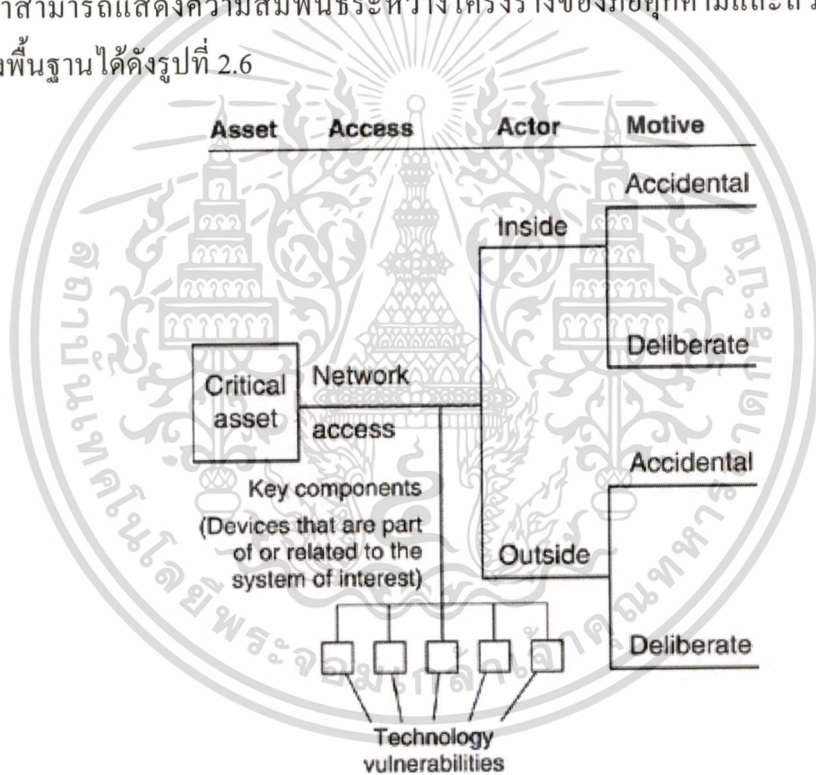
รูปที่ 2.5 ขั้นตอนที่ 2 ระบุจุดอ่อนของโครงสร้างพื้นฐาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

### กระบวนการที่ 5 : ระบุส่วนประกอบที่สำคัญ

ผู้ที่เกี่ยวข้องในกระบวนการนี้คือทีมนักวิเคราะห์และพนักงานเทคโนโลยีสารสนเทศที่ได้เลือกไว้ จุดประสงค์ของกระบวนการที่ 5 คือ เลือกส่วนประกอบของโครงสร้างพื้นฐานเพื่อนำมาทดสอบหาจุดบกพร่องต่อไปในกระบวนการที่ 6

กระบวนการที่ 5 เป็นการนำทรัพย์สินที่สำคัญและภัยคุกคามที่ได้มาจากขั้นตอนที่ 1 มาพิจารณาในส่วนของการเข้าถึงข้อมูลผ่านเครือข่าย ว่าสารสนเทศหรือบริการสามารถถูกเข้าถึงผ่านเครือข่ายขององค์กรได้อย่างไร ซึ่ง โครงร่างของภัยคุกคามของการเข้าถึงผ่านเครือข่ายที่สร้างไว้ในกระบวนการที่ 4 สามารถแสดงขอบเขตของภัยคุกคามของการเข้าถึงผ่านเครือข่ายได้ (รูปที่ 5) จากนั้นเราสามารถแสดงความสัมพันธ์ระหว่างโครงร่างของภัยคุกคามและส่วนประกอบของโครงสร้างพื้นฐานได้ดังรูปที่ 2.6



รูปที่ 2.6 ความสัมพันธ์ระหว่างโครงร่างของภัยคุกคามและส่วนประกอบของโครงสร้างพื้นฐาน

### กระบวนการที่ 6 : การประเมินส่วนประกอบที่ถูกเลือก

ในกระบวนการที่ 6 เป็นการนำส่วนประกอบของโครงสร้างพื้นฐานที่ผ่านการคัดเลือกและพิจารณาจากกระบวนการที่ 5 แล้วมาทำการทดสอบหาจุดบกพร่องโดยในการทดสอบจุดบกพร่องของระบบในแต่ละส่วนประกอบอาจใช้เครื่องมือทดสอบที่ต่างกันตามความเหมาะสมซึ่งทีมนักวิเคราะห์จะเป็นผู้เลือกเครื่องมือและวิธีการทดสอบ ผลที่ได้จากการทดสอบเบื้องต้นแสดงใน

#### ตารางที่ 2.1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## ตารางที่ 2.1 ผลที่ได้จากการทดสอบเบื้องต้น

Component	IP Address	Tool(s)	Vulnerability
Office PCs	-----	Vulnerabilitys-R-Found v 6.73	3 med 20 low
	-----	Vulnerabilitys-R-Found v 6.73	3 med 20 low
	-----	Vulnerabilitys-R-Found v 6.73	3 med 20 low
Firewall	-----	Improve-UR-network v 4.8	1 med 5 low
PIDs server	-----	Improve-UR-network v 4.8	3 high 21 med 43 low
ECDs server	-----	Improve-UR-network v 4.8	9 med 15 low
Router	-----	Improve-UR-network v 4.8	3 low
	-----	Improve-UR-network v 4.8	3 low

จากตารางที่ 2.1 เป็นผลสรุปของการทดสอบเบื้องต้นซึ่งแสดงให้เห็นข้อบกพร่องหรือจุดอ่อนของส่วนประกอบต่างๆ ว่ามีจำนวนเท่าใดและอยู่ในระดับใดบ้าง โดยแต่ละระดับมีความสำคัญและผลกระทบไม่เท่ากัน จากตารางที่ 2.2 มีการกำหนดว่าระดับสูง คือ จุดบกพร่องที่ถูกต้องพบมีความเสี่ยงและผลกระทบสูง ต้องมีการแก้ไขทันที (ภายใน 24 ชั่วโมง) ระดับกลาง ต้องแก้ไขภายใน 1 เดือน และระดับต่ำ อาจทำการแก้ไขในภายหลังได้

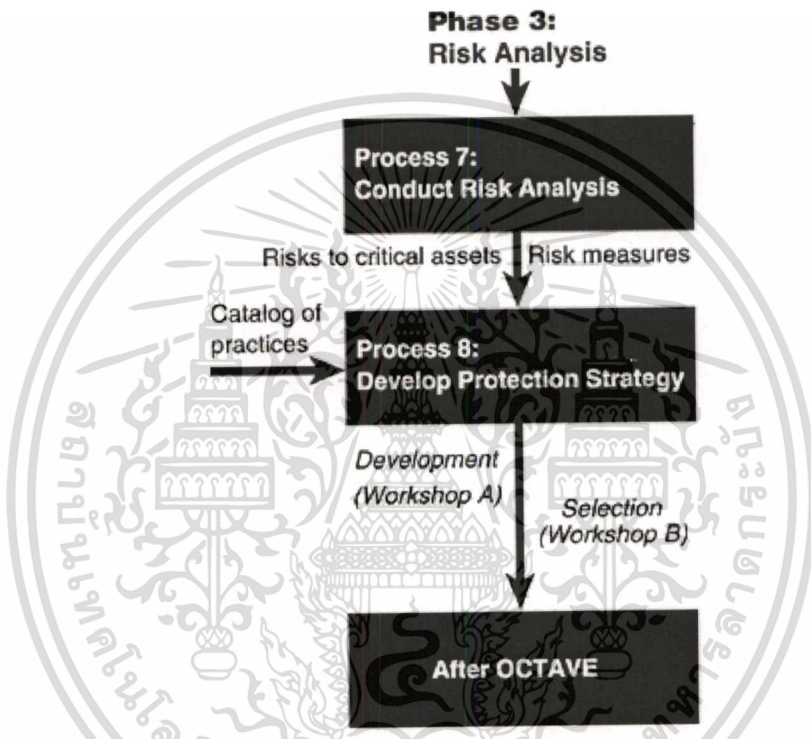
## ตารางที่ 2.2 ระดับของจุดบกพร่อง

Vulnerability Security Level	Definition
High-severity vulnerability	Must be fixed immediately (within the next 24 hours)
Medium-severity vulnerability	Must be fixed soon (1 month)
Low-severity vulnerability	May be fixe later

### 2.2.3 ขั้นตอนที่ 3 : พัฒนากลยุทธ์และแผนการเกี่ยวกับความปลอดภัย

ขั้นตอนที่ 3 เป็นขั้นตอนสุดท้ายของแนวคิด OCTAVE ซึ่งเป็นการนำข้อมูลที่ได้จากการวิเคราะห์และประเมินในขั้นตอนที่ 1 กับขั้นตอนที่ 2 มาใช้ในการพัฒนากลยุทธ์และวางแผนเกี่ยวกับความปลอดภัย โดยในขั้นตอนที่ 3 ประกอบไปด้วย 2 กระบวนการ คือ กระบวนการที่ 7 การดำเนินการวิเคราะห์ความเสี่ยง และกระบวนการที่ 8 พัฒนากลยุทธ์การป้องกัน ซึ่งแบ่งออกเป็น 2 กระบวนการย่อย ได้แก่กระบวนการที่ 8A และกระบวนการที่ 8B

ส่วนแรกในขั้นตอนที่ 3 คือ การดำเนินการวิเคราะห์ความเสี่ยง โดยทำการระบุผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินที่สำคัญ แล้วสร้างมาตรฐานในการประเมินความเสี่ยงขึ้นมา จากนั้นจึงทำการประเมินผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินที่เกิดขึ้น โดยใช้ผลกระทบและความสูญเสียที่เกิดขึ้นจากภัยคุกคามเป็นปัจจัยในการประเมิน ส่วนหลัง คือ นำผลลัพธ์จากการประเมินมาสร้างแผนกลยุทธ์การป้องกันและแผนการลดความเสี่ยง ขั้นตอนที่ 3 แสดงดังรูปที่ 2.7



รูปที่ 2.7 ขั้นตอนที่ 3 พัฒนากลยุทธ์และแผนการเกี่ยวกับความปลอดภัย

**กระบวนการที่ 7 : การดำเนินการวิเคราะห์ความเสี่ยง**

ในกระบวนการที่ 7 เป็นการดำเนินการวิเคราะห์ความเสี่ยงโดยมีวิธีการโดยสรุป คือ เริ่มต้นจากการระบุผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินที่สำคัญ แล้วสร้างมาตรฐานในการประเมินความเสี่ยงขึ้นมา จากนั้นจึงทำการประเมินผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินที่เกิดขึ้น

แนวคิดของ OCTAVE มีการกำหนดระดับของผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินเป็น 3 ระดับ คือ สูง กลาง ต่ำ ซึ่งเป็นการแบ่งอย่างง่าย ๆ แต่ที่นักวิเคราะห์อาจกำหนดระดับของภัยคุกคามที่แตกต่างไปจากนี้ได้ตามความเหมาะสม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การวิเคราะห์ผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินทำให้สามารถบอกได้ว่าภัยคุกคามอะไรมีผลกระทบมากน้อยเท่าใด แต่ภัยคุกคามแต่ละอย่างมีโอกาสเกิดขึ้นไม่เท่ากันเช่น ภัยคุกคามที่มีผลกระทบทำให้ระบบเสียหายอย่างมากแต่มีโอกาสดังกล่าวเกิดขึ้นน้อยมาก ๆ เป็นต้น ทำให้เราไม่สามารถสรุปได้ว่า ภัยคุกคามที่มีผลกระทบสูงมากจะมีความเสี่ยงสูงมากเสมอไป

ความน่าจะเป็นของภัยคุกคามที่จะเกิดขึ้นเป็นปัจจัยสำคัญที่ต้องนำมาใช้ร่วมกับผลกระทบของภัยคุกคามในการวิเคราะห์และประเมินความเสี่ยง โดยความน่าจะเป็นของภัยคุกคาม คือ โอกาสของภัยคุกคามที่จะเกิดขึ้นซึ่งพิจารณาจากความถี่ของภัยคุกคามที่เกิดขึ้นในช่วงระยะเวลาหนึ่ง ทีมนักวิเคราะห์จะทำหน้าที่กำหนดมาตรฐานสำหรับการประเมินความน่าจะเป็นของภัยคุกคามขึ้นมา ตัวอย่างของการการประเมินความน่าจะเป็นของภัยคุกคามที่จะเกิดขึ้นสำหรับองค์กรแสดงในตารางที่ 2.3

ตารางที่ 2.3 การประเมินความน่าจะเป็นของภัยคุกคามที่จะเกิดขึ้นสำหรับองค์กร

Value	Frequency of Occurrence
High	> 12 times per year
Medium	1 time every year – 11 times per year
Low	< 1 time every year

หลังจากทำการวิเคราะห์และประเมินผลกระทบที่เกิดขึ้นและความเป็นไปได้ที่จะเกิดจากภัยคุกคาม สามารถนำผลกระทบและความเป็นไปได้ที่จะเกิดจากภัยคุกคาม มาแสดงในโครงสร้างภัยคุกคามจากการเข้าถึงทรัพย์สินผ่านเครือข่ายได้

โครงสร้างภัยคุกคามแสดงให้เห็นว่าผลลัพธ์ที่เกิดขึ้นจากภัยคุกคามของการเข้าถึงทรัพย์สินผ่านเครือข่ายจะมีผลกระทบและความเป็นไปได้ในระดับใดบ้าง เช่น ภัยคุกคามจากภายในเครือข่ายโดยไม่เจตนาซึ่งส่งผลให้เกิดความเสียหายกับข้อมูลจะมีผลกระทบสูงและมีความน่าจะเป็นสูง ส่วนภัยคุกคามจากภายในเครือข่ายโดยไม่เจตนาซึ่งส่งผลให้เกิดการขัดจังหวะหรือขัดขวางการทำงานของระบบจะมีผลกระทบสูงแต่มีความน่าจะเป็นต่ำ เป็นต้น

Asset	Access	Actor	Motive	Outcome	Impact	Prob
PIDS	Network access	Inside	Accidental	Disclosure	Medium	High
				Modification	High-Medium	High
				Loss, destruction	High	High
			Deliberate	Disclosure	Medium	Medium
				Modification	High-Medium	Low
				Loss, destruction	High	Low
	Outside	Accidental	Disclosure	Medium	Low	
			Modification	High-Medium	Low	
			Loss, destruction	High	Low	
		Deliberate	Disclosure	Medium	Low	
			Modification	High-Medium	Low	
			Loss, destruction	High	Low	
			Interruption	High	Medium	

รูปที่ 2.8 โครงร่างภัยคุกคามการเข้าถึงทรัพย์สินผ่านเครือข่าย

**กระบวนการที่ 8 : พัฒนากลยุทธ์การป้องกัน**

กระบวนการที่ 8 เป็นกระบวนการสุดท้ายของแนวคิด OCTAVE ซึ่งประกอบไปด้วย 2 กระบวนการย่อย คือ กระบวนการ 8A และกระบวนการ 8B

**กระบวนการที่ 8A**

ในกระบวนการที่ 8A จะเป็นการสร้างกลยุทธ์ในการป้องกัน โดยก่อนเริ่มกระบวนการนี้ จะต้องทำการรวบรวมข้อมูลและสารสนเทศที่ได้มาจากกระบวนการที่ 1 ถึง 3 มาพิจารณาใหม่อีกครั้ง แล้วทำการสร้างกลยุทธ์ในการป้องกันขึ้นมา จากนั้นการวางแผนเพื่อลดความเสียหายที่เกิดขึ้น

OCTAVE มีการประเมินค่าความเสี่ยงโดยใช้ความน่าจะเป็นและผลกระทบมาจับคู่กัน

ในลักษณะเมทริกซ์ซึ่งจะได้ค่าความเสี่ยงออกมาเป็น 3 ระดับ วิธีการนี้เป็นการประเมินแบบเชิง

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์ การใช้งานเพื่อการศึกษาเท่านั้น เมื่ออยู่ใต้เห็นาขอสงวนสิทธิ์ในการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คุณภาพ (qualitative) คือ ค่าที่นำมาใช้ในการประเมินและผลลัพธ์ที่ได้จากการประเมินเป็นค่าระดับต่างๆ ที่กำหนดขึ้น ค่าที่ได้จึงเป็นช่วงกว้างๆ ไม่สามารถบอกเป็นตัวเลขได้ ตัวอย่างเช่น ผลการประเมินมีค่าระดับความเสี่ยงสูง (high) ทำให้รู้ว่ามีความเสี่ยงสูงแต่ไม่สามารถบอกได้ว่าระดับความเสี่ยงสูงนั้นสูงเท่าไร เพราะคำว่าสูงของแต่ละคนอาจไม่เท่ากัน

ตารางที่ 2.4 เมทริกซ์แสดงค่าระดับความเสี่ยง

		Probability		
		High	Medium	Low
Impact	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

#### กระบวนการที่ 8B

กระบวนการที่ 8B เป็นส่วนสุดท้ายของแนวคิด OCTAVE ซึ่งเป็นการสรุปผลการดำเนินงานทั้งหมดแล้วนำเสนอไปยังผู้บริหารขององค์กรเพื่อให้พิจารณาและสรุปว่าควรทำอย่างไรต่อไป มีกิจกรรมหลักๆ ที่สำคัญดังนี้

##### ▪ การเตรียมการก่อนเข้าพบผู้บริหาร

ทำการสร้างรายงานสรุปการทำงาน โดยแบ่งเป็น 2 ส่วน โดยส่วนแรกเป็นรายงานสรุปสารสนเทศเกี่ยวกับความเสี่ยงที่ได้รวบรวมระหว่างการประเมิน และส่วนที่ 2 เป็นรายงานสรุปผลลัพธ์ที่สำคัญของการประเมิน รวมถึงแผนกลยุทธ์ในการป้องกันและแผนการลดความเสี่ยง

##### ▪ นำเสนอสารสนเทศเกี่ยวกับความเสี่ยง

สารสนเทศเกี่ยวกับความเสี่ยงที่เกิดขึ้นระหว่างกระบวนการของ OCTAVE ที่สำคัญที่จะนำเสนอ คือ ช่องโหว่หรือข้อบกพร่องของระบบในปัจจุบัน สารสนเทศเกี่ยวกับทรัพย์สินที่สำคัญ และโครงสร้างของความเสี่ยงที่มีต่อทรัพย์สินที่สำคัญ

##### ▪ การทบทวนตรวจสอบ

นำเสนอแผนกลยุทธ์ในการป้องกันและแผนการลดความเสี่ยงให้ผู้บริหารพิจารณาตรวจสอบและอาจมีการแก้ไขหรือทำใหม่ตามความเหมาะสม

##### ▪ ทำขั้นตอนต่อไป

สุดท้ายผู้บริหารจะเป็นคนตัดสินใจว่าจะนำแผนกลยุทธ์ในการป้องกันและแผนการลดความเสี่ยงมาประยุกต์ใช้อย่างไร โดยจะพิจารณาว่าจะทำอะไรเป็นขั้นตอนต่อไปหลังจากการเอกสารนี้เป็นเอกสารที่ส่งมอบไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประเมิน ใครจะเป็นผู้รับผิดชอบในการทำขั้นตอนต่อไปและจะอย่างไรต่อไปเมื่อขั้นตอนนี้เสร็จสิ้น

### 2.3 การวิเคราะห์ความเสี่ยงของสารสนเทศโดยใช้แนวคิด CobiT

CobiT (Control Objectives for Information and Related Technology) เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของ CobiT ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ (Business Process) ซึ่งแบ่งเป็น 4 โดเมนหลัก (Domain)

#### โดเมนหลักของ CobiT

##### 1. การวางแผนและการจัดการองค์กร (Planning and Organization)

โดเมนนี้ครอบคลุมถึงกลยุทธ์และการระบุทิศทางของการนำเทคโนโลยีสารสนเทศมาช่วยในการดำเนินไปยังเป้าหมายธุรกิจขององค์กร รวมถึงการวางแผนกลยุทธ์ การติดต่อสื่อสารกัน การจัดการมุมมองที่แตกต่างกัน และความเหมาะสมของ โครงสร้างพื้นฐานของเทคโนโลยีกับองค์กร

##### 2. การจัดหาและติดตั้ง (Acquisition and Implementation)

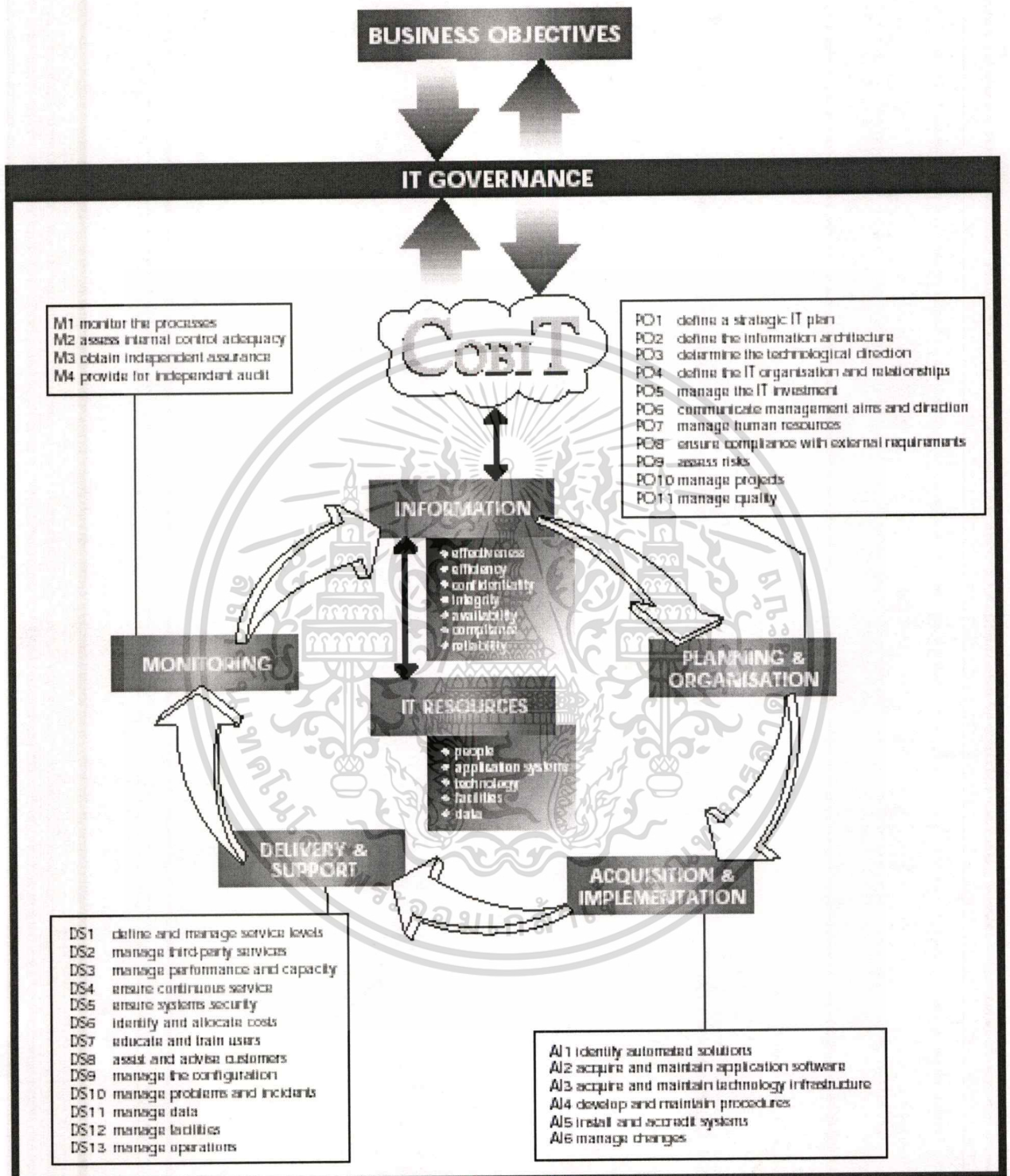
โดเมนนี้เกี่ยวกับการทำตามกลยุทธ์ที่กำหนดไว้ เป็นการนำเทคโนโลยีสารสนเทศมาติดตั้งและประยุกต์ใช้ร่วมกับกระบวนการทางธุรกิจขององค์กร รวมถึงการเปลี่ยนแปลงและการบำรุงรักษาระบบที่มีอยู่

##### 3. การส่งมอบและบำรุงรักษา (Delivery and Support)

โดเมนนี้เกี่ยวกับการให้บริการซึ่งอยู่ในขอบเขตของความปลอดภัยและความต่อเนื่อง รวมถึงส่วนของการประมวลผลข้อมูล โดยระบบงาน

##### 4. การติดตามผล (Monitoring)

กระบวนการทางเทคโนโลยีสารสนเทศทั้งหมดจะต้องมีการประเมินเกี่ยวกับคุณภาพและการปฏิบัติตามข้อบังคับ โดเมนนี้จะต้องแก้ไขการจัดการที่ผิดพลาดของกระบวนการควบคุมขององค์กร อาจมีการตรวจสอบจากผู้ตรวจสอบภายในองค์กรเองหรือจากบุคคลภายนอก



รูปที่ 2.9 กระบวนการทางเทคโนโลยีสารสนเทศของ CobiT ถูกกำหนดไว้ภายใต้ 4 โดเมน

จากรูปที่ 2.9 แสดงให้เห็นภาพรวมของกระบวนการดำเนินงานทางเทคโนโลยีสารสนเทศ  
 ในองค์กร ซึ่งในการวิเคราะห์ความเสี่ยงตามแนวคิดของ CobiT จะมีองค์ประกอบที่สำคัญ คือ  
 เอกสารที่เป็นเอกสารที่ส่งมอบไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นิยามให้ไปใช้ประโยชน์ด้านการค้า  
 ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดเมนหลักทั้ง 4 โดเมน คุณภาพหรือมาตรฐานของระบบสารสนเทศ 7 ประการ และทรัพยากรด้านเทคโนโลยีสารสนเทศ 5 ประเภท ซึ่งมีรายละเอียดดังนี้

#### คุณภาพของระบบสารสนเทศ 7 ประการ (Information Criteria)

- ประสิทธิภาพ (Effectiveness) หมายถึงข้อมูลที่ใช้เกี่ยวข้องกับกระบวนการทางธุรกิจ รวมทั้งมีการส่งมอบข้อมูลแก่ผู้ใช้ได้อย่าง ถูกต้อง ตรงเวลา สม่าเสมอ และใช้ประโยชน์ได้
- ประสิทธิภาพ (Efficiency) หมายถึง มีการใช้ประโยชน์จากทรัพยากรอย่างเต็มที่เพื่อให้ได้มาซึ่งข้อมูลสารสนเทศ
- ความลับ (Confidentiality) หมายถึง การป้องกันการเปิดเผยข้อมูลที่สำคัญต่อบุคคลหรือหน่วยงานที่ไม่ได้รับอนุญาต
- ความสมบูรณ์และถูกต้อง (Integrity) หมายถึงความครบถ้วนถูกต้องของข้อมูล ตลอดจนเป็นข้อมูลใช้ได้ ในแง่ของความคาดหมายและการให้ความสำคัญของธุรกิจ (business values and expectations)
- การมีใช้เมื่อต้องการ (Availability) หมายถึง เป็นข้อมูลที่สามารถใช้ได้เมื่อต้องการและจำเป็นใช้ทั้งในปัจจุบันและอนาคต และรวมทั้งการป้องกันภัยให้กับทรัพยากรต่างๆที่จำเป็นและการรักษาระดับความสามารถในการทำงานของทรัพยากรเหล่านั้น
- การปฏิบัติตามระบบ (Compliance) หมายถึง การที่ข้อมูลได้จัดทำขึ้นตามกฎหมาย ระเบียบ ข้อบังคับ หลักเกณฑ์ ข้อตกลง หรือกฎหมาย ที่มีขึ้นเพื่อบังคับใช้ทั้งจากหน่วยงานภายในและภายนอกองค์กร เช่น ข้อบังคับของตลาดหลักทรัพย์ ประมวลกฎหมายอาญาอากร หลักการบัญชีที่ยอมรับโดยทั่วไป เป็นต้น
- ความน่าเชื่อถือของข้อมูล (Reliability of Information) หมายถึงความสามารถในการจัดหาข้อมูลที่เหมาะสมให้แก่ผู้บริหารของกิจการเพื่อสามารถดำเนินธุรกิจและเพื่อให้สามารถจัดทำรายงานทางการเงินและรายงานที่จำเป็นอื่นๆภายใต้ความรับผิดชอบของผู้บริหาร

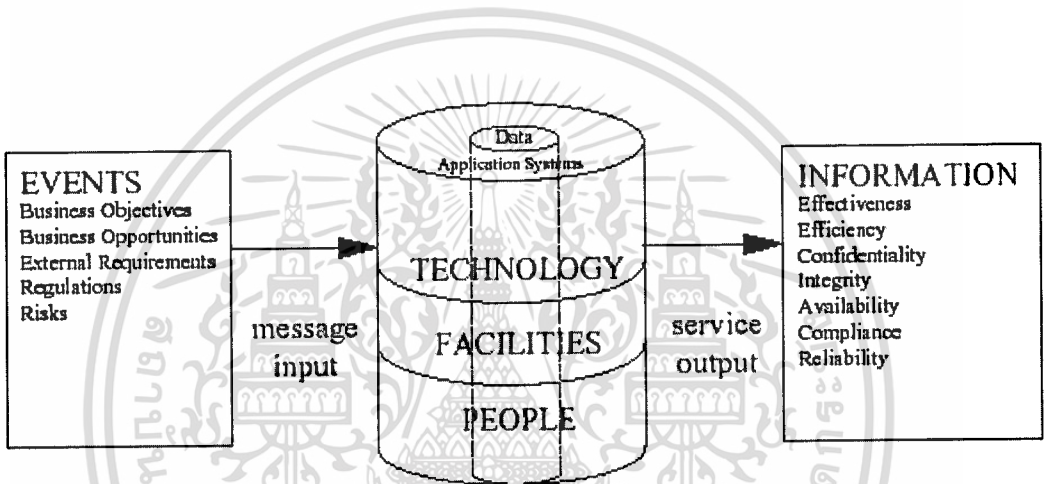
#### ทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resources) 5 ประเภท

- ข้อมูล (Data) รวมความถึงข้อมูลในรูปแบบต่างๆทั้งที่มีโครงสร้างและไม่มีโครงสร้าง ข้อมูลด้านกราฟฟิค และข้อมูลที่เป็นเสียง
- ระบบงาน (Application System) ได้แก่ ขั้นตอนและกระบวนการปฏิบัติงานทั้งที่ทำด้วยมือและโปรแกรมคอมพิวเตอร์
- เทคโนโลยี (Technology) ได้แก่ เครื่องคอมพิวเตอร์ ระบบปฏิบัติการ ระบบบริหารฐานข้อมูล ระบบเครือข่ายและระบบมัลติมีเดีย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- สิ่งอำนวยความสะดวก (Facilities) ได้แก่ทรัพยากรต่างๆที่ใช้เป็นสถานที่ติดตั้งหรือจัดวาง ตลอดจนสาธารณูปโภคที่จำเป็นเพื่อการปฏิบัติงานของระบบสารสนเทศ
- บุคลากร (People) ได้แก่บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงาน สำหรับการดูแลและจัดทำระบบสารสนเทศ

จากมาตรฐานของระบบสารสนเทศ 7 ประการ และทรัพยากรด้านเทคโนโลยีสารสนเทศ 5 ประเภท สามารถนำมาแสดงความสัมพันธ์ในการดำเนินงานของระบบสารสนเทศในองค์กร ร่วมกับความต้องการตามกระบวนการธุรกิจขององค์กรได้ดังรูปที่ 2.10



รูปที่ 2.10 โครงสร้างการดำเนินงานของธุรกิจและเทคโนโลยีสารสนเทศ

จากรูปที่ 2.10 จะเห็นได้ว่าการดำเนินงานของธุรกิจจะต้องอาศัยกระบวนการของระบบสารสนเทศ โดยเหตุการณ์ต่างๆที่เป็น message input เข้ามา จะต้องผ่านการดำเนินงานของระบบ และได้ service output ออกมาเป็นสารสนเทศที่มีส่วนประกอบ 7 ประการ แต่ message input ที่เข้ามาจะมีความเสี่ยงรวมอยู่ด้วยเสมอ ทำให้สารสนเทศที่ได้ออกมาจากระบบมีความเสี่ยงเช่นกัน

การวิเคราะห์ความเสี่ยงของ CobIT ได้กำหนดโครงสร้างและขอบเขตไว้โดยพิจารณาจากองค์ประกอบที่สำคัญที่ได้กล่าวไปแล้ว ดังรูปที่ 2.11

DOMAIN	PROCESS	Information Criteria							IT Resources				
		effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Planning & Organisation	PO1 Define a strategic IT plan	P	S						✓	✓	✓	✓	✓
	PO2 Define the information architecture	P	S	S	S					✓			✓
	PO3 Determine technological direction	P	S								✓		✓
	PO4 Define the IT organisation and relationships	P	S						✓				
	PO5 Manage the IT investment	P	P					S	✓	✓	✓	✓	
	PO6 Communicate management aims and direction	P					S		✓				
	PO7 Manage human resources	P	P						✓				
	PO8 Ensure compliance with external requirements	P					P	S	✓	✓			✓
	PO9 Assess risks	P	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10 Manage projects	P	P						✓	✓	✓	✓	
	PO11 Manage quality	P	P	P				S	✓	✓	✓	✓	
Acquisition & Implementation	A11 Identify automated solutions	P	S							✓	✓	✓	
	A12 Acquire and maintain application software	P	P		S	S	S		✓				
	A13 Acquire and maintain technology infrastructure	P	P		S						✓		
	A14 Develop and maintain procedures	P	P		S	S	S		✓	✓	✓	✓	
	A15 Install and accredit systems	P			S	S			✓	✓	✓	✓	
	A16 Manage changes	P	P	P	P			S	✓	✓	✓	✓	
Delivery & Support	DS1 Define and manage service levels	P	P	S	S	S	S	S	✓	✓	✓	✓	
	DS2 Manage third-party services	P	P	S	S	S	S	S	✓	✓	✓	✓	
	DS3 Manage performance and capacity	P	P		S				✓	✓	✓	✓	
	DS4 Ensure continuous service	P	S			P			✓	✓	✓	✓	
	DS5 Ensure systems security			P	P	S	S	S	✓	✓	✓	✓	
	DS6 Identify and allocate costs		P					P	✓	✓	✓	✓	
	DS7 Educate and train users	P	S						✓				
	DS8 Assist and advise customers	P	P						✓	✓			
	DS9 Manage the configuration	P				S	S		✓	✓	✓	✓	
	DS10 Manage problems and incidents	P	P			S			✓	✓	✓	✓	
	DS11 Manage data				P			P	✓			✓	
	DS12 Manage facilities				P	P			✓			✓	
	DS13 Manage operations	P	P		S	S			✓	✓	✓	✓	
Monitoring	M1 Monitor the processes	P	P	S	S	S	S	S	✓	✓	✓	✓	
	M2 Assess internal control adequacy	P	P	S	S	S	P	S	✓	✓	✓	✓	
	M3 Obtain independent assurance	P	P	S	S	S	P	S	✓	✓	✓	✓	
	M4 Provide for independent audit	P	P	S	S	S	P	S	✓	✓	✓	✓	

[P] primary [S] secondary

(✓) applicable to

รูปที่ 2.11 สรุป Control Objectives ของ CobiT

จากรูปที่ 2.11 เป็นการแสดง Control Objective ในแต่ละ โดเมนว่าใน Control Objective แต่ละตัวมีความเกี่ยวข้องกับมาตรฐานของระบบสารสนเทศในส่วนไหนบ้าง ตัวอย่างเช่น PO1 (Define a Strategy IT plan) มีผลกระทบกับมาตรฐานของระบบสารสนเทศในส่วนประสิทธิภาพ (Effectiveness) ในระดับ P และประสิทธิผล (Efficiency) ในระดับ S โดยที่ P คือ Primary หมายความว่า มีผลกระทบโดยตรง ส่วน S คือ Secondary หมายถึง มีผลกระทบทางอ้อม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 3

### การวิเคราะห์และออกแบบระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

#### 3.1 ลักษณะและขอบเขตของระบบ

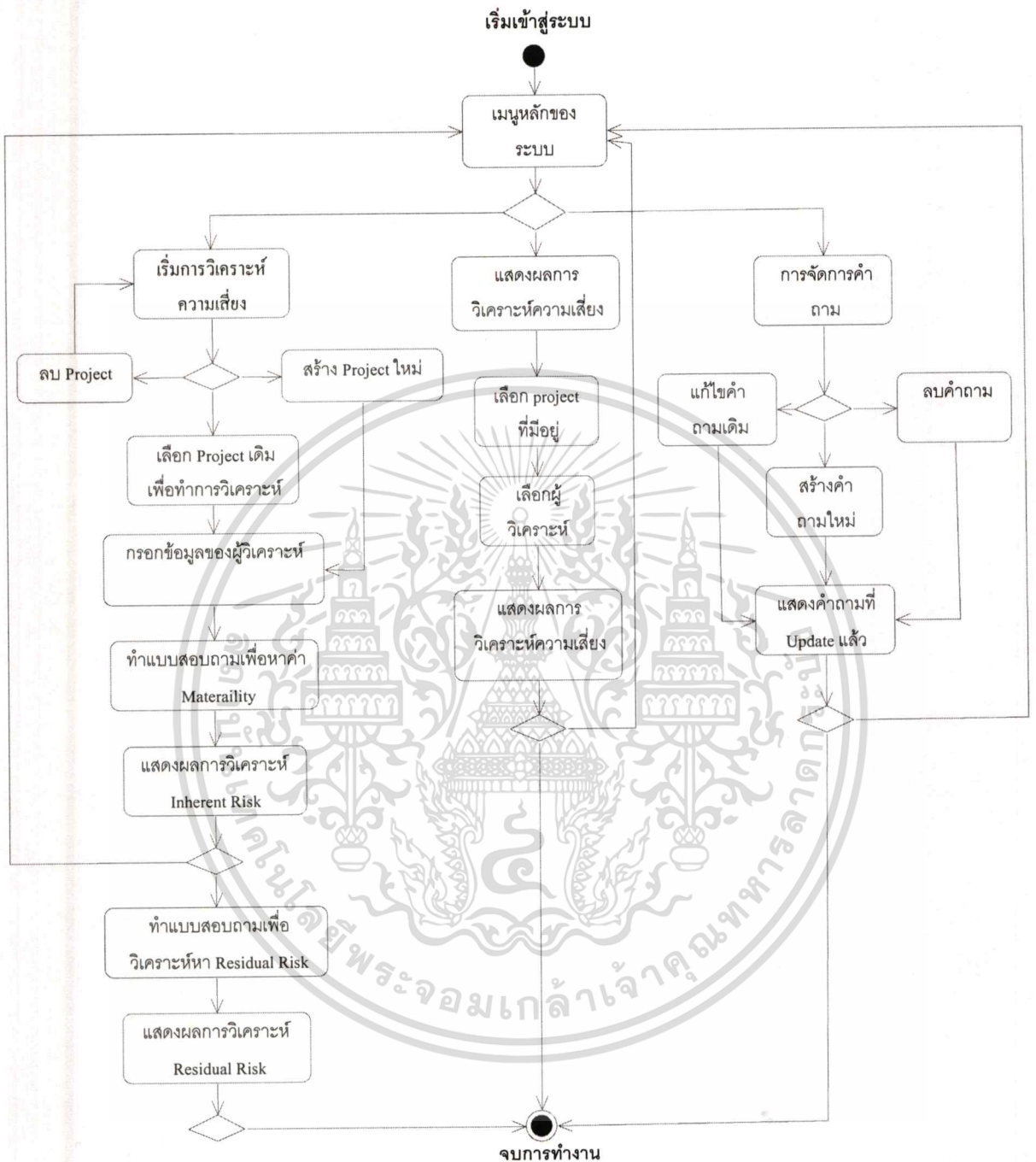
##### 3.1.1 กิจกรรมโดยรวมของระบบ

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ เป็นการนำระบบคอมพิวเตอร์มาช่วยในการวิเคราะห์ความเสี่ยงของสารสนเทศภายในองค์กร ซึ่งกิจกรรมโดยรวมของระบบสามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.1 โดยมีขั้นตอนการทำงานดังต่อไปนี้

เมื่อเริ่มเข้าสู่ระบบ จะเข้ามาที่เมนูหลักของระบบ ประกอบด้วย 3 ส่วนหลัก คือ เริ่มการวิเคราะห์ความเสี่ยง แสดงผลวิเคราะห์ความเสี่ยง และการจัดการคำถาม ส่วนการจัดการผู้ใช้ระบบ จะขออธิบายในส่วน Sequence Diagram ของการจัดการผู้ใช้ระบบ

- กรณีเลือกเข้าไปในส่วน เริ่มการวิเคราะห์ความเสี่ยง จะสามารถเลือกได้ 3 อย่าง คือ สร้าง Project ใหม่ เลือก Project เดิมเพื่อทำการวิเคราะห์ หรือ ลบ Project
- 1. กรณีผู้วิเคราะห์ เลือกลบ Project ระบบจะทำการลบ Project ที่ถูกเลือกและกลับไปในส่วน เริ่มการวิเคราะห์ความเสี่ยง เพื่อรอรับคำสั่งใหม่
- 2. กรณีผู้วิเคราะห์ เลือก Project เดิมเพื่อทำการวิเคราะห์ ระบบจะเลือก Project นั้นแล้วผ่านไปยังขั้นตอนต่อไป
- 3. กรณีผู้วิเคราะห์ เลือกสร้าง Project ใหม่ ระบบจะเลือก Project นั้นแล้วผ่านไปยังขั้นตอนต่อไป
- 4. ผู้วิเคราะห์จะทำการกรอกข้อมูลส่วนตัว
- 5. ระบบจะให้ผู้วิเคราะห์ตอบแบบสอบถามเพื่อนำมาหาค่า materiality และนำมาใช้เป็นข้อมูลในการวิเคราะห์ความเสี่ยงต่อไป
- 6. ระบบแสดงผลการวิเคราะห์ในส่วน Inherent Risk
- 7. ผู้วิเคราะห์เลือกที่จะทำการวิเคราะห์ในส่วน Residual Risk ต่อไป หรือจะกลับไปยังเมนูหลักของระบบ
- 8. ระบบจะให้ผู้วิเคราะห์ตอบแบบสอบถามเพื่อนำไปใช้ในการวิเคราะห์หา Residual Risk
- 9. ระบบแสดงผลการวิเคราะห์ในส่วน residual Risk
- 10. ผู้วิเคราะห์เลือกที่จะออกจากระบบ หรือจะกลับไปยังเมนูหลักของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.1 Activity Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

- กรณีเลือกเข้าไปในส่วน แสดงผลวิเคราะห์ความเสี่ยง
- 1. ผู้วิเคราะห์จะทำการเลือก Project ที่ต้องการจะดู จากรายการของ Project ที่มีอยู่
- 2. ผู้วิเคราะห์จะทำการเลือกว่าใน Project นี้ จะดูผลการวิเคราะห์ของใคร เพราะใน 1 Project อาจมีผู้วิเคราะห์หลายคน

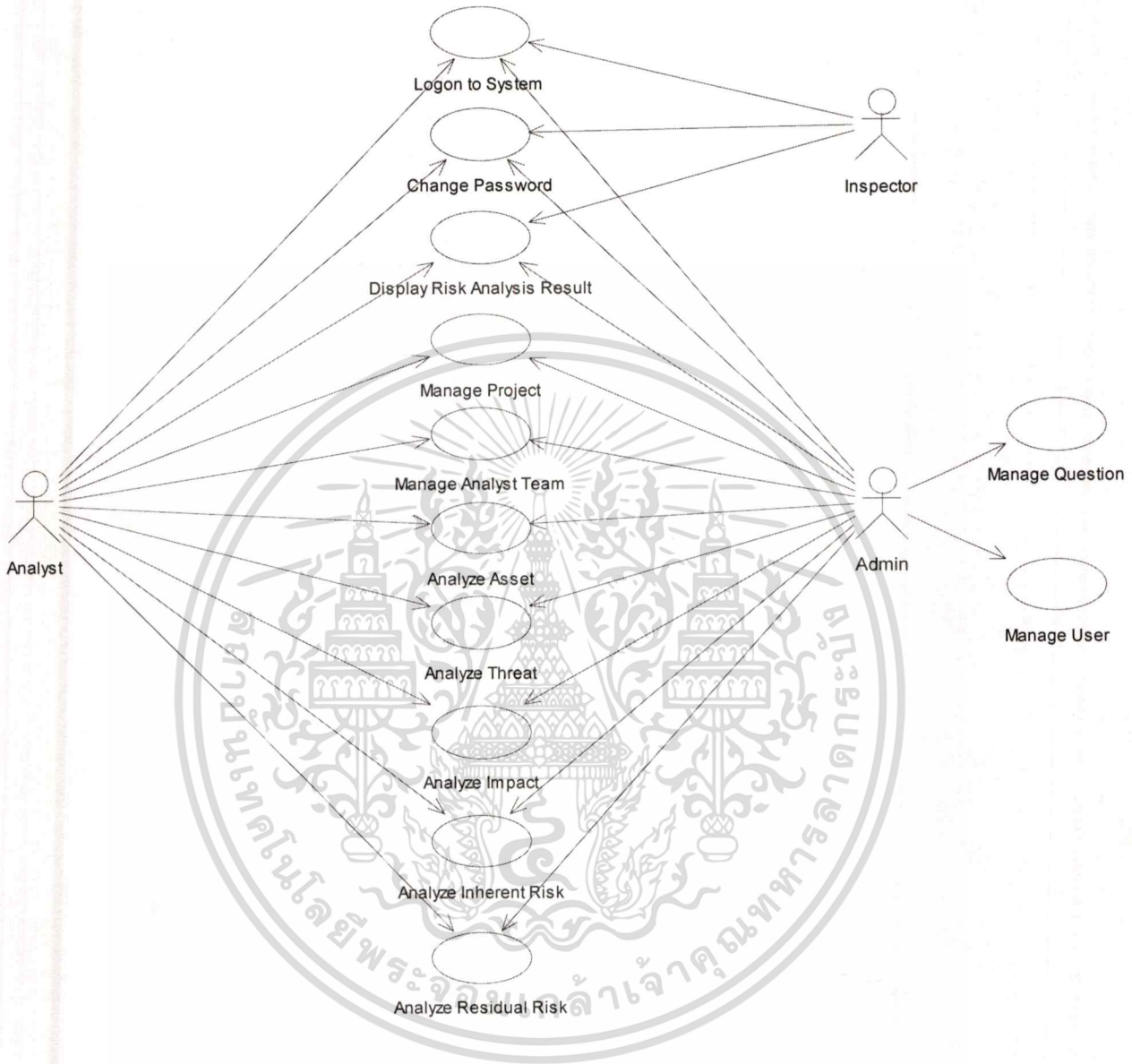
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. ระบบแสดงผลการวิเคราะห์ตามที่เลือกไว้
4. ผู้วิเคราะห์เลือกว่าจะออกจากระบบ หรือจะกลับไปยังเมนูหลักของระบบ
  - กรณีเลือกเข้าไปในส่วน การจัดการคำถาม (ผู้ดูแลระบบเท่านั้นที่สามารถเข้าใช้ส่วนนี้ได้)
    1. กรณีผู้ดูแลระบบ เลือกลบคำถาม ระบบจะทำการลบคำถามที่ถูกเลือก
    2. กรณีผู้ดูแลระบบ เลือกสร้างคำถาม ระบบให้ผู้ดูแลระบบ สร้างคำถามใหม่
  - 3. กรณีผู้ดูแลระบบ เลือกแก้ไขคำถามเดิม ระบบให้ผู้ดูแลระบบแก้ไขคำถามที่ผู้ดูแลระบบเป็นคนเลือก
  - 4. ระบบแสดงคำถามที่ได้ทำการ Update แล้วให้ผู้ดูแลระบบดู
  - 5. ผู้ดูแลระบบ เลือกว่าจะออกจากระบบ หรือจะกลับไปยังเมนูหลักของระบบ

### 3.1.2 ภาพรวมของฟังก์ชันการทำงานในระบบ

ภาพรวมของฟังก์ชันการทำงานในระบบวิเคราะห์ความเสี่ยงของสารสนเทศสามารถแสดงได้โดยใช้ Use Case Diagram โดยมีจุดประสงค์เพื่อแสดงให้เห็นว่าภายในระบบ จะมีการแบ่งออกเป็นส่วนประกอบย่อยๆ อะไรบ้าง ซึ่งจะให้เห็นฟังก์ชันหลักที่เกิดขึ้นในระบบและแสดงความสัมพันธ์ระหว่างผู้ใช้กับระบบ

จาก Use Case Diagram ในรูปที่ 3.2 จะประกอบด้วย Actor ซึ่งแสดงแทนด้วยสัญลักษณ์รูปคน หมายถึง ผู้ที่เกี่ยวข้องกับระบบ จะเห็นว่าในระบบวิเคราะห์ความเสี่ยงของสารสนเทศ ประกอบด้วย Actor 3 ตัว ได้แก่ ผู้วิเคราะห์หรือนักวิเคราะห์(Analist) และผู้ใช้ทั่วไป (Inspector) ซึ่งเปรียบเสมือน User ที่เข้ามาใช้งานระบบ และผู้ดูแลระบบ (Admin) ส่วน Use Case จะแสดงแทนด้วยสัญลักษณ์รูปวงรี แสดงถึงฟังก์ชันการทำงานของระบบ สามารถบอกได้ว่าระบบสามารถทำอะไรได้บ้าง ซึ่งได้มาจากความต้องการของระบบ นอกจากนั้นยังมีการแสดงความสัมพันธ์ระหว่าง Actor กับ Use Case ด้วยเส้นที่ลากจาก Actor ไปยัง Use Case โดยทุกเส้นจะมีความสัมพันธ์แบบ <<communicate >> ซึ่งขอละไว้ไม่แสดงในเส้นเพื่อความดูง่าย



รูปที่ 3.2 Use Case Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

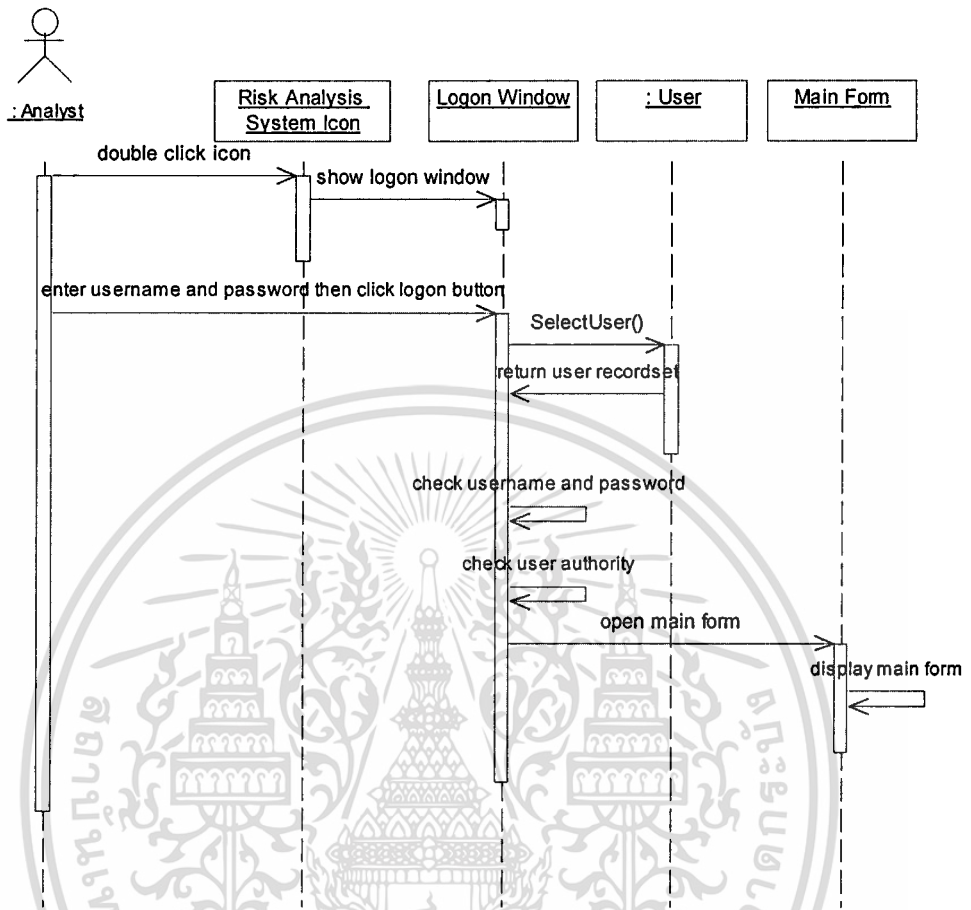
ระบบวิเคราะห์ความเสี่ยงของสารสนเทศประกอบด้วยฟังก์ชันการทำงานต่อไปนี้

- Logon to System                      หมายถึง                      การ Logon เข้าสู่ระบบ
- Change Password                      หมายถึง                      เปลี่ยนรหัสผ่าน
- Display Risk Analysis Result                      หมายถึง                      แสดงผลการวิเคราะห์ความเสี่ยง
- Manage Project                      หมายถึง                      สร้างจัดการ โครงการ
- Manage Analyst Team                      หมายถึง                      สร้างจัดการทีมนักวิเคราะห์ความเสี่ยง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

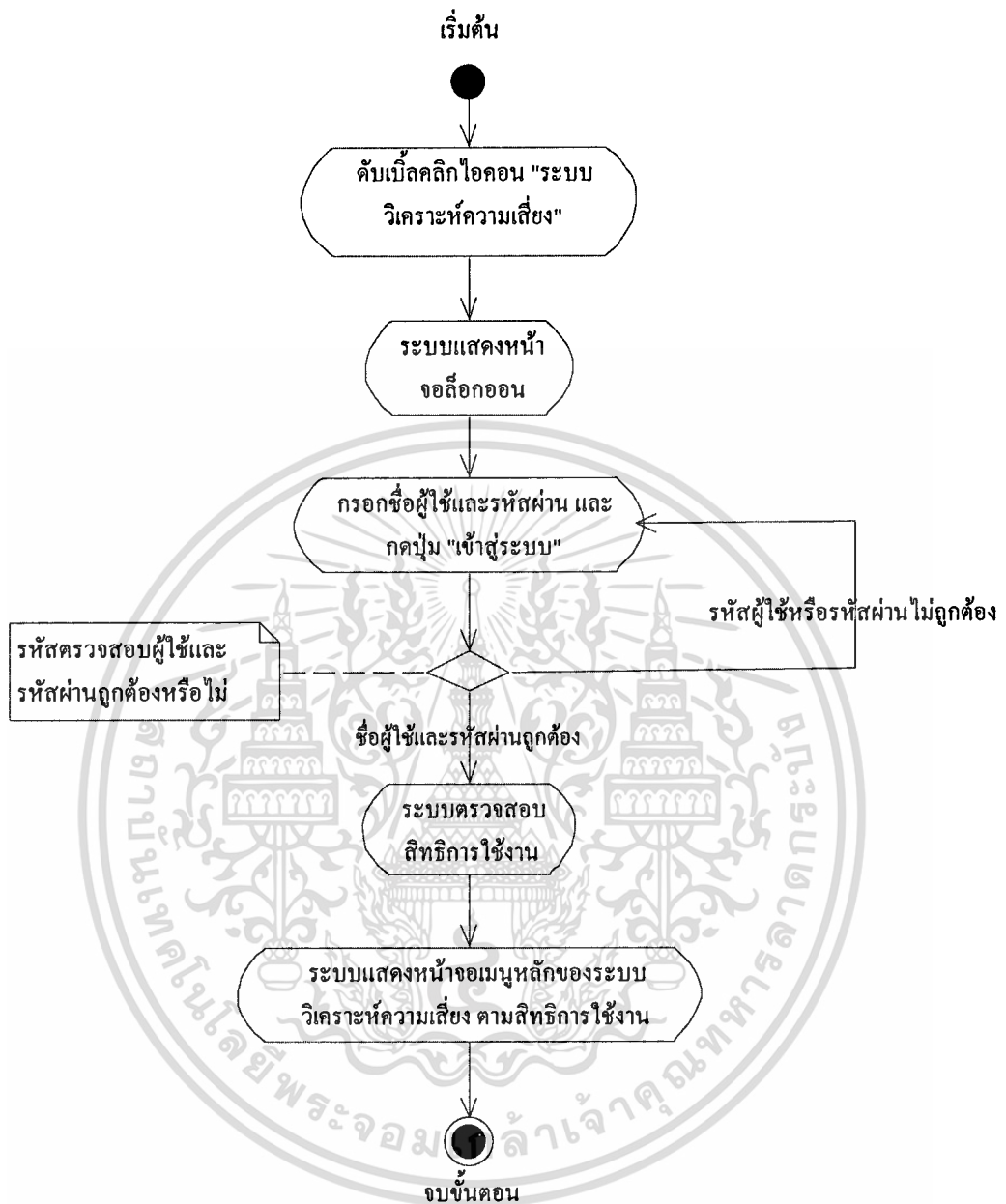






รูปที่ 3.3 Sequence Diagram : Logon to System

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



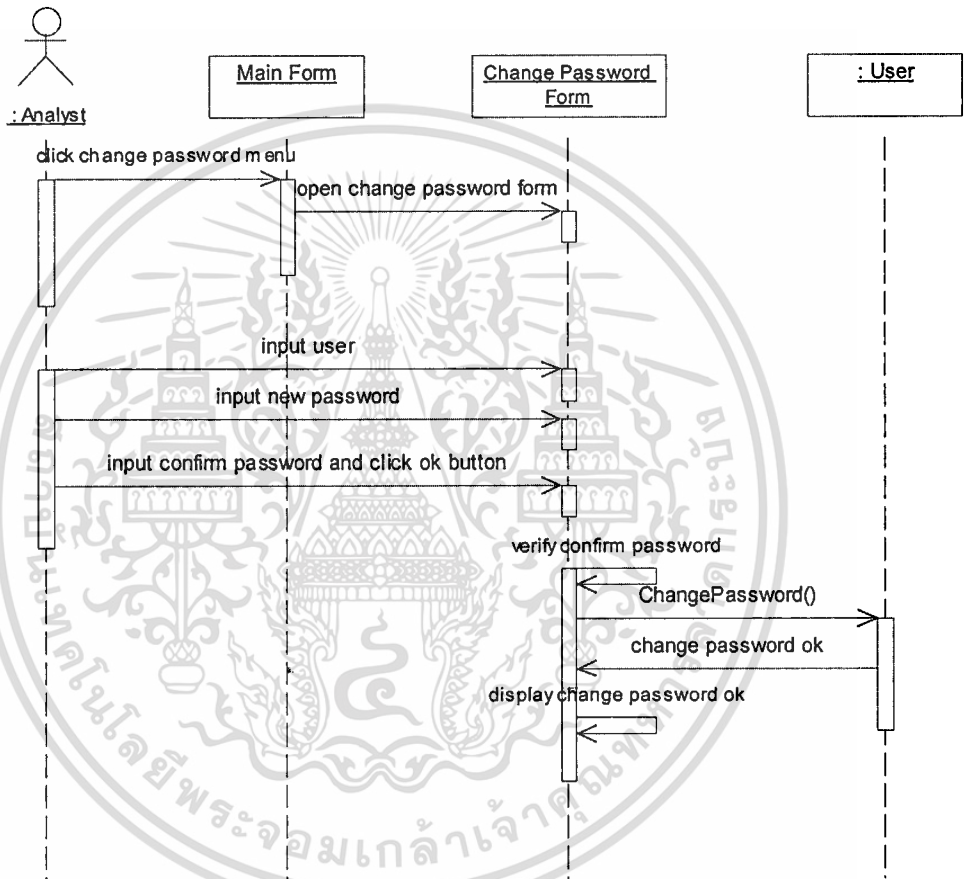
รูปที่ 3.4 Activity Diagram : Logon to System

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Logon to System สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.4 โดยมีขั้นตอนดังต่อไปนี้

1. ดับเบิลคลิกไอคอน “ระบบวิเคราะห์ความเสี่ยง”
2. ระบบแสดงหน้าจอล็อกอิน
3. กรอกชื่อผู้ใช้และรหัสผ่านและกดปุ่ม “เข้าสู่ระบบ”

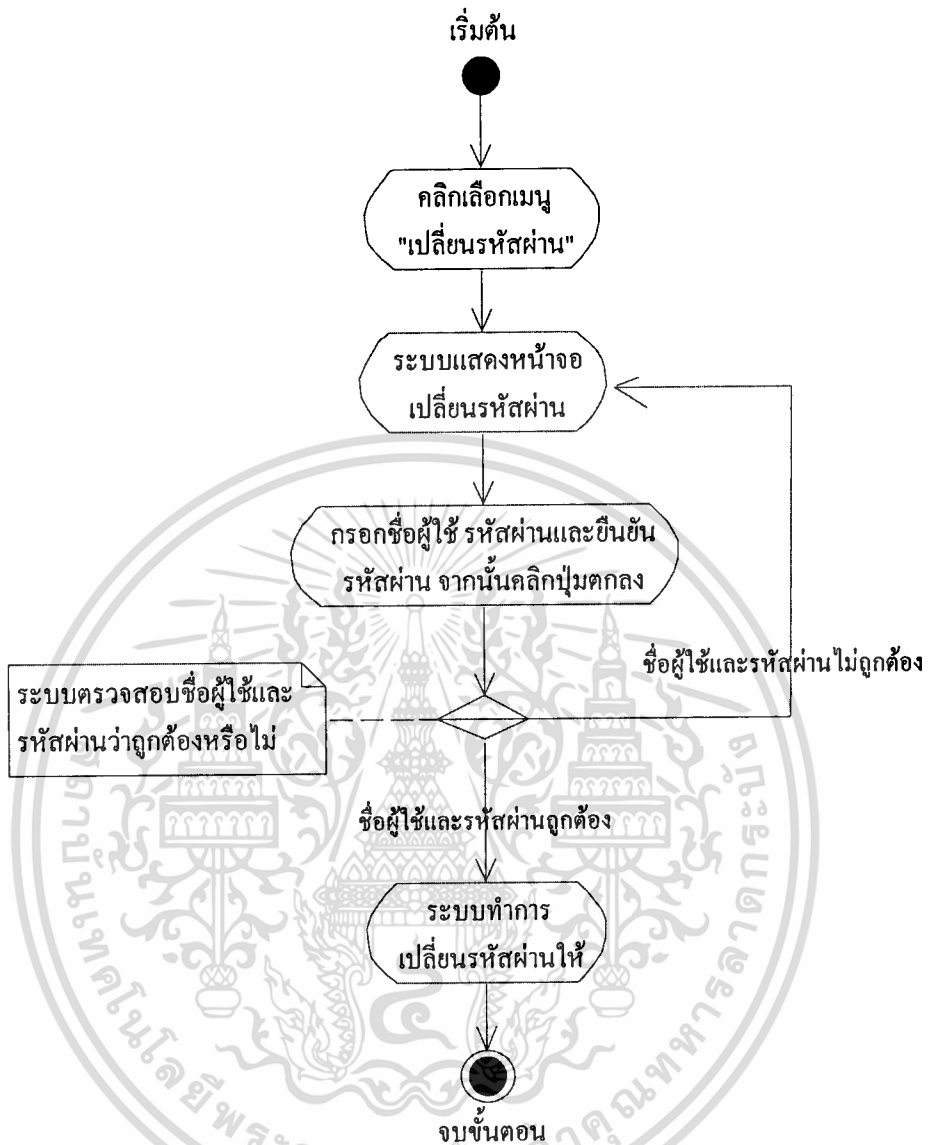
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4. ระบบตรวจสอบชื่อผู้ใช้และรหัสผ่าน ถ้าชื่อผู้ใช้และรหัสผ่าน ไม่ถูกต้องจะกลับไปยังหน้าจอล็อกออน
5. ถ้าชื่อผู้ใช้และรหัสผ่านถูกต้องระบบจะทำการตรวจสอบสิทธิการใช้งาน
6. ระบบแสดงหน้าจอเมนูหลักของระบบวิเคราะห์ความเสี่ยง ตามสิทธิการใช้งาน



รูปที่ 3.5 Sequence Diagram : Change Password

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



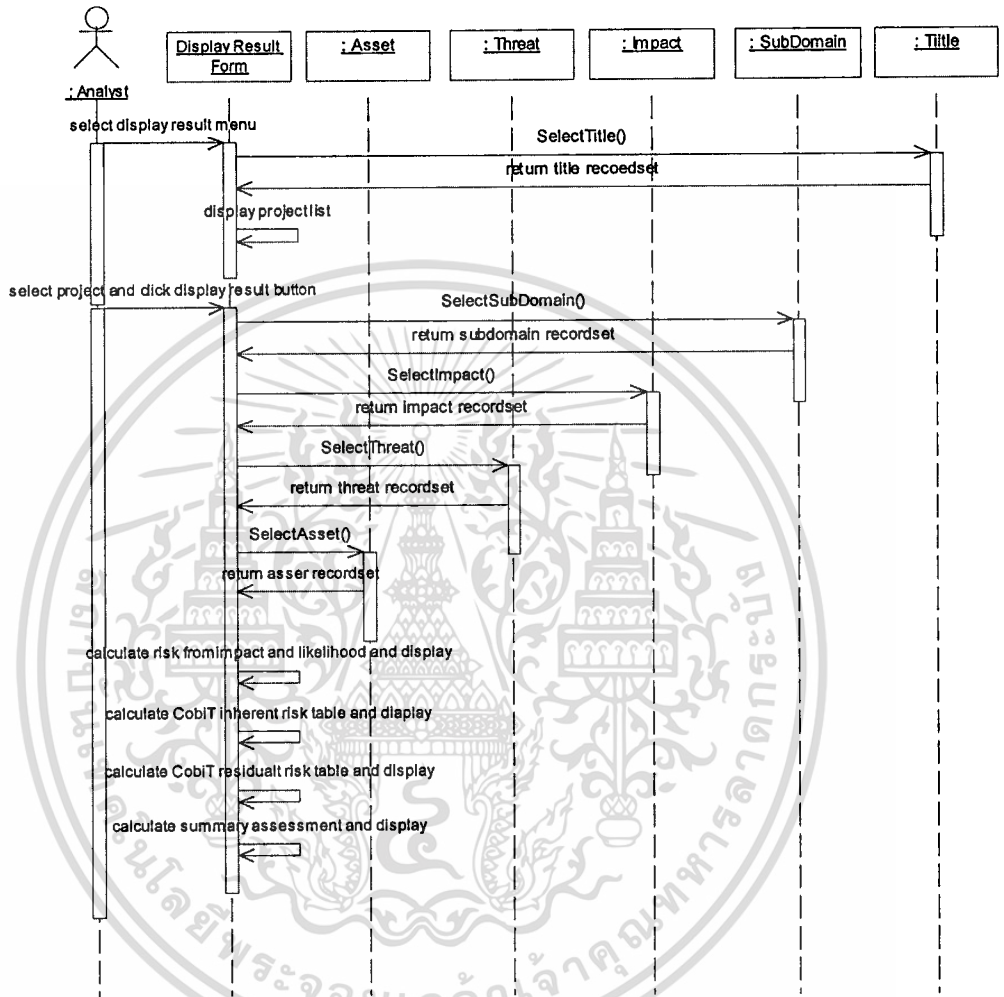
รูปที่ 3.6 Activity Diagram : Change Password

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Change Password สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.6 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกเลือกเมนู “เปลี่ยนรหัสผ่าน”
2. ระบบแสดงหน้าจอเปลี่ยนรหัสผ่าน
3. กรอกชื่อผู้ใช้ รหัสผ่าน และยืนยันรหัสผ่าน จากนั้นคลิกปุ่มตกลง
4. ระบบตรวจสอบชื่อผู้ใช้และรหัสผ่านว่าถูกต้องหรือไม่ ถ้าชื่อผู้ใช้และรหัสผ่านไม่ถูกต้องระบบจะกลับไปยังหน้าจอเปลี่ยนรหัสผ่าน

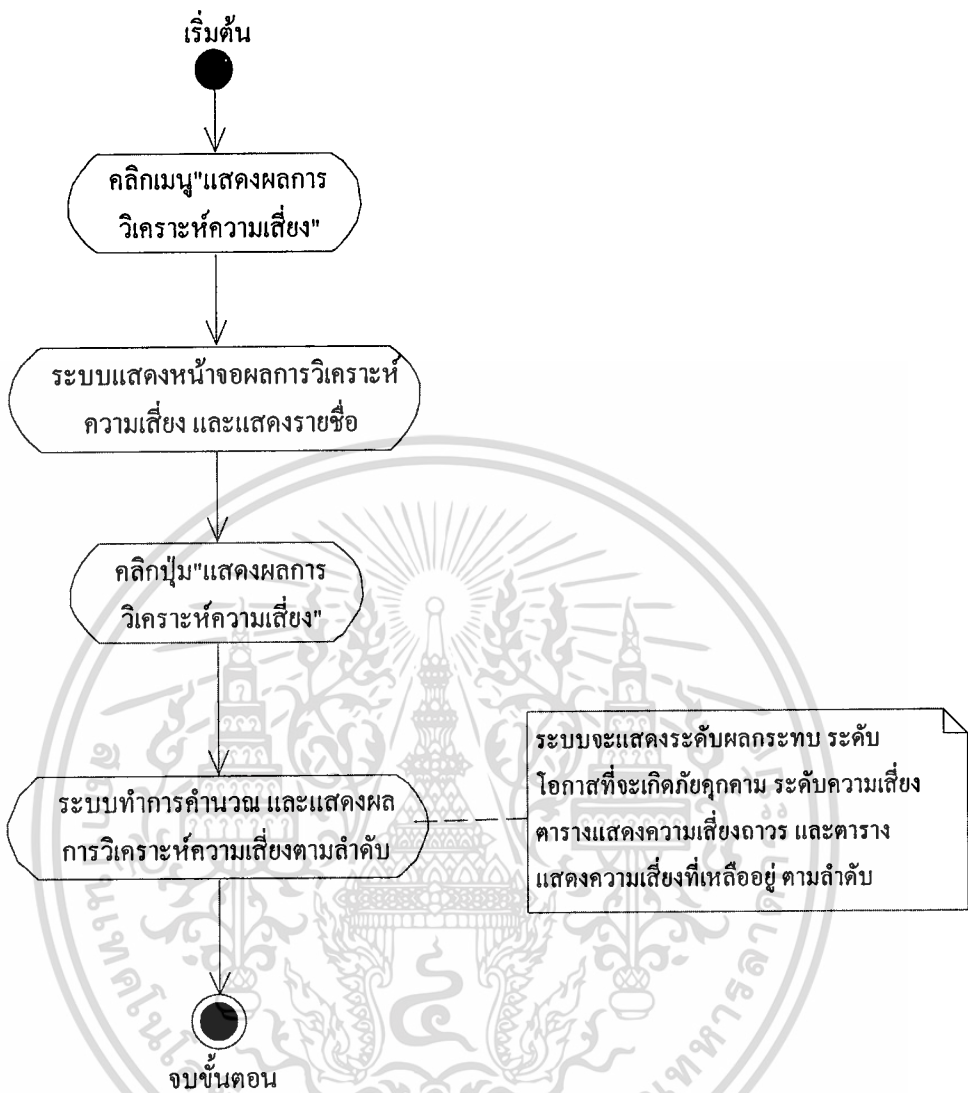
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. ถ้าชื่อผู้ใช้และรหัสผ่านถูกต้องระบบจะทำการเปลี่ยนรหัสผ่านให้



รูปที่ 3.7 Sequence Diagram : Display Risk Analysis Result

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

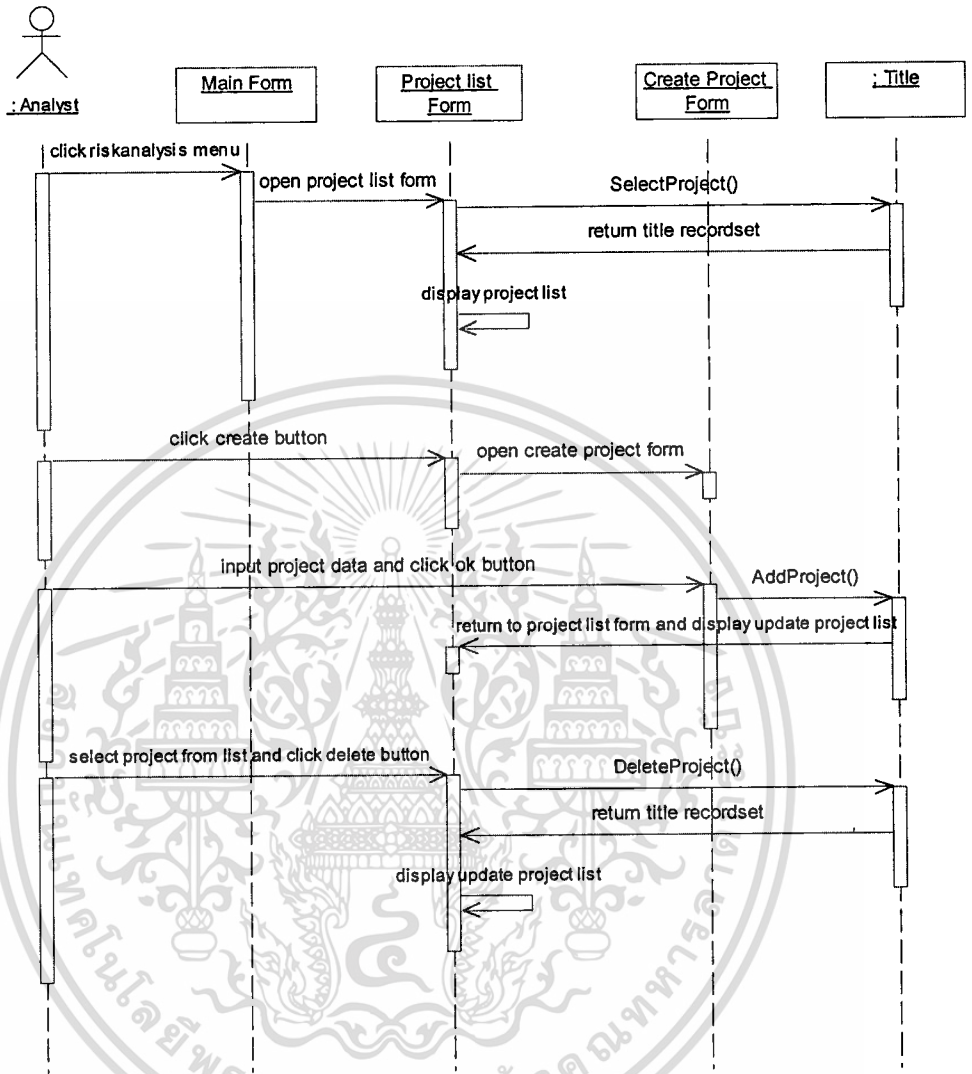


รูปที่ 3.8 Activity Diagram : Display Risk Analysis Result

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Display Risk Analysis Result สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.8 โดยมีขั้นตอนดังต่อไปนี้

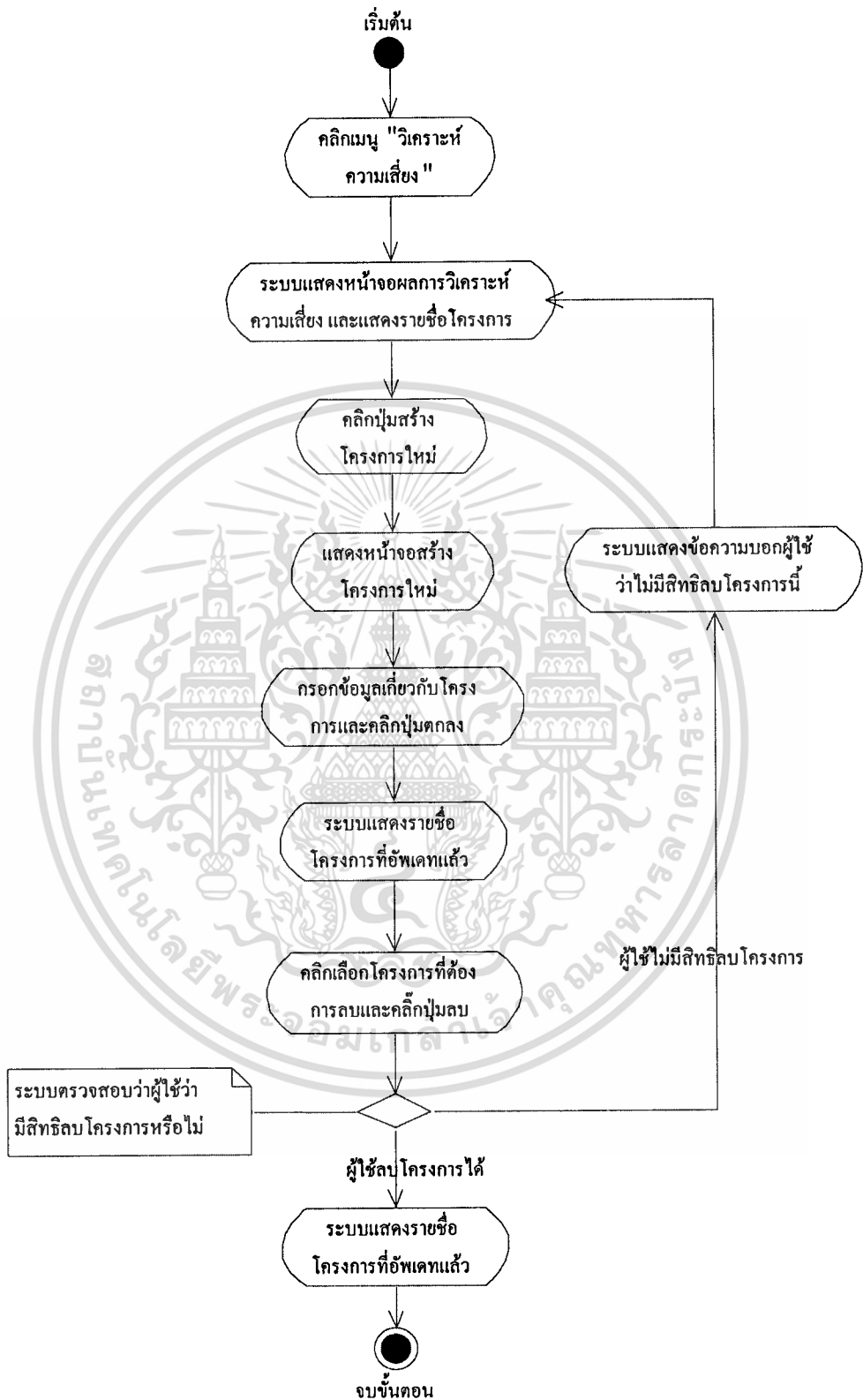
1. คลิกเมนู “แสดงผลการวิเคราะห์ความเสี่ยง”
2. ระบบแสดงหน้าจอผลการวิเคราะห์ความเสี่ยงและแสดงรายชื่อ
3. คลิกปุ่ม “แสดงผลการวิเคราะห์ความเสี่ยง ”
4. ระบบทำการคำนวณและแสดงผลการวิเคราะห์ความเสี่ยงตามลำดับ โดยระบบจะแสดงระดับผลกระทบ ระดับโอกาสที่จะเกิดภัยคุกคาม ระดับความเสี่ยง ตารางแสดงความเสี่ยงถาวร และตารางแสดงความเสี่ยงที่เหลืออยู่ ตามลำดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.9 Sequence Diagram : Manage Project

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



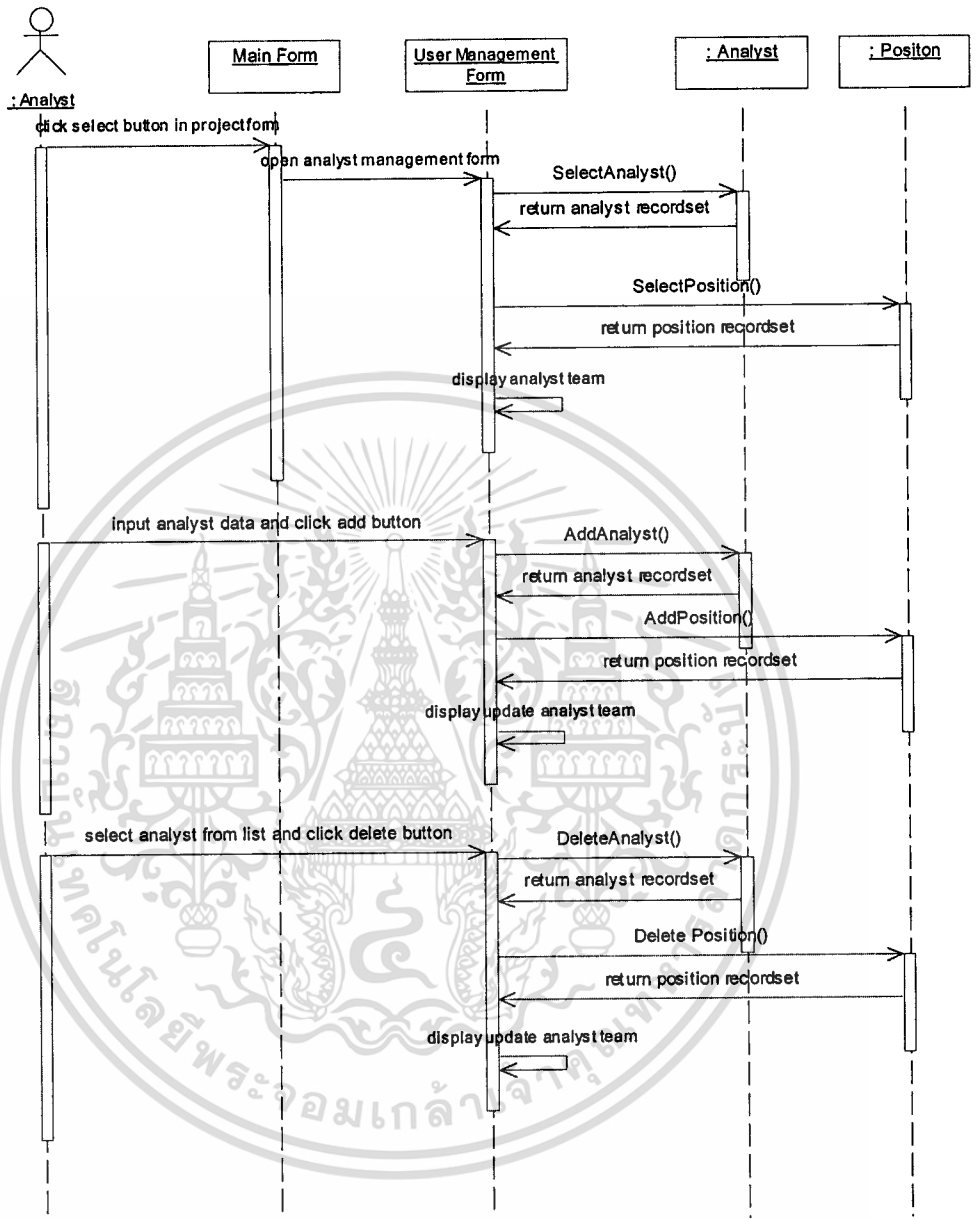
รูปที่ 3.10 Activity Diagram : Manage Project

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Manage Project สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.10 โดยมีขั้นตอนดังต่อไปนี้

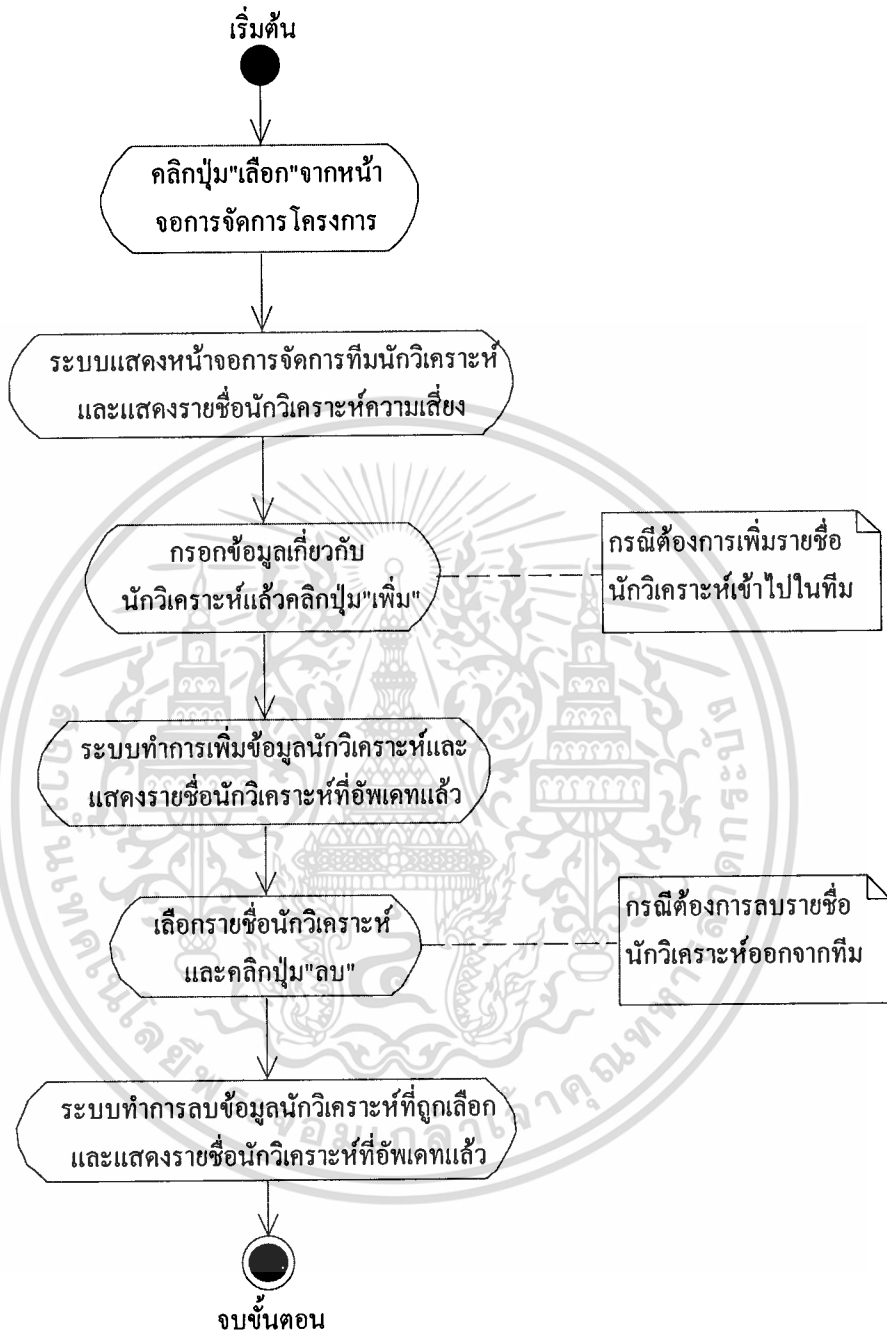
1. คลิกเมนู “วิเคราะห์ความเสี่ยง”
2. ระบบแสดงหน้าจอผลการวิเคราะห์ความเสี่ยง และแสดงรายชื่อโครงการ
3. คลิกปุ่มสร้างโครงการใหม่
4. แสดงหน้าจอสร้างโครงการใหม่
5. กรอกข้อมูลเกี่ยวกับโครงการและคลิกปุ่มตกลง
6. ระบบแสดงรายชื่อโครงการที่อัพเดทแล้ว
7. คลิกเลือกโครงการที่ต้องการลบและคลิกปุ่มลบ
8. ระบบตรวจสอบผู้ใช้งานว่ามีสิทธิลบโครงการหรือไม่ ถ้าผู้ใช้งานไม่มีสิทธิลบโครงการจะมีความแจ้งเตือนว่าไม่มีสิทธิในการลบจางนั้นระบบจะกลับไปยังหน้าจอการวิเคราะห์ความเสี่ยง และแสดงรายชื่อโครงการ





รูปที่ 3.11 Sequence Diagram : Manage Analyst Team

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



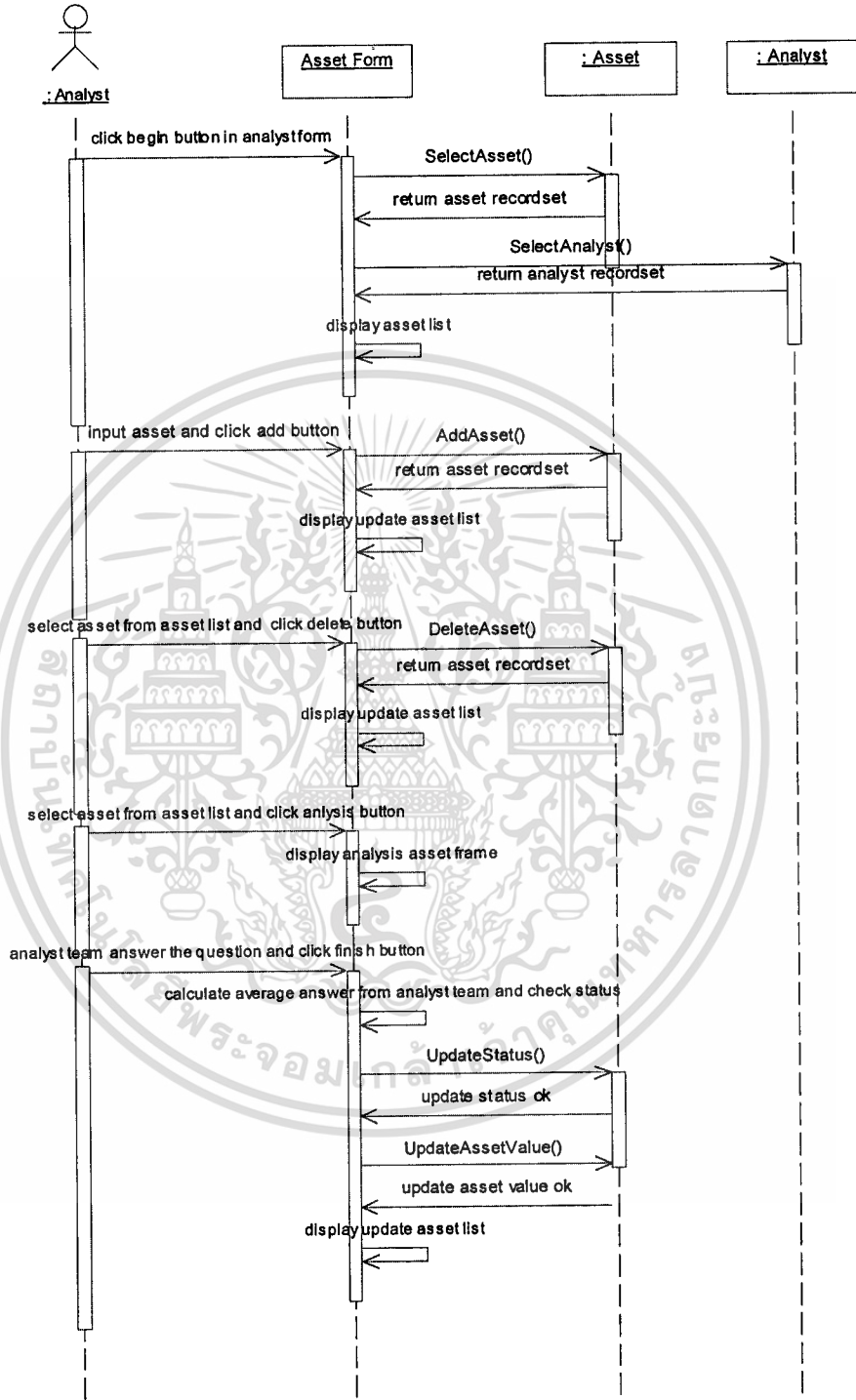
รูปที่ 3.12 Activity Diagram : Manage Analyst Team

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Manage Analyst Team สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.12 โดยมีขั้นตอนดังต่อไปนี้

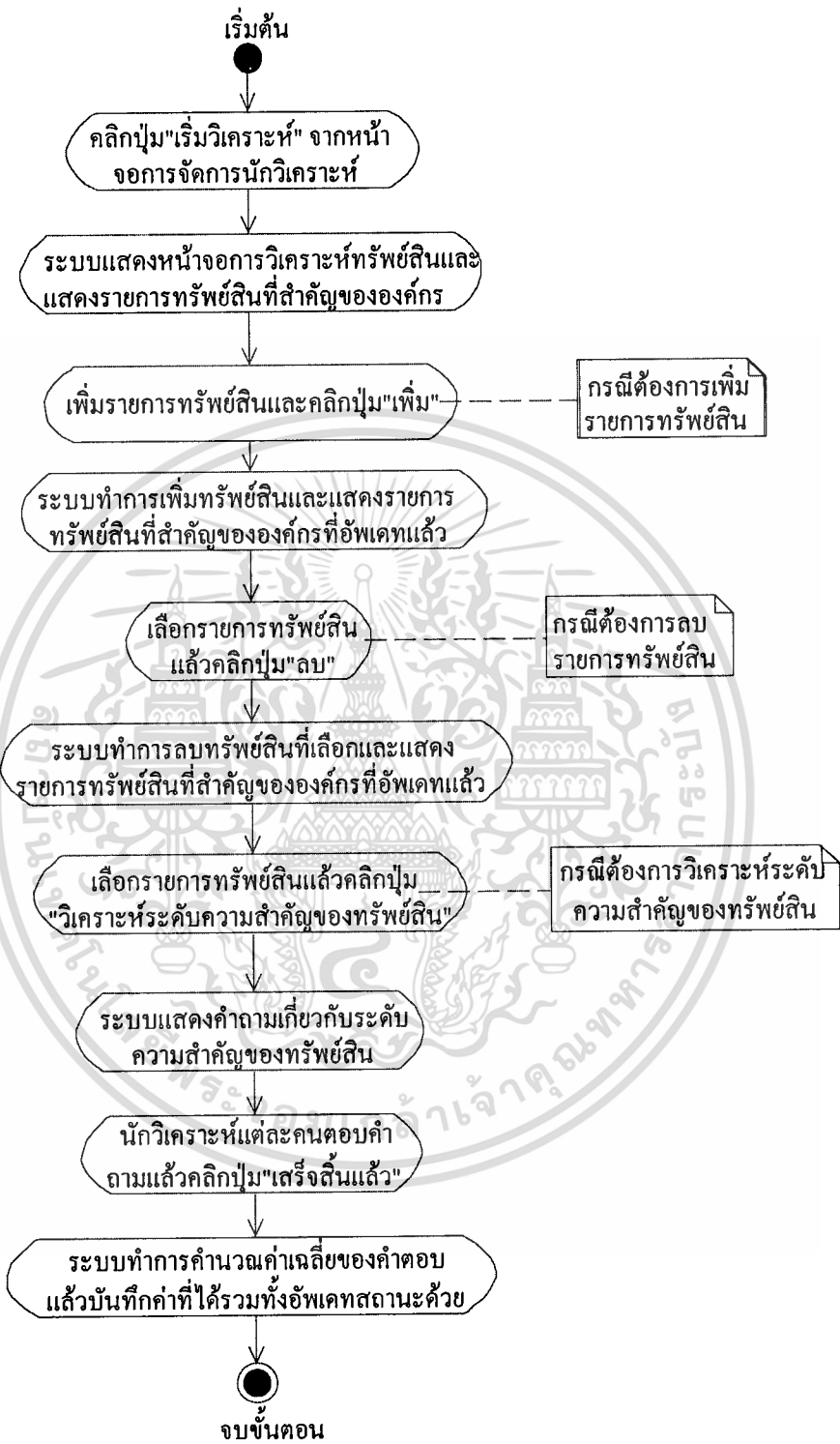
1. คลิกปุ่ม “เลือก” จากหน้าจอการจัดการโครงการ
2. ระบบแสดงหน้าจอการจัดการทีมนักวิเคราะห์และแสดงรายชื่อนักวิเคราะห์ความเสี่ยง
3. กรอกข้อมูลเกี่ยวกับนักวิเคราะห์แล้วคลิกปุ่ม “เพิ่ม” โดยทำในกรณีที่ต้องการเพิ่มรายชื่อนักวิเคราะห์เข้าไปในทีม
4. ระบบจะทำการเพิ่มข้อมูลนักวิเคราะห์และแสดงรายชื่อนักวิเคราะห์ที่อัปเดตแล้ว
5. ในกรณีที่ต้องการลบรายชื่อนักวิเคราะห์ออกจากทีมให้เลือกรายชื่อนักวิเคราะห์และคลิกปุ่ม “ลบ”
6. ระบบทำการลบข้อมูลนักวิเคราะห์ที่ถูกเลือกและแสดงรายชื่อนักวิเคราะห์ที่อัปเดตแล้ว





รูปที่ 3.13 Sequence Diagram : Analyze Asset

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

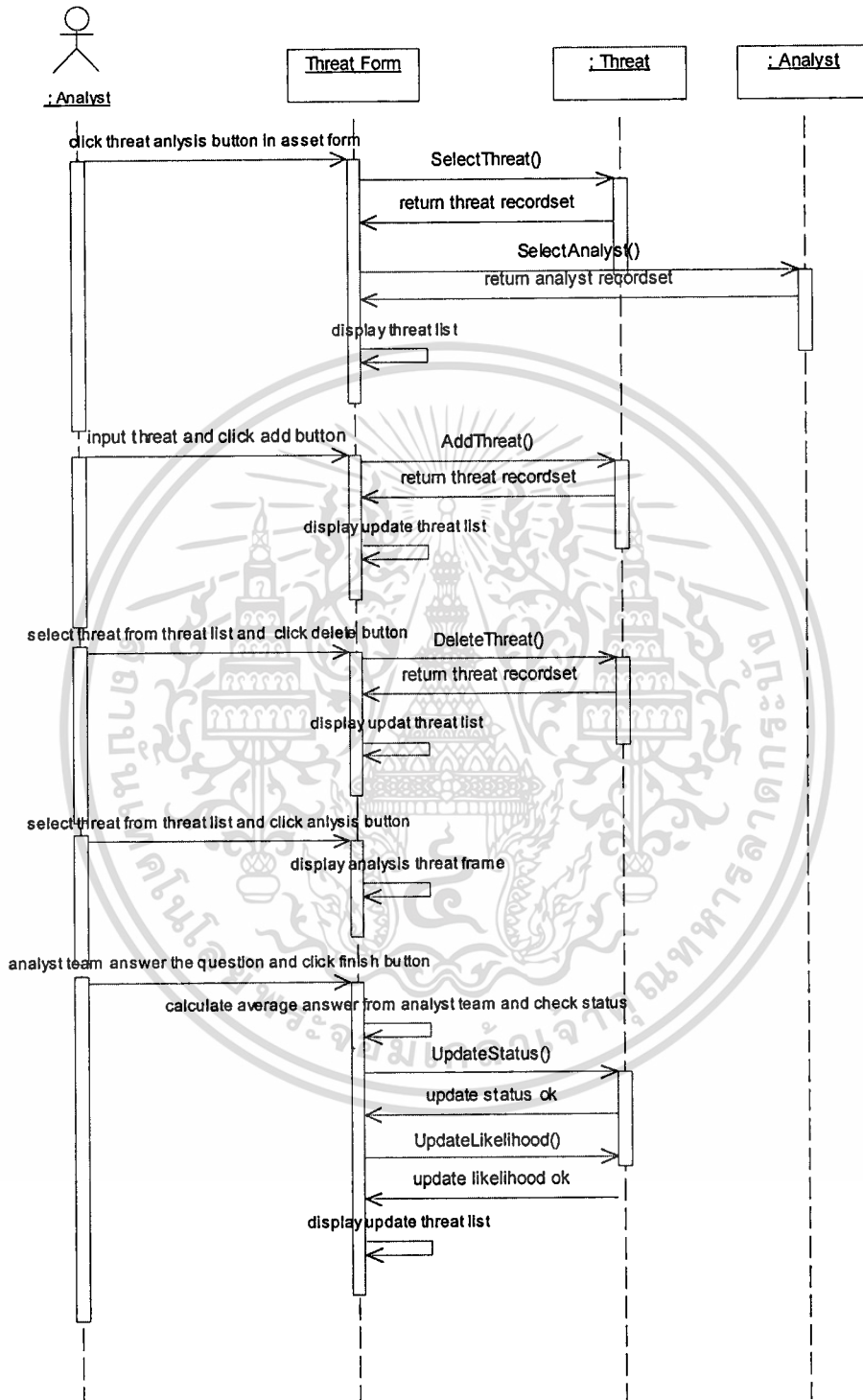


รูปที่ 3.14 Activity Diagram : Analyze Asset

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

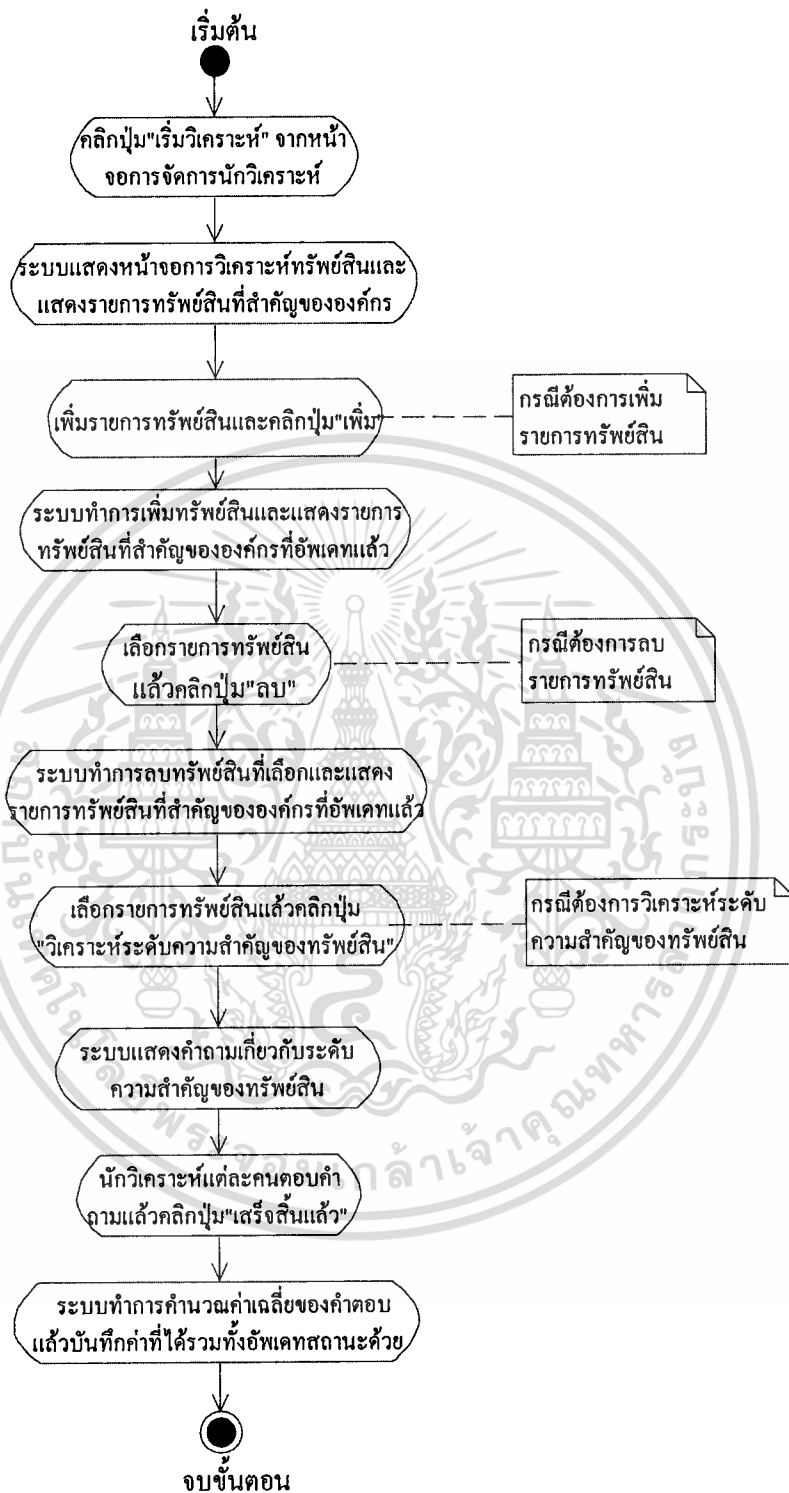
ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Analyze Asset สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.14 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกปุ่ม “เริ่มวิเคราะห์” จากหน้าจอการจัดการนักวิเคราะห์
2. ระบบแสดงหน้าจอการวิเคราะห์ทรัพย์สินและแสดงรายการทรัพย์สินที่สำคัญขององค์กร
3. ในกรณีที่ต้องการเพิ่มรายการทรัพย์สิน สามารถทำได้โดยคลิกปุ่ม “เพิ่ม”
4. ระบบทำการเพิ่มทรัพย์สินและแสดงรายการทรัพย์สินที่สำคัญขององค์กรที่อัปเดตแล้ว
5. ในกรณีที่ต้องการลบรายการทรัพย์สิน ให้เลือกรายการทรัพย์สินแล้วคลิกปุ่ม “ลบ”
6. ระบบทำการลบทรัพย์สินที่จะเลือกและแสดงรายการทรัพย์สินที่สำคัญขององค์กรที่อัปเดตแล้ว
7. ในกรณีที่ต้องการวิเคราะห์ระดับความสำคัญของทรัพย์สิน ให้เลือกรายการทรัพย์สินแล้วคลิกปุ่ม “วิเคราะห์ระดับความสำคัญของทรัพย์สิน”
8. ระบบแสดงคำถามเกี่ยวกับระดับความสำคัญของทรัพย์สิน
9. นักวิเคราะห์แต่ละคนตอบคำถามแล้วคลิกปุ่ม “เสร็จสิ้นแล้ว”
10. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัปเดตสถานะด้วย



รูปที่ 3.15 Sequence Diagram : Analyze Threat

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

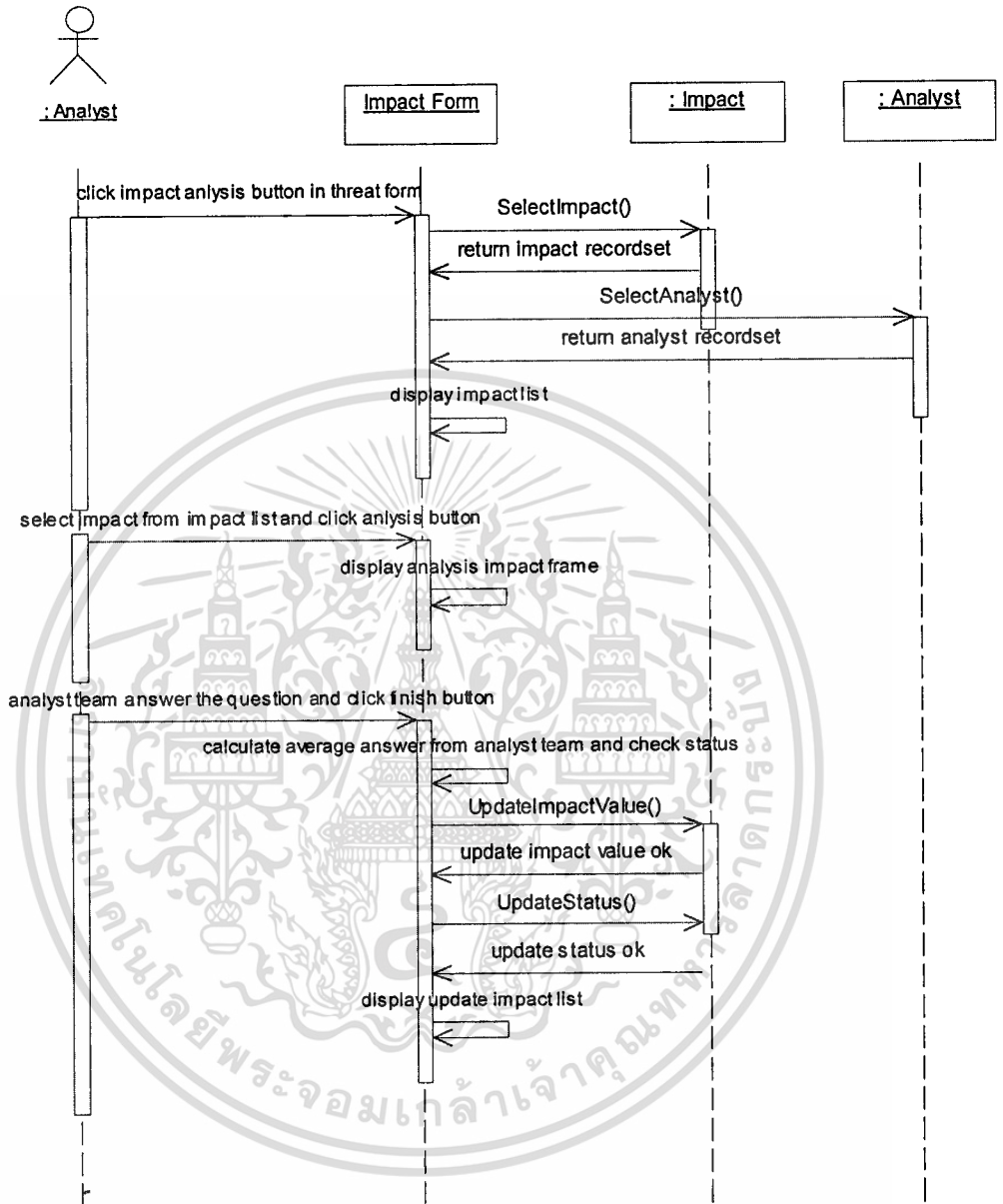


รูปที่ 3.16 Activity Diagram : Analyze Threat

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

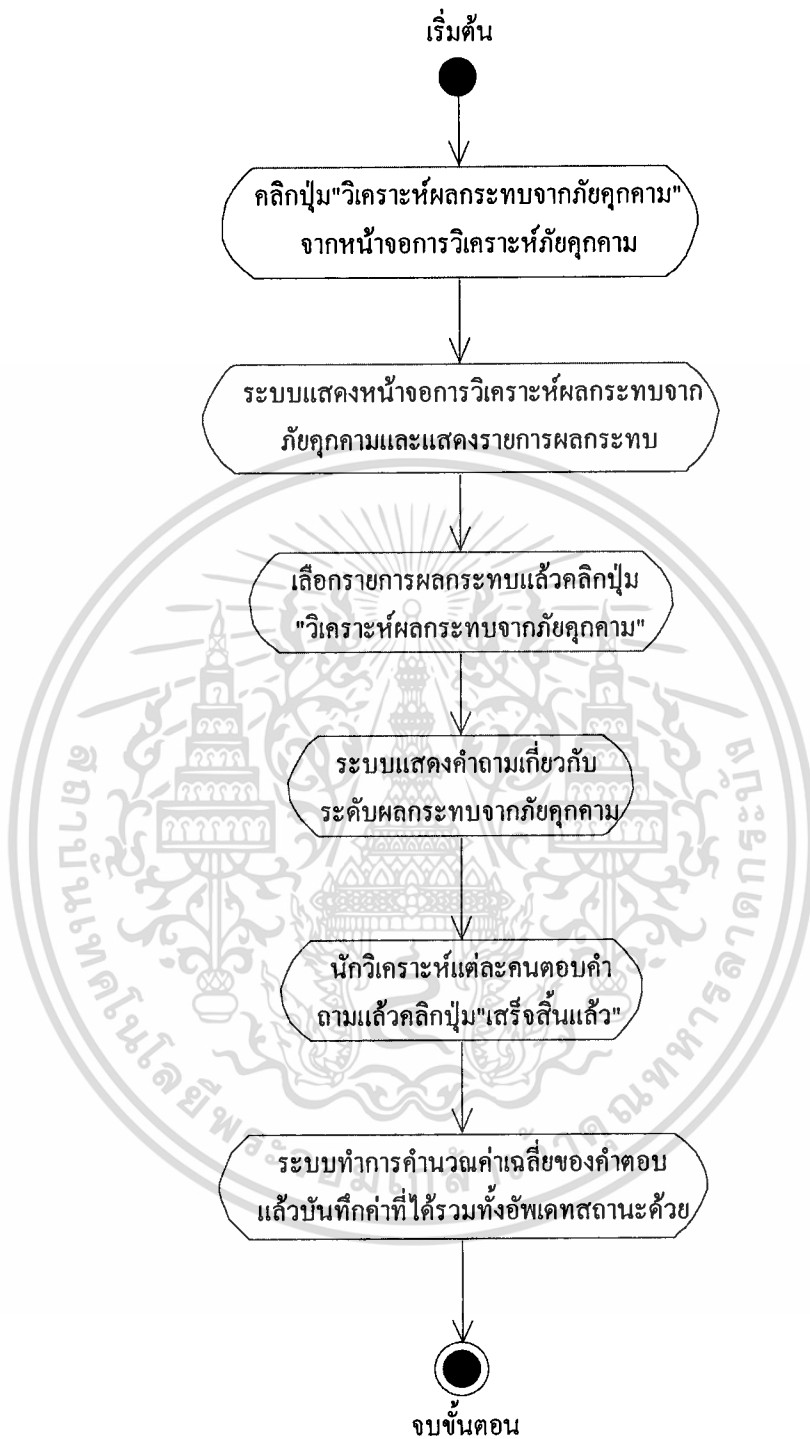
ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Analyze Threat สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.16 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกปุ่ม “เริ่มวิเคราะห์” จากหน้าจอการจัดการนักวิเคราะห์
2. ระบบแสดงหน้าจอการวิเคราะห์ทรัพย์สินและแสดงรายการทรัพย์สินที่สำคัญขององค์กร
3. ในกรณีที่ต้องการเพิ่มรายการทรัพย์สิน ให้คลิกปุ่ม “เพิ่ม”
4. ระบบทำการเพิ่มทรัพย์สินและแสดงรายการทรัพย์สินที่สำคัญขององค์กรที่อัปเดตแล้ว
5. ในกรณีที่ต้องการลบรายการทรัพย์สิน ให้คลิกปุ่ม “ลบ”
6. ระบบทำการลบทรัพย์สินที่เลือกและแสดงรายการทรัพย์สินที่สำคัญขององค์กรที่อัปเดตแล้ว
7. ในกรณีที่ต้องการวิเคราะห์ระดับความสำคัญของทรัพย์สินให้คลิกปุ่ม “วิเคราะห์ระดับความสำคัญของทรัพย์สิน”
8. ระบบแสดงคำถามเกี่ยวกับระดับความสำคัญของทรัพย์สิน
9. นักวิเคราะห์แต่ละคนตอบคำถามแล้วคลิกปุ่ม “เสร็จสิ้นแล้ว”
10. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัปเดตสถานะด้วย



รูปที่ 3.17 Sequence Diagram : Analyze Impact

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

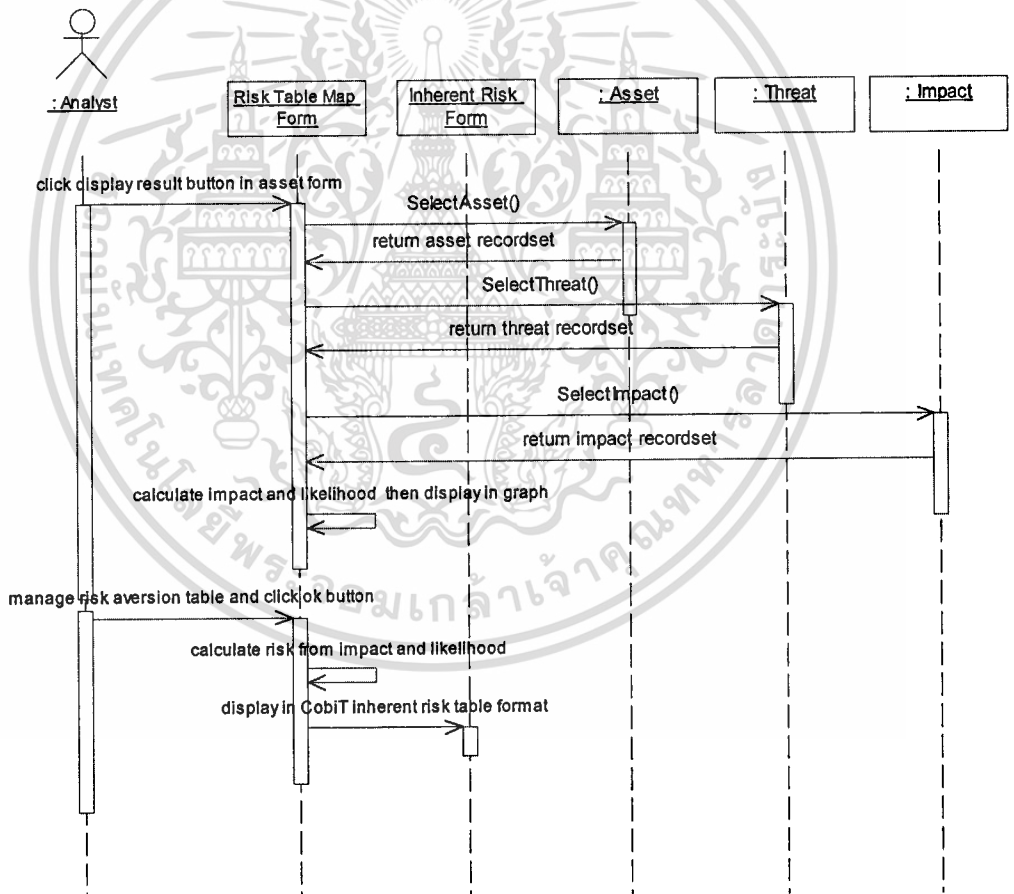


รูปที่ 3.18 Activity Diagram : Analyze Impact

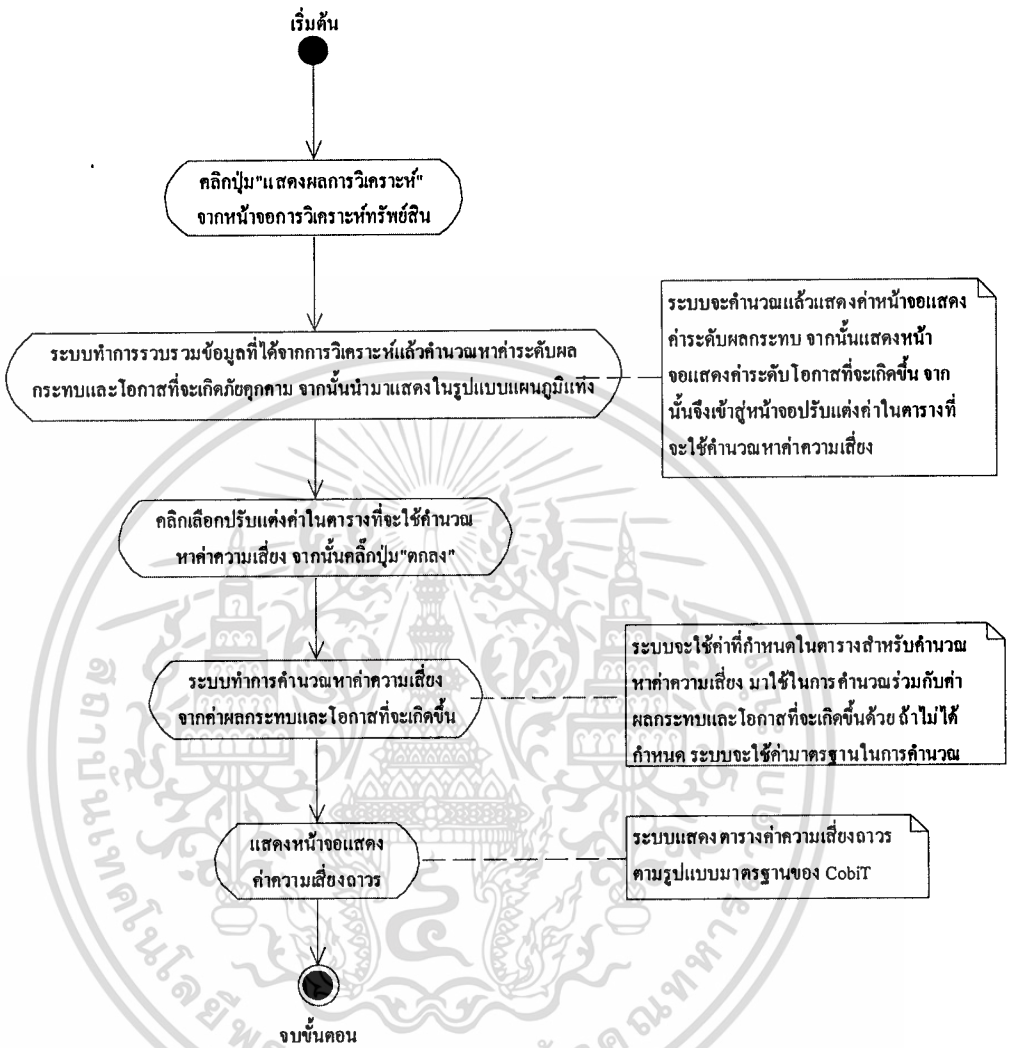
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Analyze Impact สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.18 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกปุ่ม “วิเคราะห์ผลกระทบจากภัยคุกคาม” จากหน้าจอการวิเคราะห์ภัยคุกคาม
2. ระบบแสดงหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคามและแสดงรายการผลกระทบ
3. เลือกรายการผลกระทบแล้วคลิกปุ่ม “วิเคราะห์ผลกระทบจากภัยคุกคาม”
4. ระบบแสดงคำถามเกี่ยวกับระดับผลกระทบจากภัยคุกคาม
5. นักวิเคราะห์แต่ละคนตอบคำถามแล้วคลิกปุ่ม “เสร็จสิ้นแล้ว”
6. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัปเดตสถานะด้วย



รูปที่ 3.19 Sequence Diagram : Analyze Inherent Risk



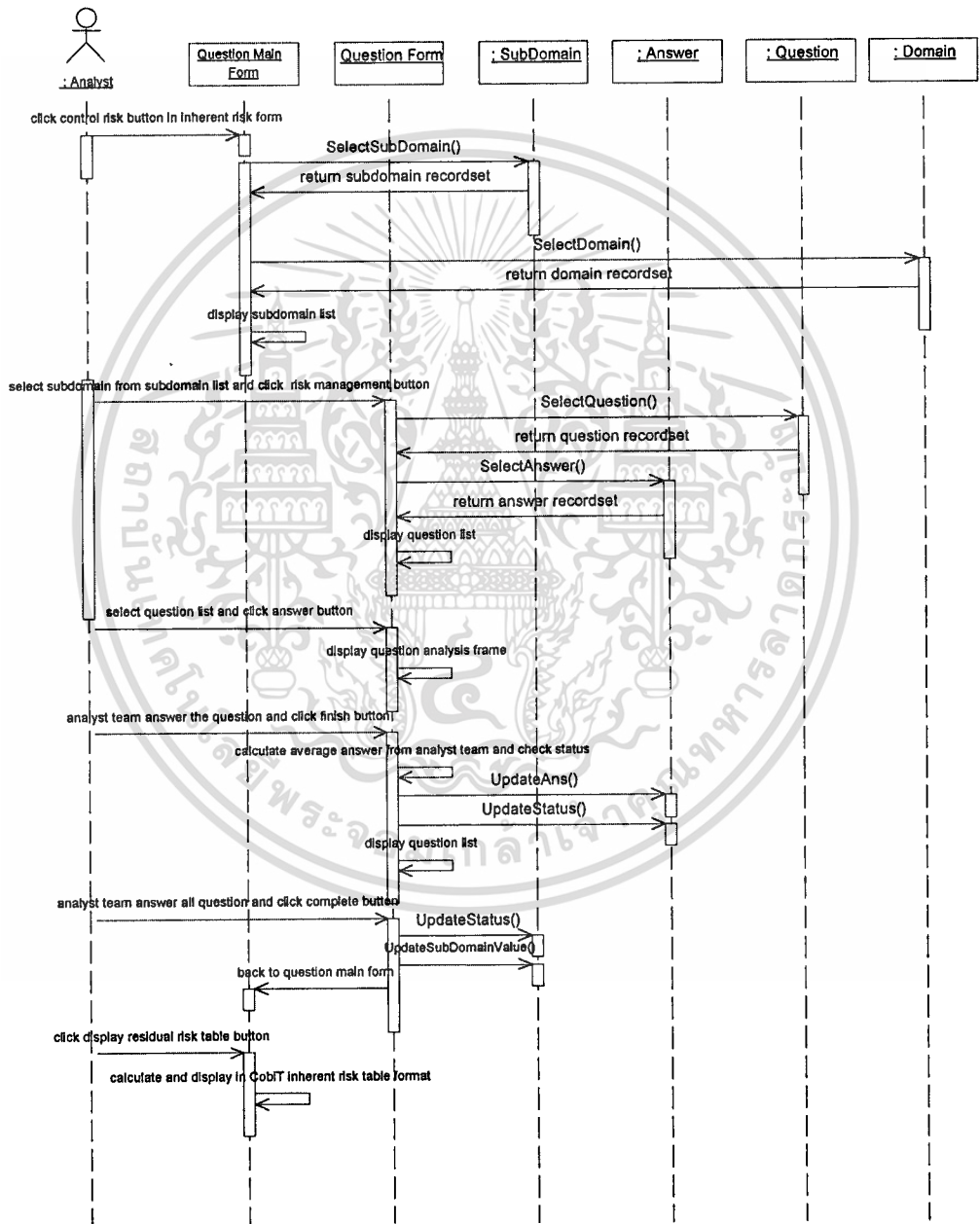
รูปที่ 3.20 Activity Diagram : Analyze Inherent Risk

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Analyze Inherent Risk สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.20 โดยมีขั้นตอนดังต่อไปนี้

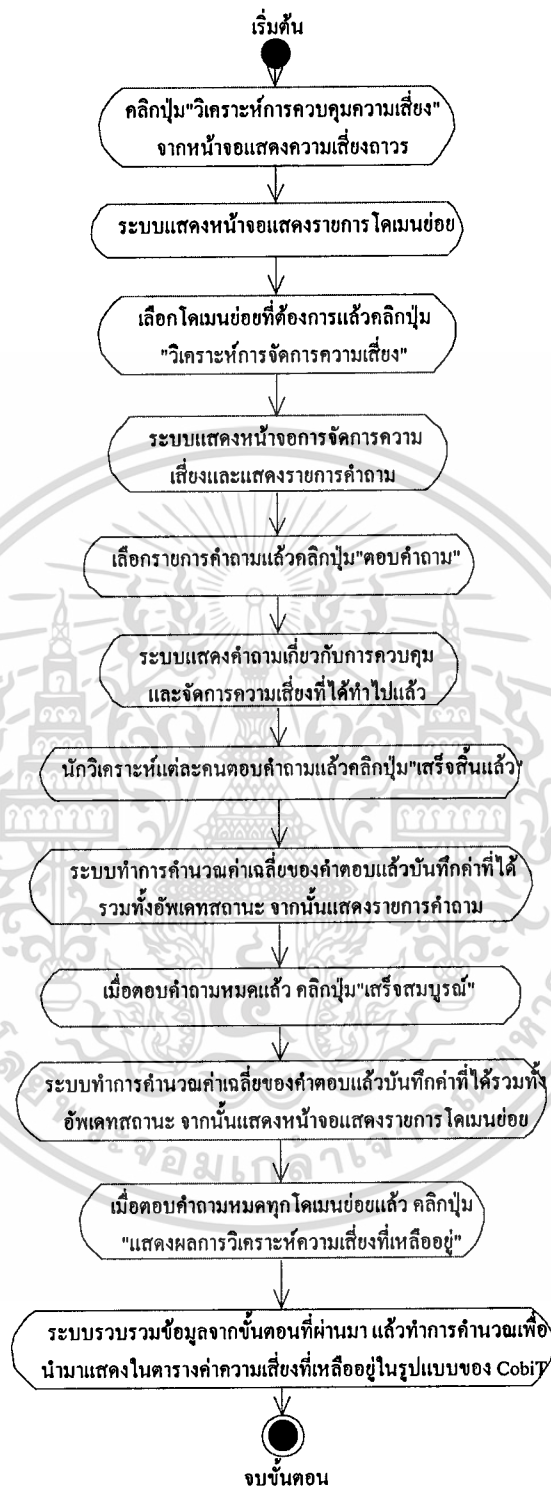
1. คลิกปุ่ม “แสดงผลการวิเคราะห์” จากหน้าจอการวิเคราะห์ทรัพย์สิน
2. ระบบทำการรวบรวมข้อมูลที่ได้จากการวิเคราะห์แล้วคำนวณหาค่าระดับผลกระทบและโอกาสที่จะเกิดภัยคุกคาม จากนั้นนำมาแสดงในรูปแบบแผนภูมิแท่ง
3. คลิกเลือกปรับแต่งค่าในตารางที่จะใช้คำนวณหาค่าความเสี่ยง จากนั้นคลิกปุ่ม “ตกลง”

4. ระบบจะใช้ค่าที่กำหนดในตารางสำหรับคำนวณหาค่าความเสี่ยงมาใช้ในการคำนวณร่วมกับค่าผลกระทบและโอกาสที่จะเกิดขึ้นด้วย ถ้าไม่ได้กำหนดระบบจะใช้ค่ามาตรฐานในการคำนวณ

5. ระบบแสดงตารางค่าความเสี่ยงตามรูปแบบมาตรฐานของ CobiT



รูปที่ 3.21 Sequence Diagram :: Analyze Residual Risk

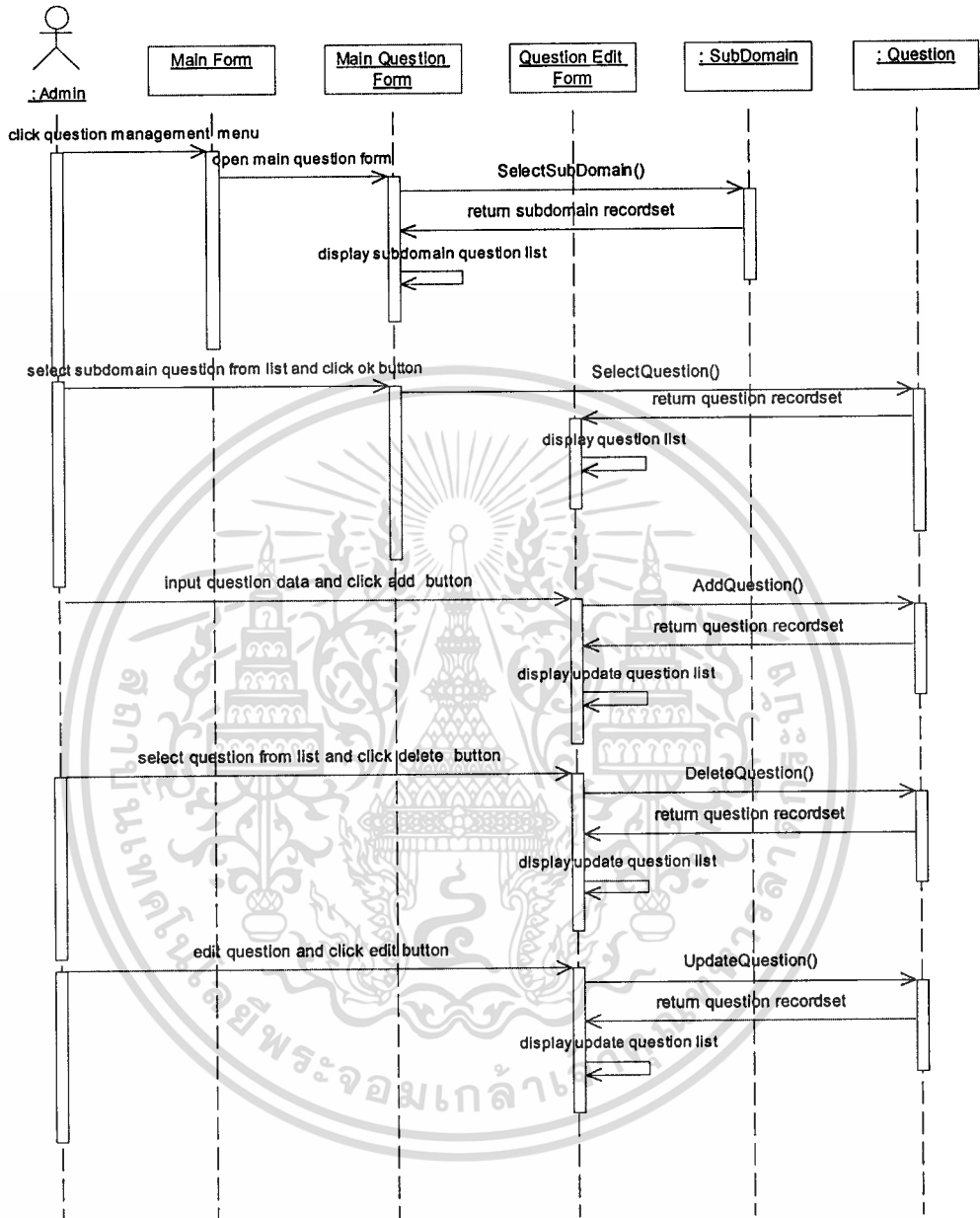


รูปที่ 3.22 Activity Diagram : Analyze Residual Risk

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

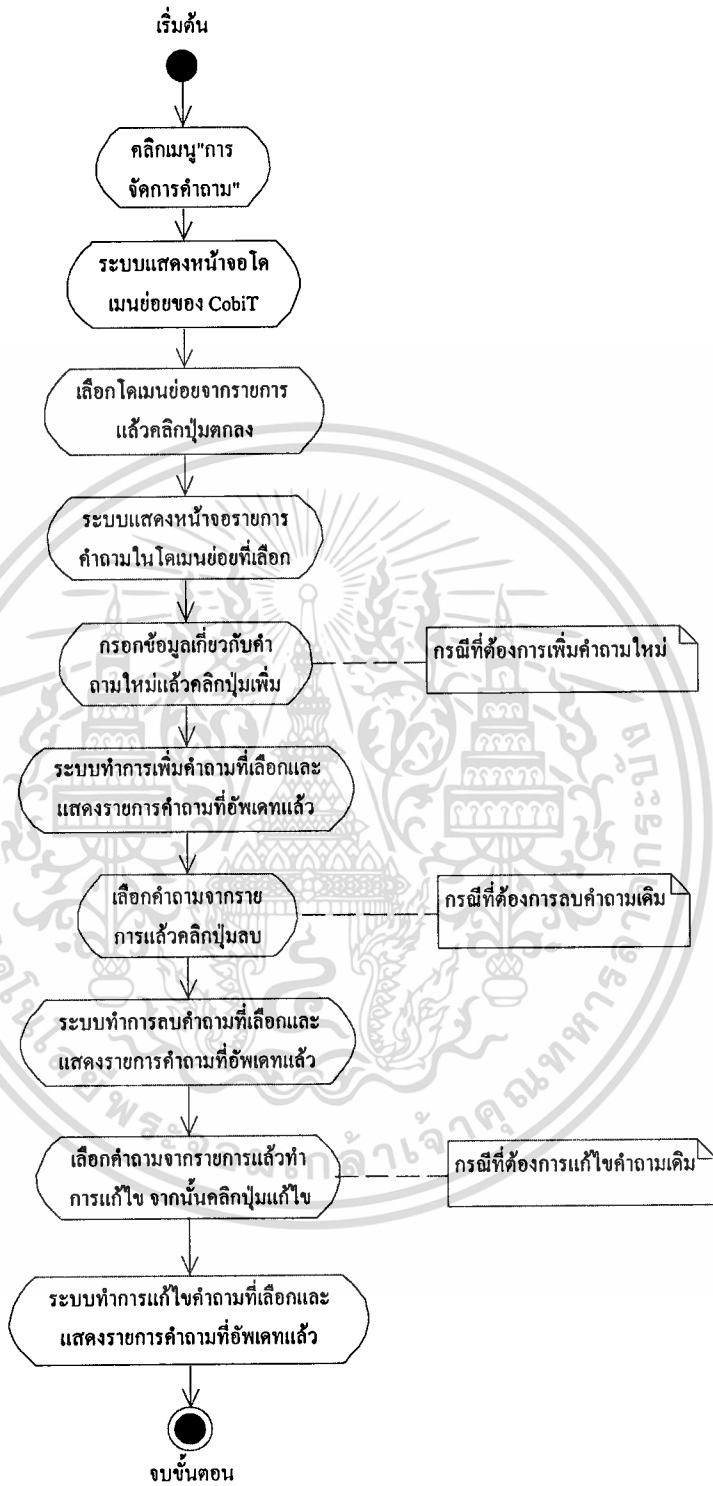
ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Analyze Residual Risk สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.22 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกปุ่ม “วิเคราะห์การควบคุมความเสี่ยง” จากหน้าจอแสดงความเสี่ยงดาว
2. ระบบแสดงหน้าจอแสดงรายการ โดเมนย่อย
3. เลือกโดเมนย่อยที่ต้องการแล้วคลิกปุ่ม “วิเคราะห์การจัดการความเสี่ยง”
4. ระบบแสดงหน้าจอการจัดการความเสี่ยงและแสดงรายการคำถาม
5. เลือกรายการคำถามแล้วคลิกปุ่ม “ตอบคำถาม”
6. ระบบแสดงคำถามเกี่ยวกับการควบคุมและการจัดการความเสี่ยงที่ได้ทำไปแล้ว
7. นักวิเคราะห์แต่ละคนตอบคำถามแล้วคลิกปุ่ม “เสร็จสิ้นแล้ว”
8. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัปเดตสถานะจากนั้นแสดงรายการคำถาม
9. เมื่อตอบคำถามหมดแล้ว คลิกปุ่ม “เสร็จสมบูรณ์”
10. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัปเดตสถานะจากนั้นแสดงหน้าจอแสดงรายการ โดเมนย่อย
11. เมื่อตอบคำถามหมดทุก โดเมนย่อยแล้วคลิกปุ่ม “แสดงผลการวิเคราะห์ความเสี่ยงที่เหลืออยู่”
12. ระบบรวบรวมข้อมูลจากขั้นตอนที่ผ่านมา แล้วทำการคำนวณเพื่อนำมาแสดงในตารางค่าความเสี่ยงที่เหลืออยู่ในรูปแบบของ CobIT



รูปที่ 3.23 Sequence Diagram : Manage Question

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

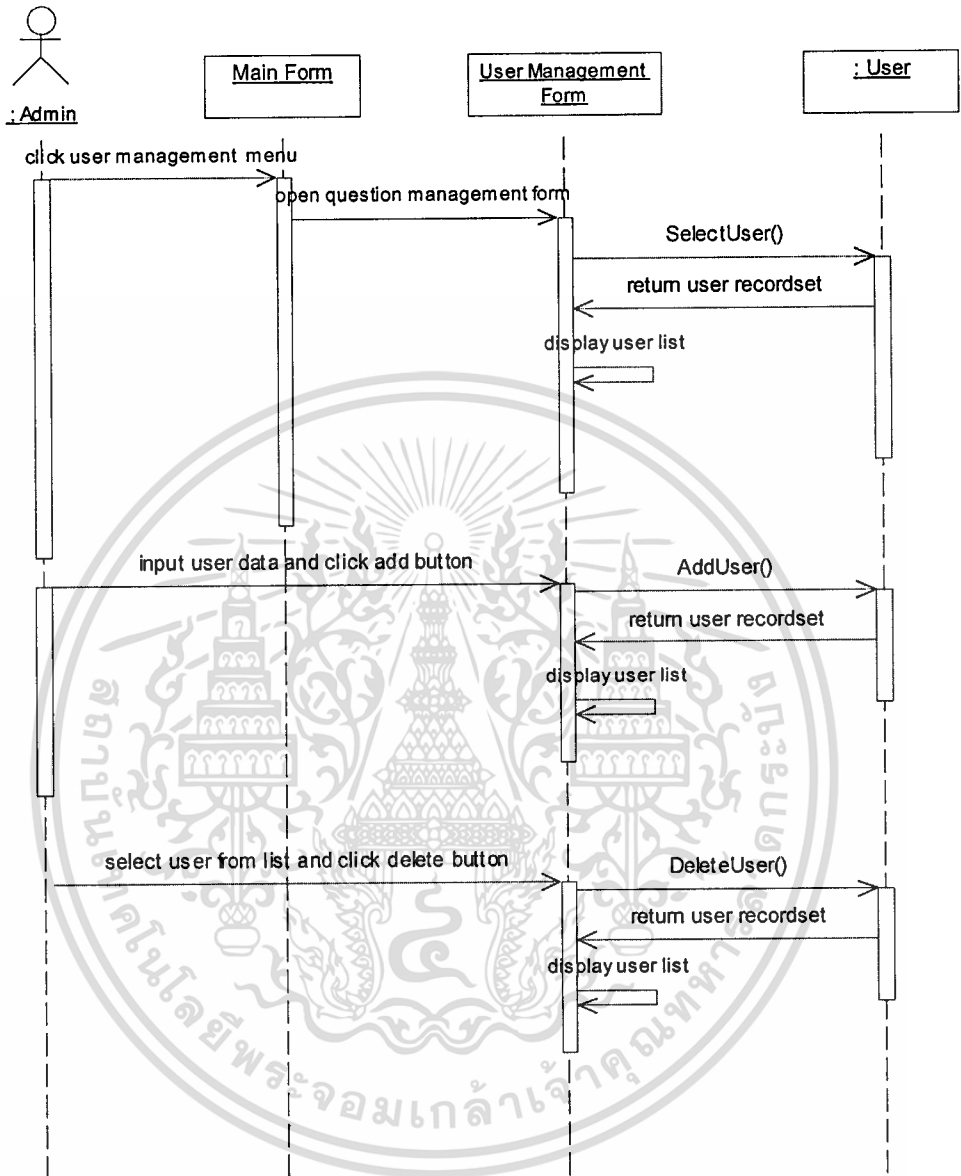


รูปที่ 3.24 Activity Diagram : Manage Question

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Manage Question สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.24 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกเมนู “การจัดการคำถาม”
2. ระบบแสดงหน้าจอ โดเมนย่อยของ CobiT
3. เลือก โดเมนย่อยจากรายการแล้วคลิกปุ่มตกลง
4. ระบบแสดงหน้าจอรายการคำถามใน โดเมนย่อยที่เลือก
5. กรณีที่ต้องการเพิ่มคำถามใหม่ให้กรอกข้อมูลเกี่ยวกับคำถามใหม่แล้วคลิกปุ่มเพิ่ม
6. ระบบทำการเพิ่มคำถามที่เลือกและแสดงรายการคำถามที่อัปเดตแล้ว
7. กรณีที่ต้องการลบคำถามเดิม ให้เลือกคำถามจากรายการแล้วคลิกปุ่มลบ
8. ระบบทำการลบคำถามที่เลือกและแสดงรายการคำถามที่อัปเดตแล้ว
9. กรณีที่ต้องการแก้ไขคำถามเดิม ให้เลือกคำถามจากรายการแล้วทำการแก้ไขจากนั้นคลิกปุ่มแก้ไข
10. ระบบทำการแก้ไขคำถามที่เลือกและแสดงรายการคำถามที่อัปเดตแล้ว



รูปที่ 3.25 Sequence Diagram : Manage User

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.26 Activity Diagram : Manage User

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Manage User สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.26 โดยมีขั้นตอนดังต่อไปนี้

1. คลิกเลือกเมนู “การจัดการผู้ใช้”
2. ระบบแสดงหน้าจอการจัดการผู้ใช้และแสดงรายชื่อผู้ใช้ระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

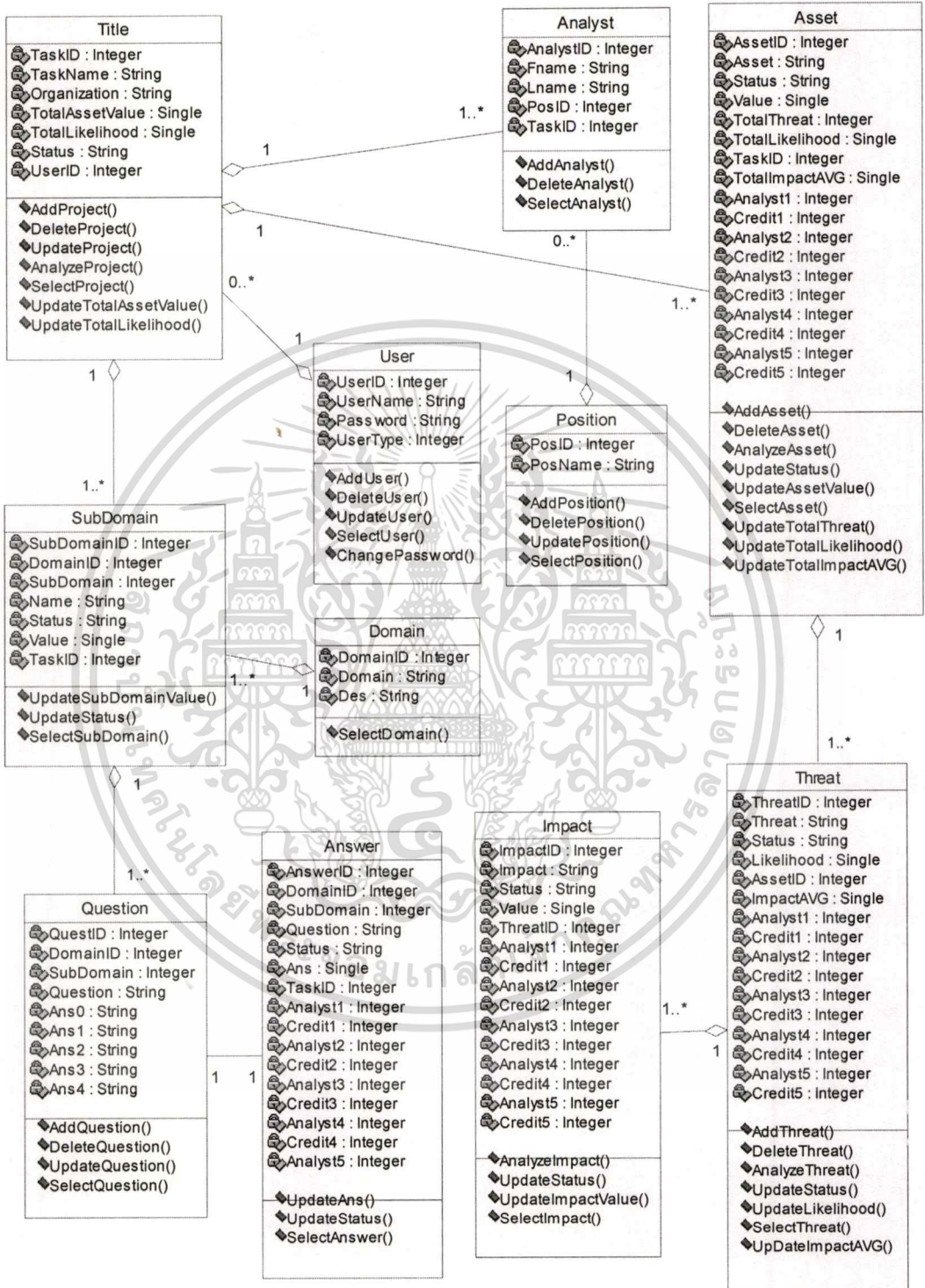
3. กรณีต้องการเพิ่มผู้ใช้ระบบให้เพิ่มข้อมูลเกี่ยวกับผู้ใช้ระบบแล้วคลิกปุ่ม “เพิ่ม”
4. ระบบทำการเพิ่มผู้ใช้และแสดงรายชื่อผู้ใช้ระบบที่อัปเดตแล้ว
5. กรณีต้องการลบผู้ใช้ระบบให้เลือกรายชื่อผู้ใช้ระบบที่ต้องการจะลบแล้วคลิกปุ่ม “ลบ”
6. ระบบทำการลบผู้ใช้ที่เลือกและแสดงรายชื่อผู้ใช้ระบบที่อัปเดตแล้ว

Class Diagram เป็นแผนภาพที่แสดงความสัมพันธ์ของคลาสทั้งหมดที่ควรมีในระบบ ซึ่งจะทำให้เห็นโครงสร้างของระบบด้วย จากการวิเคราะห์ Use Case Diagram ทำให้ได้คลาสรูปพื้นฐานสำหรับระบบวิเคราะห์ความเสี่ยงของสารสนเทศดังต่อไปนี้

- Analyst	หมายถึง	คลาสนักวิเคราะห์ความเสี่ยง
- Answer	หมายถึง	คลาสคำถามและคำตอบที่ใช้ในการวิเคราะห์
- Asset	หมายถึง	คลาสทรัพย์สินที่สำคัญขององค์กร
- Domain	หมายถึง	คลาสโดเมนหลักของ CobiT
- Impact	หมายถึง	คลาสผลกระทบจากภัยคุกคาม
- Position	หมายถึง	คลาสตำแหน่งงานในองค์กร
- Question	หมายถึง	คลาสคำถามเกี่ยวกับการจัดการความเสี่ยง
- SubDomain	หมายถึง	คลาสโดเมนย่อยของ CobiT
- Threat	หมายถึง	คลาสภัยคุกคามต่อทรัพย์สิน
- Title	หมายถึง	คลาสโครงการวิเคราะห์ความเสี่ยง
- User	หมายถึง	คลาสผู้ใช้งานระบบ

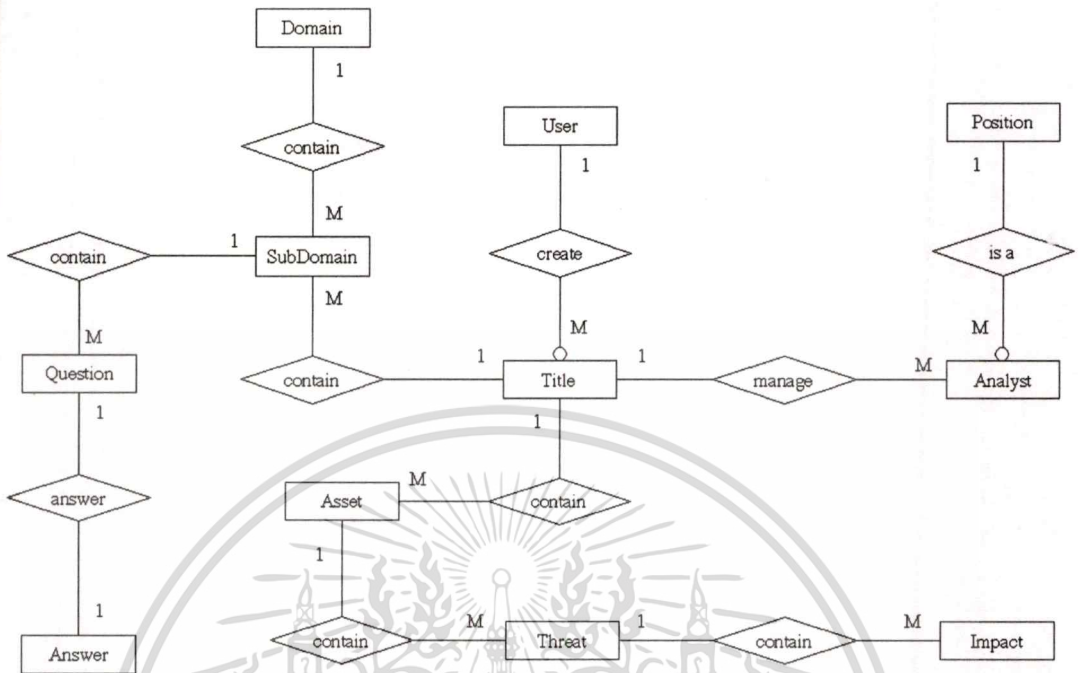
ความสัมพันธ์ของแต่ละคลาสภายในระบบสามารถแสดงด้วย Class Diagram ดังรูปที่ 3.27 จากรูป Class Diagram ของระบบวิเคราะห์ความเสี่ยงของสารสนเทศนี้ แสดงให้เห็นความสัมพันธ์ของคลาสต่างๆ ที่มีในระบบ ซึ่งมีการกำหนดแอตทริบิวต์ และเมธอด ของแต่ละคลาส

นอกจาก Class Diagram แล้ว ยังสามารถอธิบายได้โดยใช้ ER Diagram ดังรูปที่ 3.28



รูปที่ 3.27 Class Diagram ระบบวิเคราะห์ความถี่ของสารสนเทศ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.28 ER Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

จาก Class Diagram และ ER Diagram สามารถอธิบายความสัมพันธ์ได้ดังนี้

- **User** กับ **Title** มีความสัมพันธ์กันคือ ผู้ใช้ (User) 1 คน สามารถสร้างโครงการ (Title) ได้หลายโครงการหรืออาจไม่สร้างเลยก็ได้ ส่วนโครงการ 1 โครงการต้องถูกสร้างจากผู้ใช้เพียงคนเดียว
- **Title** กับ **Analyst** มีความสัมพันธ์กันคือ โครงการ 1 โครงการ สามารถถูกจัดการวิเคราะห์โดยนักวิเคราะห์อย่างน้อย 1 คน นักวิเคราะห์ 1 คน จัดการวิเคราะห์โครงการได้ที่ละ 1 โครงการ
- **Analyst** กับ **Position** มีความสัมพันธ์กันคือ นักวิเคราะห์ 1 คน เป็นพนักงานในองค์กรที่มีตำแหน่งเพียงตำแหน่งเดียว ตำแหน่ง 1 ตำแหน่ง มีพนักงานได้หลายคน
- **Title** กับ **Asset** มีความสัมพันธ์กันคือ โครงการ 1 โครงการซึ่งเปรียบเสมือนเป็นองค์กร 1 องค์กร มีทรัพย์สินที่สำคัญอย่างน้อย 1 รายการ ทรัพย์สินที่สำคัญขององค์กร 1 รายการ ต้องเป็นทรัพย์สินขององค์กรนั้นองค์กรเดียว
- **Asset** กับ **Threat** มีความสัมพันธ์กันคือ ทรัพย์สิน 1 รายการ จะมีภัยคุกคามอย่างน้อย 1 ภัยคุกคาม ภัยคุกคามต่อทรัพย์สินนั้น 1 ภัยคุกคาม จะเป็นภัยคุกคามต่อทรัพย์สินนั้นเพียงรายการเดียว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **Threat** กับ **Impact** มีความสัมพันธ์กันคือ ภัยคุกคาม 1 ภัยคุกคาม จะมีผลกระทบจากภัยคุกคามอย่างน้อย 1 รายการ ผลกระทบจากภัยคุกคามนั้น 1 รายการ จะเป็นผลกระทบจากภัยคุกคามนั้นเพียงภัยคุกคามเดียว
- **Title** กับ **SubDomain** มีความสัมพันธ์กันคือ โครงการ 1 โครงการซึ่งเปรียบเสมือนเป็นองค์กร 1 องค์กร มีกระบวนการดำเนินงานย่อยหรือโดเมนย่อยอย่างน้อย 1 โดเมนย่อย โดเมนย่อยของโครงการนั้น 1 โดเมนย่อย จะเป็นโดเมนย่อยของโครงการนั้นโครงการเดียว
- **Domain** กับ **SubDomain** มีความสัมพันธ์กันคือ โดเมน 1 โดเมน มีโดเมนย่อยอย่างน้อย 1 โดเมนย่อย โดเมนย่อยของโดเมนนั้น 1 โดเมน เป็น โดเมนย่อยของโดเมนนั้น โดเมนเดียว
- **SubDomain** กับ **Question** มีความสัมพันธ์กันคือ โดเมนย่อย 1 โดเมนย่อย มีคำถามเกี่ยวกับการควบคุมความเสี่ยงอย่างน้อย 1 คำถาม คำถามของโดเมนย่อยนั้น 1 คำถาม เป็น คำถามของโดเมนย่อยนั้น โดเมนย่อยเดียว
- **Question** กับ **Answer** มีความสัมพันธ์กันคือ คำถาม 1 คำถาม มีคำตอบได้คำตอบเดียว คำตอบของคำถามนั้น 1 คำตอบ เป็นตอบของคำถามนั้นคำถามเดียว

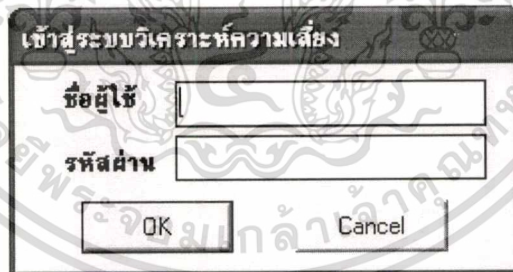
## บทที่ 4

### การใช้งานระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

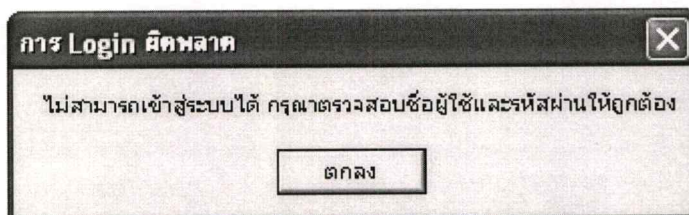
#### 4.1 การเข้าสู่ระบบ

จากหน้าจอคอมพิวเตอร์ ดับเบิลคลิกไอคอน “ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ” ระบบจะแสดงหน้าจอเข้าสู่ระบบดังรูปที่ 4.1 ถ้าผู้ใช้กรอกชื่อผู้ใช้หรือรหัสผ่านไม่ถูกต้อง ระบบจะแสดงข้อความดังรูปที่ 4.2 ส่วนรูปที่ 4.3 คือหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ โดยจะแสดงตามสิทธิของผู้ใช้ระบบแต่ละคน เมนูส่วนไหนที่ผู้ใช้ไม่มีสิทธิจะไม่สามารถคลิกเข้าไปได้

เมื่อเริ่มเข้าสู่ระบบ จะเข้ามาที่เมนูหลักของระบบ ประกอบด้วย 5 ส่วนหลัก คือ การวิเคราะห์ความเสี่ยง แสดงผลวิเคราะห์ความเสี่ยง การจัดการคำถาม การจัดการผู้ใช้งาน การเปลี่ยนรหัสผ่าน และออกจากระบบ ซึ่งผู้ใช้สามารถเข้าไปยังส่วนต่างๆ ได้โดยการคลิกปุ่มที่หน้าจอหรือคลิกที่เมนูข้างบน

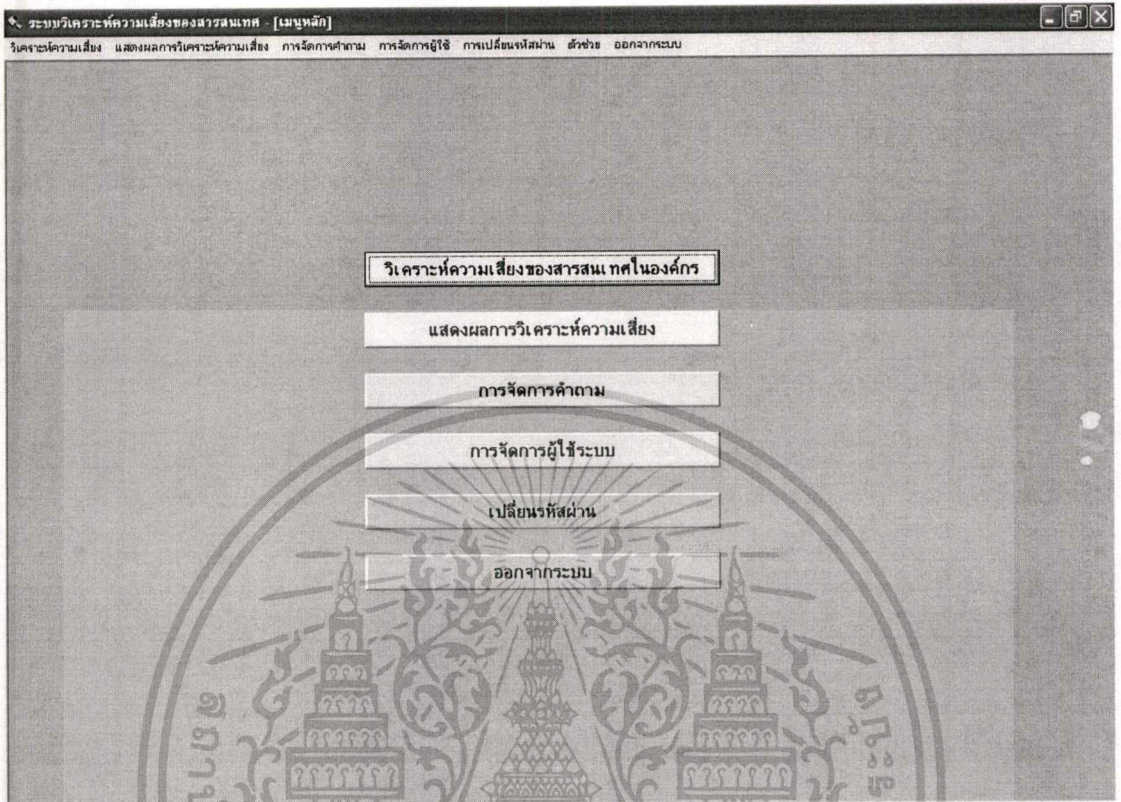


รูปที่ 4.1 หน้าจอเข้าสู่ระบบ



รูปที่ 4.2 เข้าสู่ระบบผิดพลาด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.3 หน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

#### 4.2 การเปลี่ยนรหัสผ่าน

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มเปลี่ยนรหัสผ่าน หลังจากนั้นระบบจะแสดงหน้าจอเปลี่ยนรหัสผ่านดังรูปที่ 4.4

รูปที่ 4.4 หน้าจอเปลี่ยนรหัสผ่าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 4.5 เป็นข้อความที่แสดงเมื่อผู้ใช้ใส่รหัสผ่านใหม่และยืนยันรหัสผ่านไม่ตรงกัน ส่วนรูปที่ 4.6 เป็นข้อความที่แสดงเมื่อระบบได้ทำการเปลี่ยนรหัสผ่านให้เรียบร้อยแล้ว



รูปที่ 4.5 ข้อความยืนยันรหัสผ่าน ไม่ถูกต้อง



รูปที่ 4.6 ข้อความเปลี่ยนรหัสผ่านเรียบร้อยแล้ว

#### 4.3 การวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กร

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กรหรือคลิกการวิเคราะห์ความเสี่ยงที่เมนูข้างบน หลังจากนั้นระบบจะแสดงหน้าจอการจัดการโครงการดังรูปที่ 4.7 ซึ่งจะเป็นการแสดงรายการของโครงการวิเคราะห์ความเสี่ยงทั้งหมดทั้งที่ได้ทำการวิเคราะห์เสร็จสิ้นไปแล้วและยังไม่เสร็จ

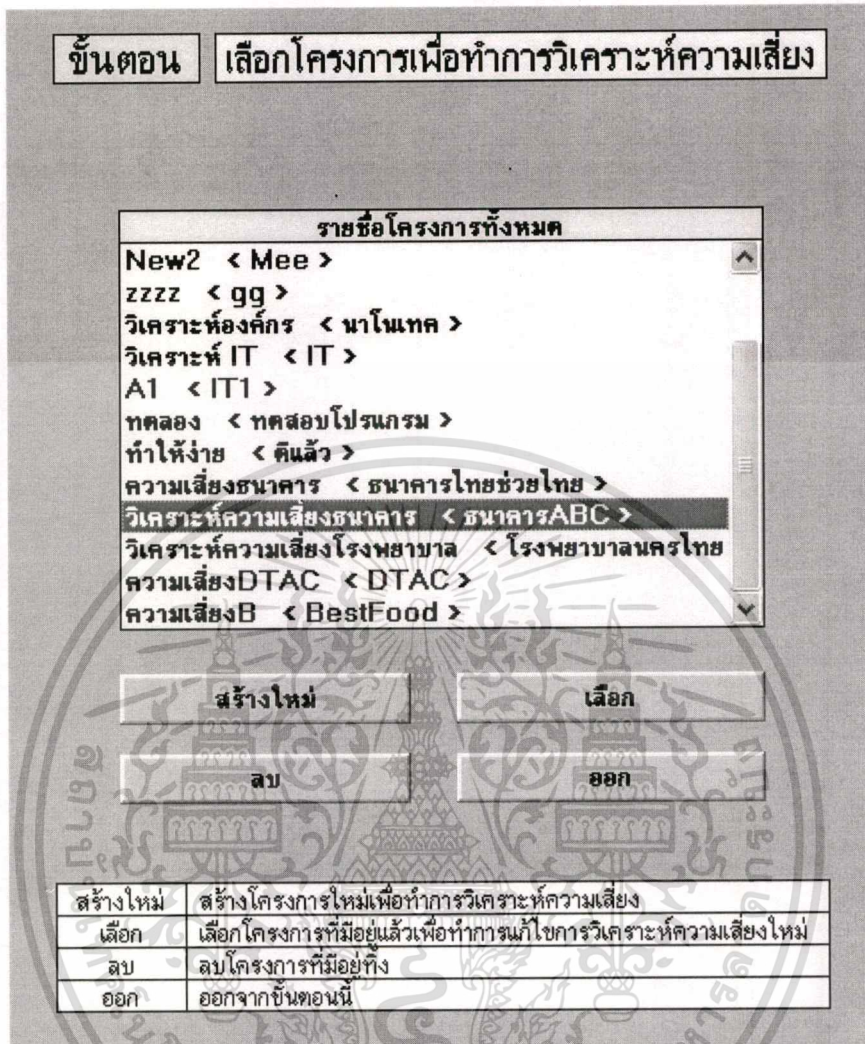
##### 4.3.1 การจัดการโครงการ

กรณีต้องการสร้างโครงการใหม่ ผู้ใช้สามารถคลิกปุ่มสร้างใหม่ ซึ่งจะแสดงหน้าจอการเพิ่มโครงการใหม่ ดังรูป 4.8 จากนั้นกรอกชื่อโครงการและชื่อองค์กรและคลิกปุ่มตกลง ระบบจะทำการเพิ่มโครงการใหม่แล้วกลับไปหน้าจอการจัดการโครงการ

กรณีต้องการลบโครงการ ผู้ใช้สามารถเลือกโครงการที่ต้องการลบแล้วคลิกปุ่มลบ ระบบจะแสดงข้อความยืนยันการลบโครงการดังรูป 4.9 เมื่อผู้ใช้ยืนยันระบบจะทำการลบโครงการที่เลือกและกลับไปหน้าจอการจัดการโครงการ

กรณีต้องการเริ่มทำการวิเคราะห์ความเสี่ยง ผู้ใช้สามารถเลือกโครงการและคลิกปุ่มเลือกได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.7 หน้าจอการจัดการ โครงการ

การเพิ่มโครงการใหม่

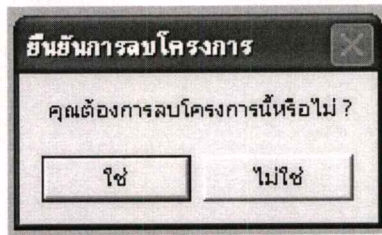
ชื่อโครงการ

องค์กร

ตกลง      ยกเลิก

รูปที่ 4.8 หน้าจอการเพิ่มโครงการใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.9 ข้อความยืนยันการลบโครงการ

#### 4.2.2 การจัดการทีมนักวิเคราะห์

เมื่อผู้ใช้คลิกเลือกโครงการที่จะทำการวิเคราะห์แล้ว ระบบจะแสดงหน้าจอการจัดการทีมนักวิเคราะห์ดังรูปที่ 4.10

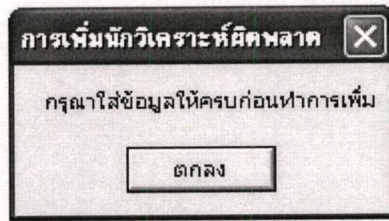
กรณีต้องการเพิ่มรายชื่อนักวิเคราะห์เข้าทีม ผู้ใช้สามารถใส่ ชื่อ นามสกุล ตำแหน่งงาน แล้วคลิกปุ่มเพิ่มผู้วิเคราะห์ ถ้าใส่ข้อมูลไม่ครบระบบจะแสดงข้อความเตือนดังรูปที่ 4.11

รายชื่อทีมนักวิเคราะห์ความเสี่ยง		
ชื่อ	นามสกุล	ตำแหน่ง
เจียงชัย	คงดี	พนักงานการเงิน
พรพรวณ	วงกลม	พนักงานบัญชี
สามารถ	แสนใจ	นักพัฒนาระบบ

ชื่อ	นามสกุล	ตำแหน่ง
		[ ตำแหน่งในองค์กร ]

รูปที่ 4.10 หน้าจอการจัดการทีมนักวิเคราะห์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.11 ข้อความเตือนให้ใส่ข้อมูลให้ครบก่อนคลิกปุ่มเพิ่มผู้วิเคราะห์

กรณีต้องการลบรายชื่อนักวิเคราะห์ออกจากทีม ผู้ใช้สามารถเลือกรายชื่อนักวิเคราะห์ที่ต้องการลบแล้วคลิกปุ่มลบ ระบบจะแสดงข้อความยืนยันการลบ เมื่อผู้ใช้ยืนยันระบบจะทำการลบรายชื่อนักวิเคราะห์ที่เลือกออกจากทีม

กรณีต้องการกลับไปหน้าการจัดการโครงการ ผู้ใช้สามารถคลิกปุ่มยกเลิกเพื่อกลับไปยังหน้าการจัดการโครงการได้

กรณีเลือกทีมนักวิเคราะห์เสร็จแล้ว ต้องการเริ่มวิเคราะห์ความเสี่ยง คลิกปุ่มเริ่มทำการวิเคราะห์ความเสี่ยง ระบบจะแสดงหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร ดังรูป 4.12

#### 4.3.3 การวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร

ระบบแสดงหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร ดังรูป 4.12 ซึ่งหน้าจอนี้จะเป็นการเพิ่ม ลบและวิเคราะห์ระดับความสำคัญของทรัพย์สิน

กรณีต้องการเพิ่มรายการทรัพย์สิน ผู้ใช้สามารถใส่รายการทรัพย์สิน แล้วคลิกปุ่มเพิ่มรายการทรัพย์สิน ถ้าใส่ข้อมูลไม่ครบระบบจะแสดงข้อความเตือนลักษณะเดียวกับรูป 4.11

กรณีต้องการลบรายการทรัพย์สิน ผู้ใช้สามารถเลือกรายการทรัพย์สินที่ต้องการลบแล้วคลิกปุ่มลบ ระบบจะแสดงข้อความยืนยันการลบ เมื่อผู้ใช้ยืนยัน ระบบจะทำการลบรายการทรัพย์สินที่เลือกออกไป

กรณีต้องการวิเคราะห์ระดับความสำคัญของทรัพย์สิน สามารถเลือกรายการทรัพย์สินที่ต้องการแล้วคลิกปุ่มวิเคราะห์ระดับความสำคัญของทรัพย์สิน ระบบจะแสดงหน้าจอ ดังรูป 4.13 ซึ่งให้นักวิเคราะห์แต่ละคนตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญของทรัพย์สิน โดยจะให้มีการกำหนดระดับความมั่นใจในการตอบด้วย แสดงในรูป 4.14 เมื่อนักวิเคราะห์ตอบหมดทุกคนแล้วจะสามารถคลิกปุ่มเสร็จสิ้นได้ ระบบจะทำการหาค่าเฉลี่ยโดยมีการนำระดับความมั่นใจในการตอบมาคิดด้วย จากนั้นระบบจะอัปเดตสถานะและบันทึกข้อมูล

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ - [การวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร]

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการค่าตาม การจัดการผู้ใช้ การเปลี่ยนแปลงผ่าน ผู้ช่วย ออกจากระบบ

**ขั้นตอน** **ระบุและวิเคราะห์ภัยการทรัพย์สินที่สำคัญขององค์กร**

ผลการวิเคราะห์ระดับความสำคัญของรายการทรัพย์สินในองค์กร									
ทรัพย์สิน	สถานะ	ระดับความสำคัญ	เรียงข้อ	ความมั่นใจ	พรพรหม	ความมั่นใจ	สามารถ	ความ	
ข้อมูลส่วนตัวลูกค้า	เสร็จสิ้นแล้ว	2.1666667	2		2	3		1	2
บัญชีเงินฝาก	เสร็จสิ้นแล้ว	3.2857143	3		2	3		3	4
เงินในตู้เซฟ	เสร็จสิ้นแล้ว	4	4		3	4		3	4
เครื่องเซิร์ฟเวอร์	เสร็จสิ้นแล้ว	3	3		2	3		3	3
ข้อมูลพนักงาน	ยังไม่ได้ทำ	0			0			0	

ทรัพย์สินที่วิเคราะห์ที่ ----- โครงการ วิเคราะห์ความเสี่ยงธนาคาร

ผู้วิเคราะห์ที่ ----- องค์กร ธนาคารABC

เหมือนรายการทรัพย์สินที่สำคัญ

ลบรายการ

วิเคราะห์ระดับความสำคัญของทรัพย์สิน

วิเคราะห์ที่ถูกลบก่อนทรัพย์สิน

แก้ไข

ยกเลิก

แสดงผลการวิเคราะห์

รูปที่ 4.12 หน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ - [การวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร]

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการค่าตาม การจัดการผู้ใช้ การเปลี่ยนแปลงผ่าน ผู้ช่วย ออกจากระบบ

**ขั้นตอน** **ระบุและวิเคราะห์ภัยการทรัพย์สินที่สำคัญขององค์กร**

ผลการวิเคราะห์ระดับความสำคัญของรายการทรัพย์สินในองค์กร									
ทรัพย์สิน	สถานะ	ระดับความสำคัญ	เรียงข้อ	ความมั่นใจ	พรพรหม	ความมั่นใจ	สามารถ	ความ	
ข้อมูลส่วนตัวลูกค้า	เสร็จสิ้นแล้ว	2.1666667	2		2	3		1	2
บัญชีเงินฝาก	เสร็จสิ้นแล้ว	3.2857143	3		2	3		3	4
เงินในตู้เซฟ	เสร็จสิ้นแล้ว	4	4		3	4		3	4
เครื่องเซิร์ฟเวอร์	เสร็จสิ้นแล้ว	3	3		2	3		3	3
ข้อมูลพนักงาน	ยังไม่ได้ทำ	0			0			0	

ทรัพย์สินที่วิเคราะห์ที่ ข้อมูลพนักงาน โครงการ วิเคราะห์ความเสี่ยงธนาคาร

ผู้วิเคราะห์ที่ เรียงข้อ องค์กร ธนาคารABC

คุณ เรียงชัย ในความคิดเห็นของคุณ

คุณคิดว่า ข้อมูลพนักงาน เป็นทรัพย์สินที่มีความสำคัญต่อองค์กรในระดับไหน

ไม่มี  น้อย  ปานกลาง  มาก  มากที่สุด

เป็นทรัพย์สินที่สำคัญต่อธนาคารมาก  
ซึ่งทรัพย์สินที่มีผลกระทบต่อองค์กรก่อนข้างจนแรง  
แต่ไม่ถึงกับเป็นภัยพิบัติที่ก่อให้เกิดความเสียหาย

ระดับความมั่นใจ

น้อย  ปานกลาง  มาก

ตกลง ยกเลิก

ยกเลิก

แสดงผลการวิเคราะห์

รูปที่ 4.13 หน้าจอการเมื่อคลิกปุ่มวิเคราะห์ระดับความสำคัญทรัพย์สิน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทรัพย์สินที่วิเคราะห์	ข้อมูลพนักงาน	โครงการ	วิเคราะห์ความเสี่ยงธนาคาร
ผู้วิเคราะห์	เริงชัย	องค์กร	ธนาคารABC

คุณ เริงชัย ในความคิดเห็นของคุณ  
คุณคิดว่า ข้อมูลพนักงาน เป็นทรัพย์สินที่มีความสำคัญต่อองค์กรในระดับไหน

ไม่มี  น้อย  ปานกลาง  มาก  มากที่สุด

น้อย  ปานกลาง  มาก

ระดับความมั่นใจ

น้อย  ปานกลาง  มาก

ตกลง ยกเลิก

รูปที่ 4.14 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญทรัพย์สิน

กรณีที่ทำการวิเคราะห์ระดับความสำคัญทรัพย์สินเสร็จแล้ว ต้องการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน สามารถเลือกรายการทรัพย์สินที่ต้องการแล้วคลิกปุ่มวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ระบบจะแสดงหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ดังรูป 4.15

#### 4.3.4 การวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

ระบบแสดงหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ดังรูป 4.15 ซึ่งหน้าจอนี้จะเป็นการเพิ่ม ลบและวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

กรณีต้องการวิเคราะห์ระดับ โอกาสที่จะเกิดภัยคุกคาม สามารถเลือกรายการภัยคุกคามที่ต้องการแล้วคลิกปุ่มวิเคราะห์ความน่าจะเป็นของภัยคุกคาม ระบบจะแสดงหน้าจอ ดังรูป 4.16 ซึ่งให้นักวิเคราะห์แต่ละคนตอบคำถามเพื่อวิเคราะห์ระดับ โอกาสที่จะเกิดภัยคุกคาม โดยจะให้มีการกำหนดระดับความมั่นใจในการตอบด้วย เมื่อนักวิเคราะห์ตอบหมดทุกคนแล้วจะสามารถคลิกปุ่มเสร็จสิ้นได้ ระบบจะทำการหาค่าเฉลี่ยโดยมีการนำระดับความมั่นใจในการตอบมาคิดด้วย จากนั้นระบบจะอัปเดตสถานะและบันทึกข้อมูล

กรณีต้องการเพิ่มหรือลบรายการภัยคุกคามต่อ ผู้ใช้สามารถกรอกรายการภัยคุกคามแล้วคลิกปุ่มเพิ่มเพื่อเพิ่มรายการ หรือเลือกภัยคุกคามที่ต้องการลบ แล้วคลิกปุ่มลบเพื่อลบรายการนั้น

ระบบวิเคราะห์ความเสี่ยงของสาขาพื้นที่

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการสาขาม การจัดการผู้ใช้ การเปลี่ยนรหัสผ่าน ตัวช่วย ออกจากระบบ

ขั้นตอน วิเคราะห์ภัยคุกคามต่อข้อมูลส่วนตัวลูกค้า

ผลการวิเคราะห์ระดับความน่าจะเป็นของภัยคุกคาม							
ทรัพย์สิน	สถานะ	ระดับความสำคัญ	เรียงชั้น	ความมั่นใจ	พรพรรม	ความมั่นใจ	สามารถ
Hacker	เสร็จสิ้นแล้ว	3.75	3	1	4	1	4
ท่าอากาศยาน	เสร็จสิ้นแล้ว	0.50		2	1	3	0

ภัยคุกคามต่อทรัพย์สินขององค์กร

เก็บรายการภัยคุกคามต่อทรัพย์สิน

ลบรายการ

วิเคราะห์ความน่าจะเป็นของภัยคุกคาม

วิเคราะห์ผลกระทบจากภัยคุกคาม

แก้ไข

ยกเลิก

เสร็จสมบูรณ์

โครงการ วิเคราะห์ความเสี่ยงธนาคาร

องค์กร ธนาคารABC

รูปที่ 4.15 หน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

ภัยคุกคามที่วิเคราะห์ Hacker

ผู้วิเคราะห์ เรียงชั้น

โครงการ วิเคราะห์ความเสี่ยงธนาคาร

องค์กร ธนาคารABC

คุณ เรียงชั้น ในความคิดเห็นของคุณ  
คุณคิดว่าภัยคุกคามจาก Hacker มีโอกาสที่จะเกิดขึ้นได้ในระดับไหน

ไม่มี  
 น้อย  
 ปานกลาง  
 มาก  
 มากที่สุด

มีโอกาที่จะเกิดขึ้นได้ปานกลาง เกิดขึ้นไม่สม่ำเสมอ  
คือ บางช่วงเกิดบ่อย บางช่วงไม่มี  
แต่โดยรวมเกิดขึ้นไม่บ่อยนัก

ระดับความมั่นใจ

น้อย  
 ปานกลาง  
 มาก

ตกลง เสร็จสิ้น ยกเลิก

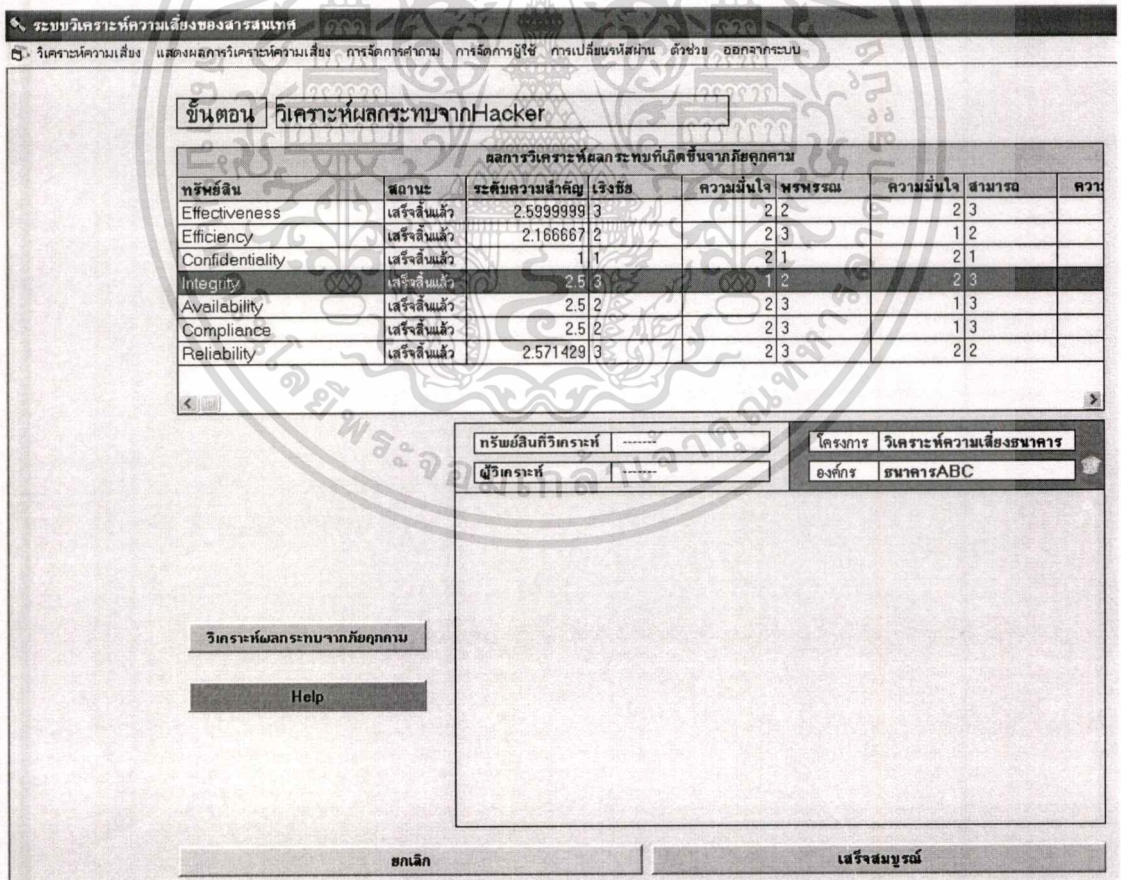
รูปที่ 4.16 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์โอกาสที่จะเกิดภัยคุกคาม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กรณีที่ทำกรวิเคราะห์โอกาสที่จะเกิดภัยคุกคามเสร็จแล้ว ต้องการวิเคราะห์ผลกระทบจากภัยคุกคาม สามารถเลือกรายการภัยคุกคามที่ต้องการแล้วคลิกปุ่มวิเคราะห์ผลกระทบจากภัยคุกคาม ระบบจะแสดงหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม ดังรูป 4.17

4.3.5 การวิเคราะห์ผลกระทบจากภัยคุกคาม

ระบบแสดงหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม ดังรูป 4.17 ซึ่งหน้าจอนี้จะเป็นการวิเคราะห์ผลกระทบจากภัยคุกคาม โดยเลือกรายการผลกระทบที่ต้องการแล้วคลิกปุ่มวิเคราะห์ผลกระทบจากภัยคุกคาม ระบบจะแสดงหน้าจอดังรูป 4.18 ซึ่งให้นักวิเคราะห์แต่ละคนตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญทรัพย์สิน โดยจะให้มีการกำหนดระดับความมั่นใจในการตอบด้วยเมื่อนักวิเคราะห์ตอบหมดทุกคนแล้วจะสามารถคลิกปุ่มเสร็จสิ้นได้ ระบบจะทำการหาค่าเฉลี่ยโดยมีการนำระดับความมั่นใจในการตอบมาคิดด้วย จากนั้นระบบจะอัปเดตสถานะและบันทึกข้อมูล



รูปที่ 4.17 หน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 2px;">ทรัพย์สินที่วิเคราะห์</td> <td style="padding: 2px;">Efficiency</td> </tr> <tr> <td style="padding: 2px;">ผู้วิเคราะห์</td> <td style="padding: 2px;">พรพรรณ</td> </tr> </table>	ทรัพย์สินที่วิเคราะห์	Efficiency	ผู้วิเคราะห์	พรพรรณ	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 2px;">โครงการ</td> <td style="padding: 2px;">วิเคราะห์ความเสี่ยงธนาคาร</td> </tr> <tr> <td style="padding: 2px;">องค์กร</td> <td style="padding: 2px;">ธนาคารABC</td> </tr> </table>	โครงการ	วิเคราะห์ความเสี่ยงธนาคาร	องค์กร	ธนาคารABC
ทรัพย์สินที่วิเคราะห์	Efficiency								
ผู้วิเคราะห์	พรพรรณ								
โครงการ	วิเคราะห์ความเสี่ยงธนาคาร								
องค์กร	ธนาคารABC								

คุณ พรพรรณ ในความคิดเห็นของคุณ  
คุณคิดว่าภัยคุกคามที่เกิดขึ้นส่งผลกระทบต่อ Efficiency ในระดับไหน

ไม่มี

น้อย

ปานกลาง

มาก

มากที่สุด

มีผลกระทบต่อองค์กรค่อนข้างรุนแรง  
อาจส่งผลกระทบต่อทั้งทางตรงและทางอ้อม  
หรือทำให้การดำเนินงานมีปัญหา  
แต่ไม่ถึงกับเป็นภัยคุกคามที่ทำให้องค์กรล้มเหลว

ระดับความมั่นใจ

ปลอดภัย

ปานกลาง

มาก

ตกลง
เสร็จสิ้น
ยกเลิก

รูปที่ 4.18 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์ผลกระทบจากภัยคุกคาม

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ [ตัวช่วย]	
วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการค่าตาม การจัดการผู้ใช้ การเปลี่ยนแปลงผ่าน ตัวช่วย ออกจากระบบ	
ค้นหาของระบบสารสนเทศ 7 ประเภท	โปรแกรมหลักของ CobIT
<b>Effectiveness</b>	ประสิทธิภาพ (Effectiveness) หมายถึงข้อมูลที่เกี่ยวข้องกับกระบวนการทางธุรกิจ รวมทั้งมีการส่งมอบข้อมูลแก่ผู้ใช้อย่างถูกต้อง ครบถ้วน สม่าเสมอ และใช้ประโยชน์ได้
<b>Efficiency</b>	ประสิทธิผล (Efficiency) หมายถึง มีการใช้ประโยชน์จากทรัพยากรอย่างเต็มที่เพื่อให้ได้มาซึ่งข้อมูลสารสนเทศ
<b>Confidentiality</b>	ความลับ (Confidentiality) หมายถึง การป้องกันความลับของข้อมูลที่สำคัญต่อบุคคลหรือหน่วยงานที่ไม่ได้รับอนุญาต
<b>Integrity</b>	ความสมบูรณ์และถูกต้อง (Integrity) หมายถึงความครบถ้วนถูกต้องของข้อมูล ตลอดจนเป็นข้อมูลใช้ได้ ในแง่ของความคาดหวังและการให้ความสำคัญของธุรกิจ (business values and expectations)
<b>Availability</b>	การมีใช้เมื่อต้องการ (Availability) หมายถึง เป็นข้อมูลที่เรียกใช้ได้เมื่อต้องการและจำเป็นใช้ ทั้งในปัจจุบันและอนาคต และรวมทั้งการป้องกันภัยให้ทันทรัพยากรต่างๆที่จำเป็นและรักษาระดับความสามารถในการทำงานของทรัพยากรเหล่านั้น
<b>Compliance</b>	การปฏิบัติตามระบบ (Compliance) หมายถึง การที่ข้อมูลได้จัดทำขึ้นตามกฎหมาย ระเบียบ ข้อบังคับ หลักเกณฑ์ ข้อตกลง หรือกฎหมาย ที่มีขึ้นเพื่อบังคับใช้ทั้งจากหน่วยงานภายในและภายนอกองค์กร เช่น ข้อบังคับของตลาดหลักทรัพย์ ประมวลกฎหมายอาญา หลักการบัญชียอมรับโดยทั่วไป เป็นต้น
<b>Reliability</b>	ความน่าเชื่อถือของข้อมูล (Reliability of Information) หมายถึงความสามารถในการรักษาข้อมูลที่เหมาะสมให้แก่ผู้บริหารของกิจการ เพื่อสามารถดำเนินธุรกิจและเพื่อให้สามารถจัดทำรายงานทางการเงินและรายงานที่จำเป็นอื่นภายใต้ความรับผิดชอบของผู้บริหาร
ตกลง	

รูปที่ 4.19 หน้าจอการช่วยอธิบายความหมายของคำต่างๆที่ใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในกรณีที่ผู้ใช้ต้องการคำแนะนำ สามารถคลิกที่เมนูตัวช่วยได้ตลอดเวลา ตัวอย่างคำอธิบายความหมายของคำที่ใช้แสดงดังรูปที่ 4.19

เมื่อนักวิเคราะห์ทำการตอบคำถามเกี่ยวกับผลกระทบจากภัยคุกคามเสร็จแต่ละรายการ สถานะจะถูกเปลี่ยนจาก “ยังไม่ได้ทำ” เป็น “เสร็จสิ้นแล้ว” ถ้าจนนักวิเคราะห์ทำเสร็จหมดทุกรายการแล้ว จะสามารถคลิกปุ่ม “เสร็จสิ้นสมบูรณ์” ได้ (ถ้ายังทำไม่เสร็จจะไม่สามารถคลิกได้)

เมื่อคลิก “ปุ่มเสร็จสิ้นสมบูรณ์” จากหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม ระบบจะทำการบันทึกค่าต่างๆ และกลับไปหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน จากนั้นระบบจะอัปเดตสถานะของรายการภัยคุกคามที่นักวิเคราะห์ผลกระทบแล้ว เปลี่ยนจาก “ยังไม่ได้ทำ” เป็น “เสร็จสิ้นแล้ว”

เมื่อวิเคราะห์ผลกระทบจากภัยคุกคามของแต่ละภัยคุกคามเสร็จแล้ว และวิเคราะห์โอกาสที่จะเกิดภัยคุกคามเสร็จแล้วทุกรายการ จะสามารถคลิกปุ่ม “เสร็จสิ้นสมบูรณ์” บนหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สินได้

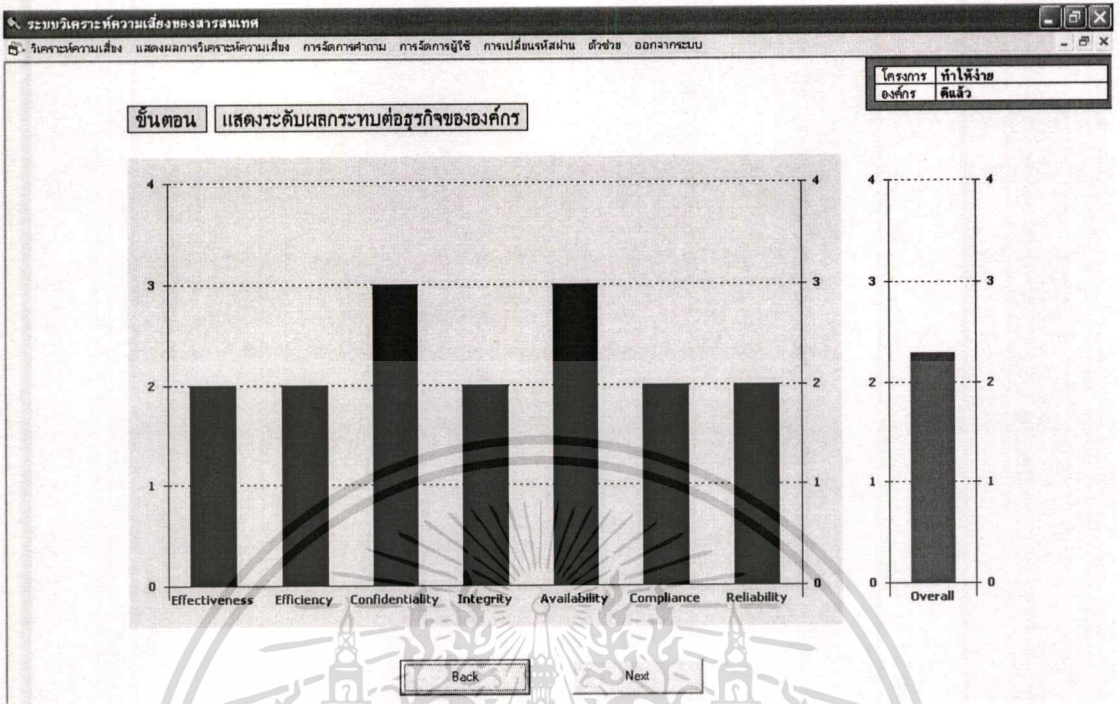
เมื่อคลิก “ปุ่มเสร็จสิ้นสมบูรณ์” จากหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ระบบจะทำการบันทึกค่าต่างๆ และกลับไปหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญ จากนั้นระบบจะอัปเดตสถานะของรายการทรัพย์สินที่นักวิเคราะห์ผลกระทบและภัยคุกคามแล้ว เปลี่ยนจาก “ยังไม่ได้ทำ” เป็น “เสร็จสิ้นแล้ว”

เมื่อวิเคราะห์ภัยคุกคามต่อทรัพย์สินเสร็จแล้ว และวิเคราะห์ระดับความสำคัญของทรัพย์สินเสร็จแล้วทุกรายการ จะสามารถคลิกปุ่ม “แสดงผลการวิเคราะห์” จากหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กรได้

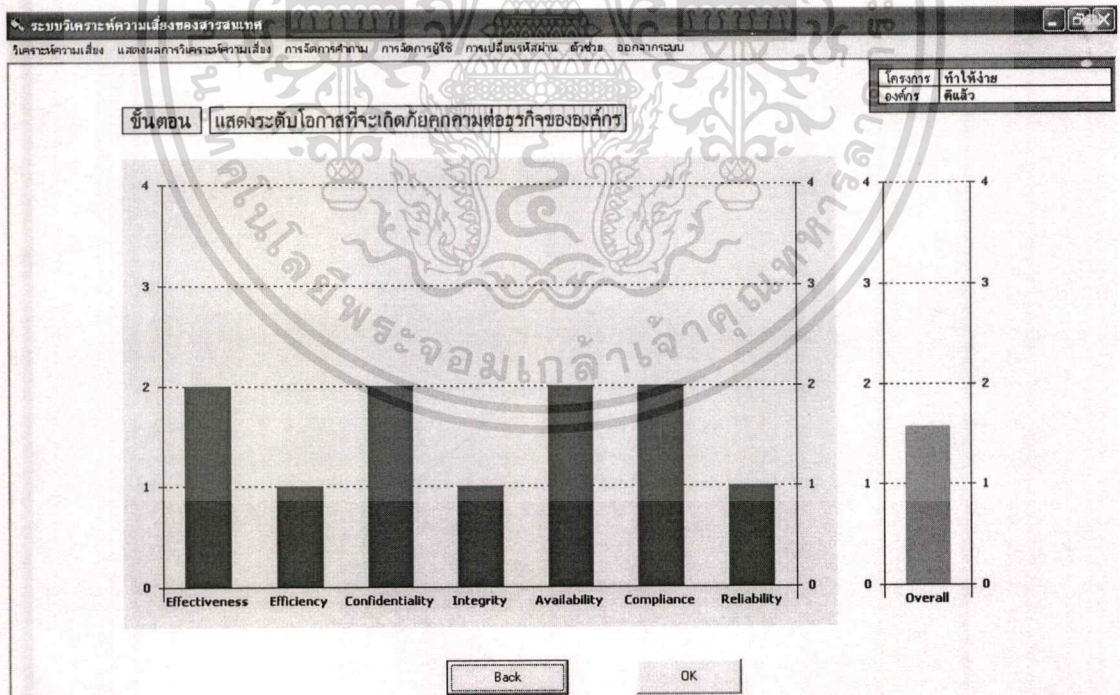
#### 4.3.6 การวิเคราะห์ความเสี่ยงถาวร (Inherent Risk)

เมื่อผู้ใช้คลิกปุ่ม “แสดงผลการวิเคราะห์” จากหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กรแล้ว ระบบจะทำการคำนวณค่าระดับผลกระทบและระดับโอกาสที่จะเกิดภัยคุกคามขึ้น ต่อปัจจัยหลัก 7 อย่าง (คุณภาพของระบบสารสนเทศ 7 ประการ) โดยจะใช้ข้อมูลจากการวิเคราะห์ที่ผ่านมาในการคำนวณ จากนั้นจะแสดงผลการคำนวณค่าระดับผลกระทบและระดับโอกาสที่จะเกิดภัยคุกคามในลักษณะแผนภูมิแท่ง ดังรูปที่ 4.20 และ 4.21 ตามลำดับ

หลังจากนั้นระบบจะแสดงหน้าจอสำหรับกำหนดค่าในตารางที่ใช้คำนวณค่าความเสี่ยง (Risk Aversion Table) แสดงดังรูปที่ 4.22 เพื่อให้ นักวิเคราะห์ทำการกำหนดค่าในตารางตามความเหมาะสม ถ้าไม่กำหนด ระบบจะใช้ค่ามาตรฐานในการคำนวณ จะได้ค่าความเสี่ยงดังรูปที่ 4.23

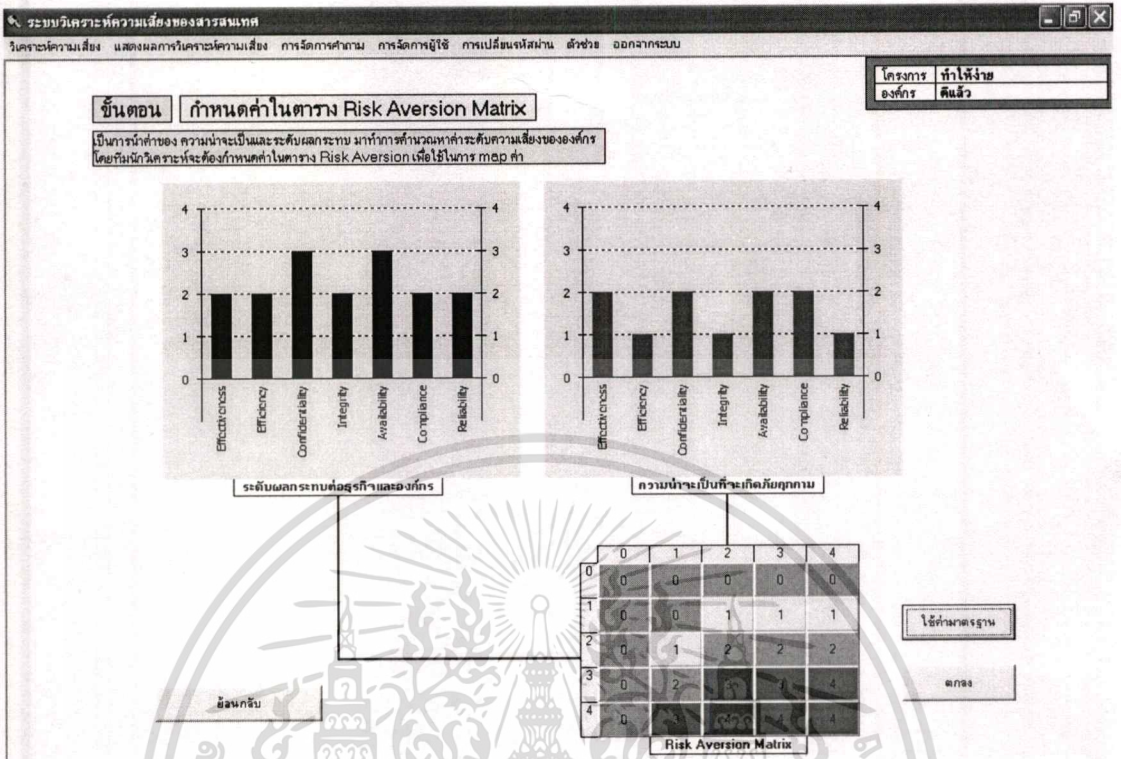


รูปที่ 4.20 ระดับผลกระทบต่อธุรกิจขององค์กร

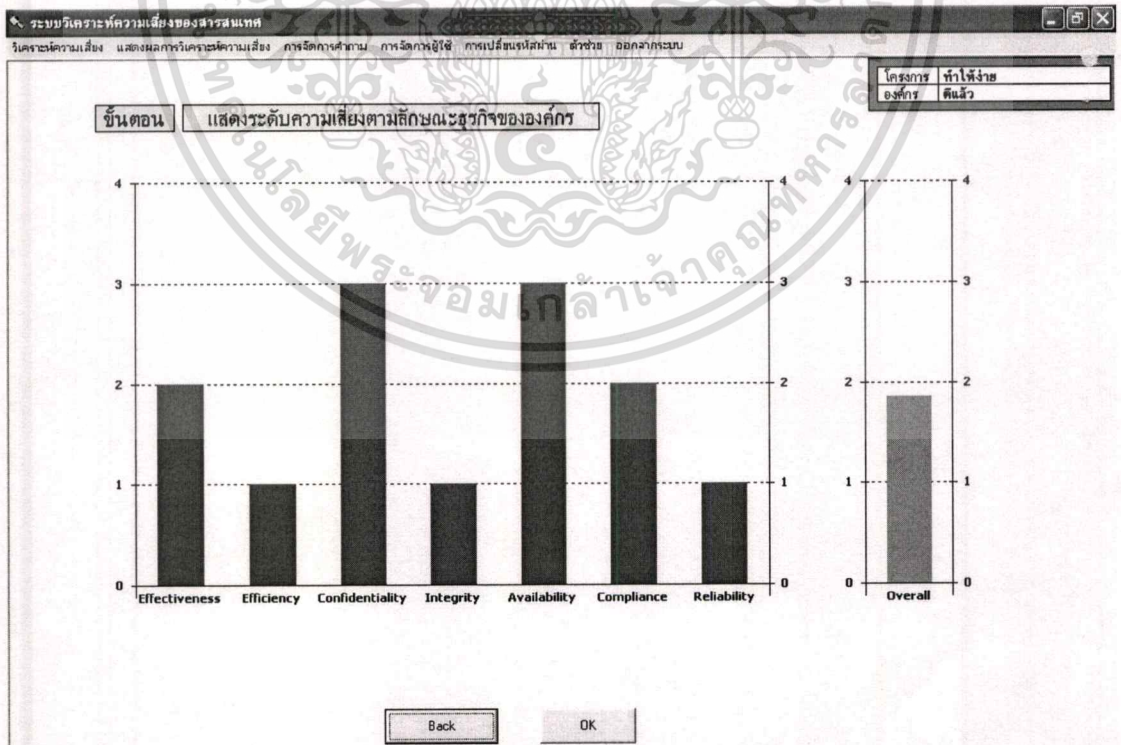


รูปที่ 4.21 ระดับโอกาสที่จะเกิดภัยคุกคามต่อธุรกิจขององค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.22 ตารางกำหนดค่าในการคำนวณหาความเสี่ยง



รูปที่ 4.23 ระดับความเสี่ยงตามลักษณะธุรกิจขององค์กร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการตาม การจัดการผู้ใช้ การเปลี่ยนแปลงผ่าน ตัวช่วย ออกจากระบบ

### Inherent Risk

โครงการ องค์กร	ทำให้ง่าย ค้นคว้า	Materiality →	Effectiveness		Confidentiality		Availability		Reliability	
			Efficiency	Integrity	Compliance	Efficiency	Integrity	Compliance		
Planning and Organization	P01	Define a Strategic IT Plan	C	H						
	P02	Define the Information Architecture	C	H	C	H				
	P03	Determine Technological Direction	C	H						
	P04	Define the IT Organisation and Relationships	C	H						
	P05	Manage the IT Investment	C	H						H
	P06	Communicate Management Aims and Direction	C						C	
	P07	Manage Human Resources	C	H						
	P08	Ensure Compliance with External Requirements	C						C	H
	P09	Assess Risks	C	H	E	H	E	C	H	
	P010	Manage Projects	C	H						
	P011	Manage Quality	C	H		H				H
Acquisition and Implementation	A11	Identify Automated Solutions	C	H						
	A12	Acquire and Maintain Application Software	C	H		H		C	H	
	A13	Acquire and Maintain Technology Infrastructure	C	H		H				
	A14	Develop and Maintain Procedures	C	H				C	H	
	A15	Install and Accredite Systems	C			H	C			
	A16	Manage Changes	C	H		H	E		H	
Delivery and Support	DS1	Define and Manage Service Levels	C	H	C	H	C	C	H	
	DS2	Manage Third-Party Services	C	H	C	H	C	C	H	
	DS3	Manage Performance and Capacity	C	H			C			
	DS4	Ensure Continuous Service	C	H						
	DS5	Ensure Systems Security			E	H	C	C	H	
	DS6	Identify and Allocate Costs		H					H	
	DS7	Educate and Train Users	C	H						
	DS8	Assist and Advise Customers	C	H						
	DS9	Manage the Configuration	C				C		H	
	DS10	Manage Problems and Incident	C	H			C			
	DS11	Manage Data				H	C		H	
	DS12	Manage Facilities				H				
	DS13	Manage Operations	C	H		H	C			
Monitoring	M1	Monitor the Processes	C	H	C	H	C	C	H	
	M2	Assess Internal Control Adequacy	C	H	C	H	C	C	H	
	M3	Obtain Independent Assurance	C	H	C	H	C	C	H	
	M4	Provide for Independent Audit	C	H	C	H	C	C	H	

Click Legend for Description

Legends

- Exposure
- Concern
- Housekeeping
- OK

ตาราง Inherent Risk เป็นภาพของความเสี่ยงที่จะถูกรับรู้ซึ่งมีความเสี่ยงในขณะองค์กรละเมิดข้อกำหนดที่อยู่กับกิจกรรมเฉพาะทางธุรกิจขององค์กรนั้นๆ สำหรับความเสี่ยงอย่างมีค่าอธิบายโดยสัญลักษณ์ Legend ด้านข้างของจอ โดยสามารถคลิกที่ Legend ด้านข้างของตาราง Inherent Risk สามารถดูได้โดยคลิกปุ่ม Help

Help

<< Back Next >>

รูปที่ 4.24 ตารางความเสี่ยงถาวร

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการตาม การจัดการผู้ใช้ การเปลี่ยนแปลงผ่าน ตัวช่วย ออกจากระบบ

ขั้นตอน เลือกโดเมนย่อยเพื่อวิเคราะห์ระดับการควบคุมและจัดการความเสี่ยง

รายการ	สถานะ	ค่า
PO 1 Define a Strategic IT Plan	ยังไม่ได้ทำ	0
PO 2 Define the Information Architecture	ยังไม่ได้ทำ	0
PO 3 Determine Technological Direction	เสร็จสิ้นแล้ว	2
PO 4 Define the IT Organisation and Relationships	เสร็จสิ้นแล้ว	1
PO 5 Manage the IT Investment	เสร็จสิ้นแล้ว	0
PO 6 Communicate Management Aims and Direction	เสร็จสิ้นแล้ว	3
PO 7 Manage Human Resources	เสร็จสิ้นแล้ว	0
PO 8 Ensure Compliance with External Requirements	เสร็จสิ้นแล้ว	0
PO 9 Assess Risks	เสร็จสิ้นแล้ว	1
PO 10 Manage Projects	เสร็จสิ้นแล้ว	0
PO 11 Manage Quality	เสร็จสิ้นแล้ว	0
AI 1 Identify Automated Solutions	เสร็จสิ้นแล้ว	1
AI 2 Acquire and Maintain Application Software	เสร็จสิ้นแล้ว	2
AI 3 Acquire and Maintain Technology Infrastructure	เสร็จสิ้นแล้ว	2
AI 4 Develop and Maintain Procedures	เสร็จสิ้นแล้ว	1
AI 5 Install and Accredite Systems	เสร็จสิ้นแล้ว	1
AI 6 Manage Changes	ยังไม่ได้ทำ	0
DS 1 Define and Manage Service Levels	ยังไม่ได้ทำ	0

แสดงเฉพาะโดเมน PO (Planning and Organization)

แสดงเฉพาะโดเมน AI (Acquisition and Implementation)

แสดงเฉพาะโดเมน DS (Delivery and Support)

แสดงเฉพาะโดเมน M (Monitoring)

แสดงทั้งหมด

Back วิเคราะห์การจัดการความเสี่ยง

รูปที่ 4.25 หน้าจอรายการ โดเมนย่อยของ CobiT

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบทำการนำค่าระดับความเสี่ยงที่คำนวณได้มาแสดงในตารางความเสี่ยงถาวรในรูปแบบที่ 4.24 โดยเป็นความเสี่ยงที่เกิดขึ้นตามลักษณะธุรกิจขององค์กรนั้น ยังไม่มีการควบคุมจัดการใดๆ ถ้าต้องการวิเคราะห์ต่อ คลิกปุ่ม Next ระบบจะแสดงหน้าจอโดเมนย่อยของ CobiT ดังรูปที่ 4.25 จากนั้นผู้วิเคราะห์สามารถเลือกโดเมนย่อยแล้วคลิกปุ่มการจัดการความเสี่ยงเพื่อทำการวิเคราะห์ได้ จากนั้นระบบจะแสดงหน้าจอการวิเคราะห์การจัดการความเสี่ยงดังรูปที่ 4.26 นักวิเคราะห์สามารถเลือกตอบคำถามจากรายการได้โดยคลิกปุ่มตอบคำถาม ระบบจะแสดงหน้าจอดังรูปที่ 4.27

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการคำถาม การจัดการผู้ใช้ การประเมินเจ้าหน้าที่ ส่วน ตัวช่วย ออกจากระบบ

ขั้นตอน **ตอบคำถามเพื่อวิเคราะห์ระดับการควบคุมและจัดการความเสี่ยง**

โครงการ: ทำใจง่าย  
องค์กร: คิวแล้ว

คำถาม	สถานะ	คำตอบ	พอใจ	ความมั่นใจ	หมายเหตุ
องค์กรมีการนำ IT มาเป็นส่วนหนึ่งของแผนการระยะสั้นและระยะยาวขององค์กรอย่างไร	เสร็จสิ้นแล้ว	2.5999999	2	2	3
องค์กรมีแผนการ IT ระยะยาวเป็นอย่างไร	เสร็จสิ้นแล้ว	2.2	4	2	1
มีการวางแผน IT ระยะยาวเกี่ยวกับแนวคิดและโครงสร้างอย่างไร	เสร็จสิ้นแล้ว	1	2	2	1
องค์กรมีการเปลี่ยนแปลงแผนการ IT ระยะยาวอย่างไร	ยังไม่ได้ทำ	0	0	0	0

ตอบคำถาม

เตรียมสินที่วิเคราะห์:

ผู้วิเคราะห์:

รูปที่ 4.26 หน้าจอการวิเคราะห์การจัดการความเสี่ยง

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการคำถาม การจัดการผู้ใช้ การประเมินเจ้าหน้าที่ ส่วน ตัวช่วย ออกจากระบบ

ขั้นตอน **ตอบคำถามเพื่อวิเคราะห์ระดับการควบคุมและจัดการความเสี่ยง**

โครงการ: ทำใจง่าย  
องค์กร: คิวแล้ว

คำถาม	สถานะ	คำตอบ	พอใจ	ความมั่นใจ	หมายเหตุ
องค์กรมีการนำ IT มาเป็นส่วนหนึ่งของแผนการระยะสั้นและระยะยาวขององค์กรอย่างไร	เสร็จสิ้นแล้ว	2.5999999	2	2	3
องค์กรมีแผนการ IT ระยะยาวเป็นอย่างไร	เสร็จสิ้นแล้ว	2.2	4	2	1
มีการวางแผน IT ระยะยาวเกี่ยวกับแนวคิดและโครงสร้างอย่างไร	เสร็จสิ้นแล้ว	1	2	2	1
องค์กรมีการเปลี่ยนแปลงแผนการ IT ระยะยาวอย่างไร	ยังไม่ได้ทำ	0	0	0	0

คุณพอใจ ในความคิด เห็นของคุณ  
คุณคิดว่า องค์กรมีการเปลี่ยนแปลงแผนการ IT ระยะยาวอย่างไร

ไม่มีการเปลี่ยนแปลงแผนการ IT ระยะยาว

มีการเปลี่ยนแปลง โดย ไม่มีการแจ้งหรือระบุไว้ชัดเจนอย่างเป็นทางการ

การเปลี่ยนแปลงแผนการ IT ระยะยาวจะเกิดขึ้นโดยฉับพลันในเวลาที่เหมาะสม

2 + มีการพิจารณาผลกระทบต่อแผนการระยะสั้นและระยะยาวขององค์กร รวมถึงการเปลี่ยนแปลงของ IT

3 + มีการกำหนดนโยบายที่เกี่ยวข้องกับแผนการ IT ระยะสั้นและระยะยาวที่เข้มงวดใหม่ และจะต้องถูกใช้

ระดับความมั่นใจ

น้อย

ปานกลาง

มาก

ตกลง

รูปที่ 4.27 นักวิเคราะห์ตอบคำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อนักวิเคราะห์ตอบคำถามหมดแล้ว ระบบจะทำการอัปเดตสถานะจากจาก “ยังไม่ได้ทำ” เป็น “เสร็จสิ้นแล้ว” และจะสามารถคลิกปุ่มแสดงความเสี่ยงที่เหลืออยู่ได้ หลังจากคลิกปุ่มแสดงความเสี่ยงที่เหลือ ระบบจะแสดงหน้าจอตารางความเสี่ยงที่เหลืออยู่ดังรูปที่ 4.28

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการความเสี่ยง การจัดการผู้ใช้ การเปลี่ยนรหัสผ่าน ตัวช่วย ออกจากระบบ

### Residual Risk

โครงการ องค์กร	ทำให้ง่าย ต้นแล้ว	Materiality →	Effectiveness		Confidentiality		Availability		Reliability	
			Efficiency	Integrity	Compliance	Efficiency	Integrity	Compliance		
			2	1	3	1	3	2	1	
Planning and Organization	P01	Define a Strategic IT Plan	0	C	H					
	P02	Define the Information Architecture	0	C	H		H			
	P03	Determine Technological Direction	2	0	+					
	P04	Define the IT Organisation and Relationships	1	H	0					
	P05	Manage the IT Investment	0	C	H					H
	P06	Communicate Management Aims and Direction	3	+					+	
	P07	Manage Human Resources	0	C	H					
	P08	Ensure Compliance with External Requirements	0	C	H					C
	P09	Assess Risks	1	H	0	C	0	C	H	0
	P010	Manage Projects	0	C	H					
	P011	Manage Quality	0	C	H		H			H
Acquisition and Implementation	A11	Identify Automated Solutions	1	H	0					
	A12	Acquire and Maintain Application Software	2	0	+		+		0	+
	A13	Acquire and Maintain Technology Infrastructure	2	0	+		+			
	A14	Develop and Maintain Procedures	1	H	0		0		H	0
	A15	Install and Accredite Systems	1	H	0		0	C		
	A16	Manage Changes	0	C	H		H			H
Delivery and Support	DS1	Define and Manage Service Levels	0	C	H		H		C	H
	DS2	Manage Third-Party Services	0	C	H		H		C	H
	DS3	Manage Performance and Capacity	1	H	0					
	DS4	Ensure Continuous Service	0	C	H					
	DS5	Ensure Systems Security	0				H		C	H
	DS6	Identify and Allocate Costs	0				H			H
	DS7	Educate and Train Users	0	C	H					
	DS8	Assist and Advise Customers	0	C	H					
	DS9	Manage the Configuration	0	C						H
	DS10	Manage Problems and Incidents	0	C	H					
	DS11	Manage Data	0				H			H
	DS12	Manage Facilities	1				0	C		
	DS13	Manage Operations	1	H	0		0	C		
Monitoring	M1	Monitor the Processes	0	C	H		H		C	H
	M2	Assess Internal Control Adequacy	0	C	H		H		C	H
	M3	Obtain Independent Assurance	0	C	H		H		C	H
	M4	Provide for Independent Audit	0	C	H		H		C	H

Click Legend for Description

Legends

- Exposure
- Concern
- Housekeeping
- OK
- OverProtect

ตาราง Inherent Risk เป็นการแสดงความเสี่ยงที่องค์กรมีแต่ยังไม่ดำเนินการป้องกัน โดยเฉพาะทางธุรกิจขององค์กรนั้นๆ ค่าระดับความเสี่ยงอาจมีค่าที่ต่างกันตามที่ Legend ซึ่งรายละเอียดนั้นจะอธิบายไว้ในตาราง Inherent Risk สามารถคลิกปุ่ม Help

<< Back Next >>

รูปที่ 4.28 ตารางความเสี่ยงที่เหลืออยู่

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการความเสี่ยง การจัดการผู้ใช้ การเปลี่ยนรหัสผ่าน ตัวช่วย ออกจากระบบ

โครงการ	Project	ระดับความเสี่ยงและการควบคุม	สถานะ	คำแนะนำเกี่ยวกับการจัดการความเสี่ยง
องค์กร	Organization			
<b>Acquisition and Implementation</b>				
A11	Identify Automated Solutions	1 2 3 4	ยอมรับได้	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นเล็กน้อย
A12	Acquire and Maintain Application Software	1 2 3 4	ดีมาก	การจัดการความเสี่ยงอยู่ในระดับที่เหมาะสมแล้ว
A13	Acquire and Maintain Technology Infrastructure	1 2 3 4	ดีมาก	การจัดการความเสี่ยงอยู่ในระดับที่เหมาะสมแล้ว
A14	Develop and Maintain Procedures	1 2 3 4	ยอมรับได้	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นเล็กน้อย
A15	Install and Accredite Systems	1 2 3 4	ความกังวล	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกอย่างมาก
A16	Manage Changes	1 2 3 4	ความกังวล	ควรปรับปรุงในและเพิ่มมาตรการจัดการความเสี่ยงทันที
1 2 3 4				

ตกลง

เอกสารนี้เป็นเอกสารที่สงวนลิขสิทธิ์หรือการเข้าถึงที่จำกัด หรือมีเงื่อนไขการใช้งานอื่น ๆ ผู้ใช้ควรปฏิบัติตามเงื่อนไขการใช้งานที่ปรากฏในเอกสารฉบับนี้ และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โครงการ องค์กร		ระดับความเสี่ยงและการควบคุม				สถานะ	คำแนะนำเกี่ยวกับการจัดการความเสี่ยง
Planning and Organization		1	2	3	4		
P01	Define a Strategic IT Plan					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P02	Define the Information Architecture					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P03	Determine Technological Direction					ดีมาก	การจัดการความเสี่ยงอยู่ในระดับที่เหมาะสมแล้ว
P04	Define the IT Organisation and Relationships					สมบูรณ์	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกน้อย
P05	Manage the IT Investment					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P06	Communicate Management Aims and Direction					มากเกินไป	ควรมีการจัดการความเสี่ยงในส่วนนี้ลง เพื่อประหยัดค่าใช้จ่าย
P07	Manage Human Resources					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P08	Ensure Compliance with External Requirements					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P09	Assess Risks					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P010	Manage Projects					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
P011	Manage Quality					ครบถ้วน	ควรมีการจัดการความเสี่ยงในส่วนนี้เพิ่มขึ้นอีกค่อนข้างมาก
		1	2	3	4	กลาง	

รูปที่ 4.30 คำแนะนำในการจัดการความเสี่ยงในโดเมน PO

จากหน้าจอตารางความเสี่ยงที่เหลืออยู่ดังรูปที่ 4.28 จะสังเกตเห็นได้ว่าค่าระดับความเสี่ยงที่อยู่ในตารางความเสี่ยงที่คงอยู่ (Residual Risk) เปลี่ยนไปจากค่าระดับความเสี่ยงในตารางความเสี่ยงถาวร (Inherent Risk) เนื่องจากค่าในตารางความเสี่ยงที่คงอยู่ (Residual Risk) เป็นค่าที่คำนวณจากค่าระดับความเสี่ยงในตารางความเสี่ยงถาวร (Inherent Risk) กับค่าการจัดการความเสี่ยงที่ได้วิเคราะห์ไป ทำให้ตารางความเสี่ยงที่คงอยู่ (Residual Risk) จะมีค่าระดับความเสี่ยงน้อยลง ขึ้นอยู่กับว่าองค์กรมีการควบคุมและจัดการความเสี่ยงมากน้อยขนาดไหน ความหมายของค่าระดับความเสี่ยงในตาราง มีคำอธิบายโดยสามารถดูได้โดยคลิกที่ Legend แต่อย่างไรก็ตาม การวิเคราะห์ค่าจากตารางยังคงดูยาก นักวิเคราะห์สามารถดูคำแนะนำได้โดยคลิกที่ปุ่มโดเมนต่างๆ ด้านซ้ายของตารางความเสี่ยงที่คงอยู่ (Residual Risk)

จากรูปที่ 4.29 และ 4.30 เป็นตัวอย่างคำแนะนำในการควบคุมและจัดการความเสี่ยงในโดเมน AI และ PO ตามลำดับ โดยระบบจะคำนวณจากระดับความเสี่ยงและการควบคุมและจัดการความเสี่ยงที่ได้ทำไปแล้ว จะสามารถบอกได้ว่าโดเมนย่อยใดในองค์กรที่มีความเสี่ยงสูง ควรเพิ่มการจัดการในส่วนนี้ โดเมนย่อยใดในองค์กรที่มีการควบคุมจัดการมากเกินไป เป็นต้น

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการความเสี่ยง การจัดการผู้ใช้ การเปลี่ยนรหัสผ่าน ตัวช่วย ออกจากระบบ

ขั้นตอน แสดงผลการวิเคราะห์ความเสี่ยงทรัพย์สินและภัยคุกคาม

5 ความเสี่ยงของทรัพย์สิน 6 ความเสี่ยงจากภัยคุกคาม 7 ภัยคุกคามต่อทรัพย์สิน 8 บทสรุปและคำแนะนำ

1 ทรัพย์สินที่สำคัญขององค์กร 2 ทรัพย์สินที่มีโอกาสโดนคุกคาม 3 ภัยคุกคามที่มีโอกาสเกิดขึ้น 4 ภัยคุกคามที่ส่งผลกระทบต่อ

**รายการภัยคุกคามที่มีโอกาสเกิดขึ้น เรียงลำดับจากมากไปน้อย**

ภัยคุกคาม	โอกาสเกิดภัยคุกคาม	ต่อทรัพย์สิน
Hecker	3.75	บัญชีเงินฝาก
Hecker	3.75	ข้อมูลส่วนตัวลูกค้า
ขโมย	1.8	เงินในตู้เซฟ
ถูกวางระเบิด	1.1666666	เงินในตู้เซฟ

ภัยคุกคามที่มีโอกาสเกิดขึ้นมากที่สุด คือ Hecker  
ซึ่งเป็นภัยคุกคามต่อ เครื่องเซิร์ฟเวอร์  
โดยโอกาสที่จะเกิดขึ้นมีค่า = 3.75  
ซึ่งเป็นค่าที่อยู่ระหว่าง 0 ถึง 4 โดยมีคำอธิบาย ดังนี้

- 0 -- ไม่มีโอกาสที่จะเกิดขึ้นได้เลย ยังไงก็ไม่สามารถเกิดขึ้นได้
- 1 -- มีโอกาสที่จะเกิดขึ้นได้น้อยมาก แทบจะไม่เกิดขึ้นเลย หรือนานมาจริงจะเกิดขึ้น 1 ครั้ง
- 2 -- มีโอกาสที่จะเกิดขึ้นได้ปานกลาง เกิดขึ้นไม่สม่ำเสมอ บ้างช่วงเกิดขึ้น บ้างช่วงไม่เกิด แต่โดยรวมเกิดขึ้นไม่บ่อยนัก
- 3 -- มีโอกาสที่จะเกิดขึ้นได้มาก เกิดขึ้นค่อนข้างบ่อย และค่อนข้างสม่ำเสมอ เช่น เกิดขึ้นทุกปีครั้งหรือทุกเดือน
- 4 -- มีโอกาสที่จะเกิดขึ้นได้ตลอดเวลา เกิดขึ้นบ่อยมาก เป็นประจำ เช่น อยุ่เกิดขึ้นได้แทบทุกวัน

ย้อนกลับ สรุปผลการวิเคราะห์ทั้งหมด

รูปที่ 4.31 ภัยคุกคามที่มีโอกาสเกิดขึ้นมากที่สุด

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการความเสี่ยง การจัดการผู้ใช้ การเปลี่ยนรหัสผ่าน ตัวช่วย ออกจากระบบ

ขั้นตอน แสดงผลการวิเคราะห์ความเสี่ยงทรัพย์สินและภัยคุกคาม

5 ความเสี่ยงของทรัพย์สิน 6 ความเสี่ยงจากภัยคุกคาม 7 ภัยคุกคามต่อทรัพย์สิน 8 บทสรุปและคำแนะนำ

1 ทรัพย์สินที่สำคัญขององค์กร 2 ทรัพย์สินที่มีโอกาสโดนคุกคาม 3 ภัยคุกคามที่มีโอกาสเกิดขึ้น 4 ภัยคุกคามที่ส่งผลกระทบต่อ

**รายการภัยคุกคามที่ส่งผลกระทบต่อโดยรวมต่อองค์กร เรียงลำดับจากมากไปน้อย**

ภัยคุกคาม	ผลกระทบจากภัยคุกคาม	ต่อทรัพย์สิน
ไฟไหม้	4	เงินในตู้เซฟ
คิดค้น	3.4761901	เงินในตู้เซฟ
ถูกวางระเบิด	3.375	เงินในตู้เซฟ
Hecker	3.3061221	เครื่องเซิร์ฟเวอร์

ภัยคุกคามที่ส่งผลกระทบต่อโดยรวมต่อองค์กรมากที่สุด คือ ไฟไหม้  
ซึ่งเป็นภัยคุกคามต่อ เงินในตู้เซฟ  
โดยผลกระทบโดยรวมที่เกิดขึ้นมีค่า = 4  
ซึ่งเป็นค่าที่อยู่ระหว่าง 0 ถึง 4 โดยมีคำอธิบาย ดังนี้

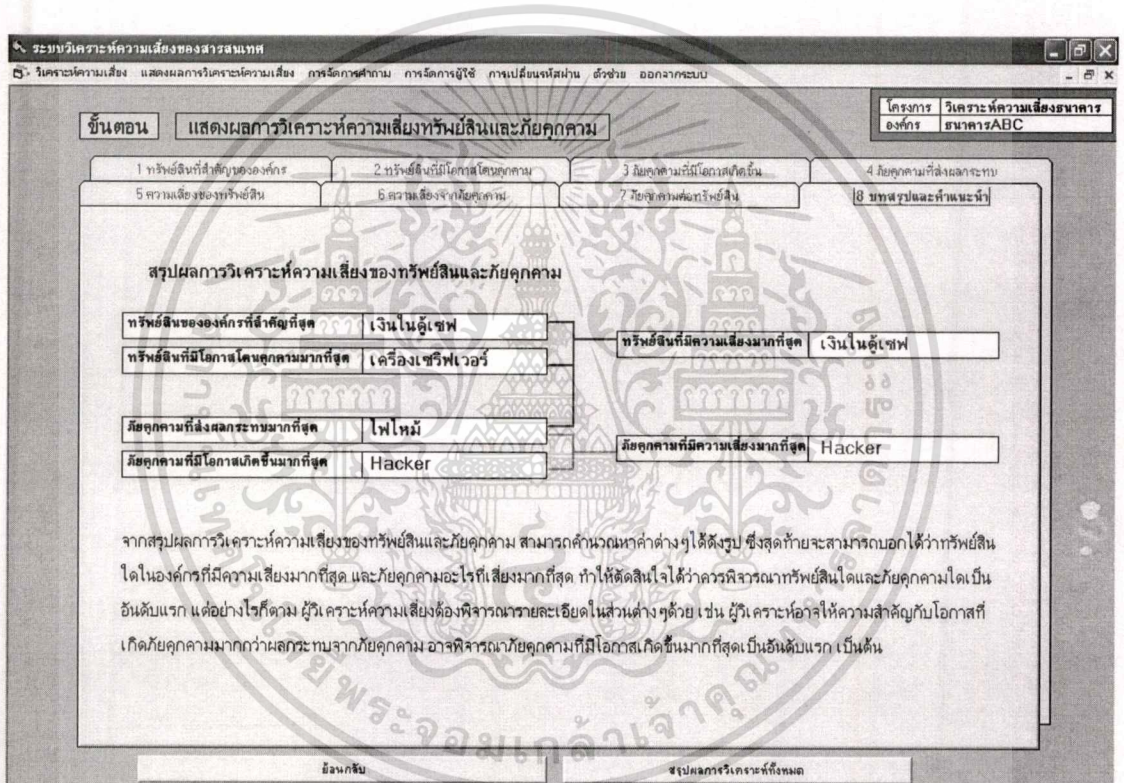
- 0 -- ไม่มีผลกระทบใดๆ เป็นภัยคุกคามที่ไม่ต้องสนใจ ปกติจะไม่เกิดขึ้นเมื่อไหร่ก็ได้ ไม่จำเป็นต้องควบคุมจัดการ
- 1 -- ส่งผลกระทบต่อทางด้านเงินขององค์กรค่อนข้างน้อย
- 2 -- ส่งผลกระทบต่อทางด้านเงินขององค์กรโดยตรงหรือทางอ้อม แต่ไม่รุนแรงนัก
- 3 -- มีผลกระทบต่อองค์กรค่อนข้างรุนแรง อาจส่งผลกระทบต่อทั้งทางตรงและทางอ้อม หรือทำให้การดำเนินงานมีปัญหา แต่ไม่ถึงกับเป็นภัยพิบัติที่ทำให้องค์กรล้มเหลว
- 4 -- มีผลกระทบอย่างรุนแรง และส่งผลกระทบต่อทั้งทางด้านเงินและเป้าหมายขององค์กร รวมทั้งมีผลต่อความอยู่รอดขององค์กร จนอาจทำให้องค์กรล้มเหลวได้

ย้อนกลับ สรุปผลการวิเคราะห์ทั้งหมด

รูปที่ 4.32 ภัยคุกคามที่ส่งผลกระทบต่อมากที่สุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนสุดท้ายเป็นหน้าจอแสดงผลการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กรและภัยคุกคามต่อทรัพย์สิน โดยวิเคราะห์เป็น 6 ส่วน คือ ความสำคัญของทรัพย์สิน ทรัพย์สินที่มีโอกาสโดนคุกคาม ภัยคุกคามที่มีโอกาสเกิดขึ้น ภัยคุกคามที่ส่งผลกระทบต่อความเสี่ยงของทรัพย์สิน ความเสี่ยงจากภัยคุกคาม โดยรูปที่ 4.31 แสดงภัยคุกคามที่มีโอกาสเกิดขึ้นเรียงจากมากไปน้อย ส่วนรูปที่ 4.32 แสดงภัยคุกคามที่ส่งผลกระทบต่อความเสี่ยงเรียงจากมากไปน้อย ส่วนรูปที่ 4.33 เป็นบทสรุปและคำแนะนำซึ่งจะช่วยให้นักวิเคราะห์ความเสี่ยงเห็นภาพรวมมากขึ้น ส่วนรายละเอียดในส่วนต่างๆ สามารถคลิกแท็บต่างๆ ได้



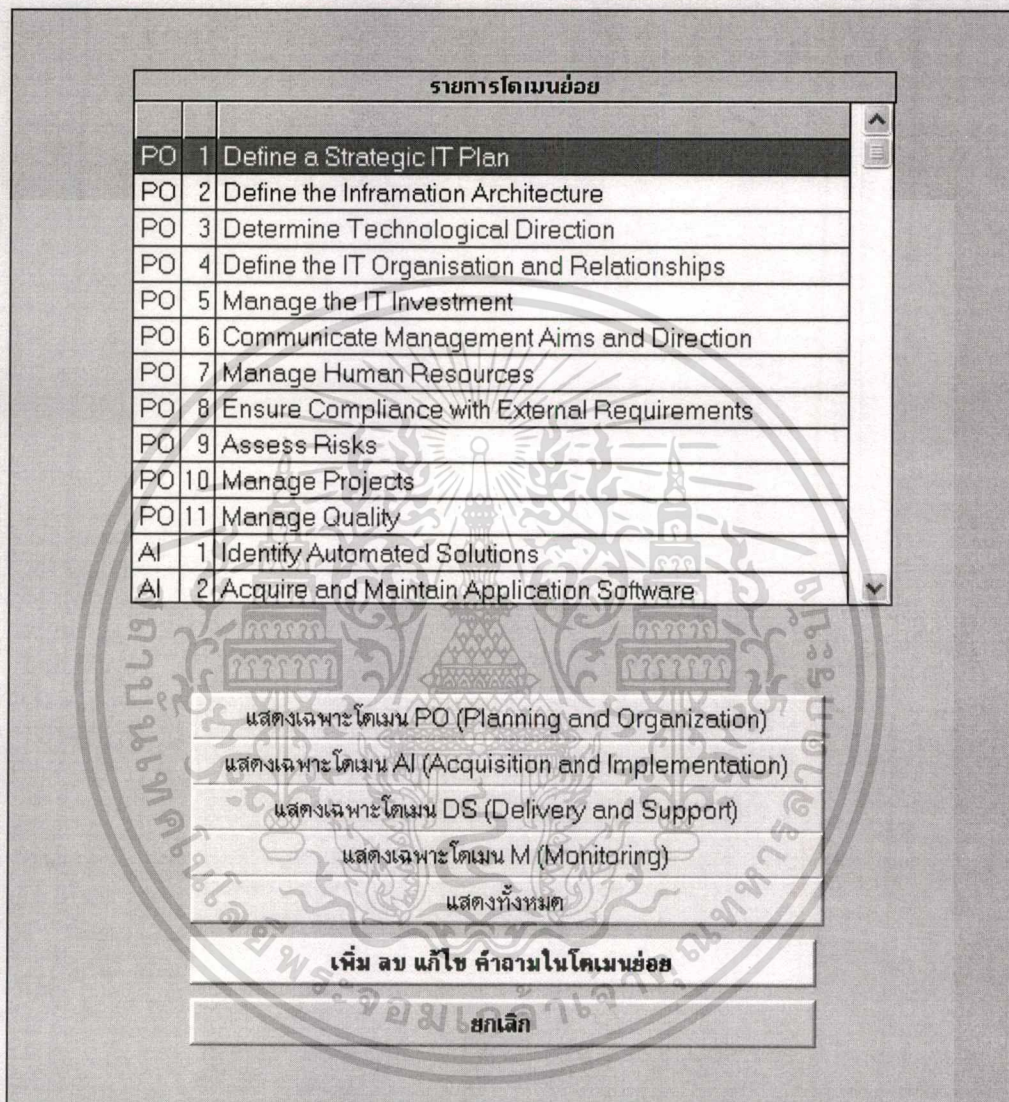
รูปที่ 4.33 บทสรุปและคำแนะนำ

#### 4.4 การจัดการคำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มการจัดการคำถามหรือคลิกการจัดการคำถามที่เมนูข้างบน หลังจากนั้นระบบจะแสดงหน้าจอการจัดการคำถามดังรูปที่ 4.34 ซึ่งจะเป็นการแสดงผลรายการโดเมนย่อยของ CobiT ทั้งหมด ซึ่งสามารถเลือกให้แสดงรายการในแต่ละโดเมนได้ เช่น คลิกปุ่มแสดงเฉพาะโดเมน PO จะแสดงเฉพาะโดเมน PO เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**ขั้นตอน** **เลือกโดเมนย่อยเพื่อ เพิ่ม ลบ แก้ไข**



**รูปที่ 4.34** หน้าจอการจัดการคำถาม

จากหน้าจอการจัดการคำถาม กรณีที่ผู้ดูแลระบบต้องการ เพิ่ม ลบ แก้ไข คำถามในโดเมนย่อย สามารถเลือกรายการโดเมนย่อย แล้วคลิกปุ่มต้องการ เพิ่ม ลบ แก้ไข คำถามในโดเมนย่อย ระบบจะแสดงหน้าจอรายการคำถามในโดเมนย่อยที่เลือก ดังรูปที่ 4.35 และสามารถเลือกคำถามที่ต้องการแก้ไข และคลิกปุ่มแก้ไข เพื่อแก้ไขได้ดังรูปที่ 4.36 ส่วนการเพิ่มและลบทำได้โดยการเลือกคำถามที่ต้องการแล้วคลิกปุ่มเพิ่มเมื่อต้องการเพิ่ม คลิกปุ่มลบเมื่อต้องการลบ โดยถ้าข้อมูลไม่ครบแล้วคลิกปุ่มเพิ่ม ระบบจะแสดงข้อความดังรูปที่ 4.37

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

วิเคราะห์ความเสี่ยง แสดงผลการวิเคราะห์ความเสี่ยง การจัดการคำถาม การจัดการผู้ใช้ การเปลี่ยนรหัสผ่าน ตัวช่วย ออกจากระบบ

ขั้นตอน    เพิ่ม ลบ แก้ไข คำถาม

รายการคำถาม

องค์กรมีการนำ IT มาเป็นส่วนหนึ่งของแผนการระยะสั้นและระยะยาวขององค์กรอย่างไร

ขอบเขตของแผนการ IT ระยะยาวเป็นอย่างไร

มีการวางแผน IT ระยะยาวไว้กับแนวคิดและโครงสร้างอย่างไร

องค์กรมีการเปลี่ยนแปลงแผนการ IT ระยะยาวอย่างไร

คำถาม    องค์กรมีการเปลี่ยนแปลงแผนการ IT ระยะยาวอย่างไร

0	ไม่มีการเปลี่ยนแปลงแผนการ IT ระยะยาว
1	มีการเปลี่ยนแปลงโดยไม่มีการแจ้งหรือระบุไว้ชัดเจนอย่างเป็นทางการ
2	การเปลี่ยนแปลงแผนการ IT ระยะยาวจะเกิดขึ้นโดยพิจารณาช่วงเวลาที่เหมาะสม
3	2 + มีการพิจารณาผลกระทบต่อแผนการระยะสั้นและระยะยาวขององค์กร รวมถึงการเปลี่ยนสถานะของ IT
4	3 + มีการกำหนดนโยบายที่เกี่ยวข้องกับแผนการ IT ระยะสั้นและระยะยาวเพิ่มขึ้นมาใหม่ และจะต้องถูกรักษาไว้

ต้องการเพิ่มคำถามใหม่

แก้ไขคำถาม

ลบคำถาม

เสร็จสิ้นแล้ว

รูปที่ 4.35 หน้าจอรายการคำถามในโดเมนย่อยที่เลือก

คำถาม	องค์กรมีการเปลี่ยนแปลงแผนการ IT ระยะยาวอย่างไร
0	ไม่มีการเปลี่ยนแปลงแผนการ IT ระยะยาว
1	มีการเปลี่ยนแปลงโดยไม่มีการแจ้งหรือระบุไว้ชัดเจนอย่างเป็นทางการ
2	การเปลี่ยนแปลงแผนการ IT ระยะยาวจะเกิดขึ้นโดยพิจารณาช่วงเวลาที่เหมาะสม
3	2 + มีการพิจารณาผลกระทบต่อแผนการระยะสั้นและระยะยาวขององค์กร รวมถึงการเปลี่ยนสถานะของ IT
4	3 + มีการกำหนดนโยบายที่เกี่ยวข้องกับแผนการ IT ระยะสั้นและระยะยาวเพิ่มขึ้นมาใหม่ และจะต้องถูกรักษาไว้

รูปที่ 4.36 คำถามและคำตอบที่ต้องการจะแก้ไข

การเพิ่มคำถามผิดพลาด

กรุณากรอกคำถามและคำตอบให้ครบก่อนทำการเพิ่ม

ตกลง

รูปที่ 4.37 ข้อความเตือนเมื่อกรอกคำถามและคำตอบไม่ครบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#### 4.5 การจัดการผู้ใช้งานระบบ

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิปุ่มการจัดการผู้ใช้งานระบบหรือคลิกการจัดการผู้ใช้งานที่เมนูข้างบน โดยผู้ดูแลระบบเท่านั้นที่มีสิทธิในการเข้าใช้ส่วนนี้ หลังจากนั้นระบบจะแสดงหน้าจอการจัดการผู้ใช้งานระบบดังรูปที่ 4.38 ซึ่งจะเป็นการแสดงรายการผู้ใช้งานระบบทั้งหมด

กรณีต้องการเพิ่มรายการผู้ใช้งานระบบ ผู้ดูแลระบบสามารถกรอกข้อมูลผู้ใช้งานระบบ แล้วคลิกปุ่มเพิ่มผู้ใช้งานระบบ ถ้าใส่ข้อมูลไม่ครบระบบจะแสดงข้อความเตือนลักษณะเดียวกันกับรูป 4.37

กรณีต้องการลบรายการผู้ใช้งานระบบ ผู้ดูแลระบบสามารถเลือกรายการผู้ใช้งานระบบที่ต้องการลบแล้วคลิกปุ่มลบผู้ใช้งานระบบ ระบบจะแสดงข้อความยืนยันการลบ เมื่อผู้ใช้งานยืนยัน ระบบจะทำการลบรายการผู้ใช้งานระบบ ที่เลือกออกไป

ประเภทของผู้ใช้งานระบบแบ่งออกเป็น 3 ประเภท คือ ผู้ดูแลระบบ นักวิเคราะห์ระบบ และผู้ใช้งานทั่วไป โดยผู้ใช้แต่ละประเภทยังมีสิทธิในการใช้ระบบไม่เท่ากัน โดยรายละเอียดเกี่ยวกับผู้ใช้งานระบบแสดงไว้ด้านซ้ายของหน้าจอการจัดการผู้ใช้งานระบบ ดังรูปที่ 4.39

The screenshot shows a web application interface for user management. At the top, there are navigation tabs: "วิเคราะห์ความเสี่ยง", "แสดงผลการวิเคราะห์ความเสี่ยง", "การจัดการค่าฐาน", "การจัดการผู้ใช้", "การเปลี่ยนรหัสผ่าน", "ตัวช่วย", and "ออกจากระบบ". Below these are buttons for "ขั้นตอน" and "เพิ่ม ลบ ผู้ใช้งานระบบ".

The main content area is divided into two sections:

- เพิ่ม ลบ รายชื่อผู้ใช้งานระบบ**: A table listing users with columns for ID, Username, Password, and Role.
 

รหัสผู้ใช้	ชื่อผู้ใช้	รหัสผ่าน	ประเภท
1	admin	a7s8d9f0	1
2	user1	111	2
3	user2	222	3
4	user3	333	3
5	user4	444	2
6	ส	1	1
12	user5	555	3
14	user7	777	1
15	user8	888	2
17	user9	999	2
- รายละเอียดเกี่ยวกับประเภทของผู้ใช้งานระบบ**: A table defining user roles and their permissions.
 

ประเภทของผู้ใช้งานระบบ	1	2	3
1 ผู้ดูแลระบบ	สามารถใช้งานได้ทุกส่วนของระบบ		
2 นักวิเคราะห์ความเสี่ยง	สามารถใช้งานในส่วนวิเคราะห์ความเสี่ยงได้		
3 ผู้ใช้งานทั่วไป	สามารถดูผลการวิเคราะห์ความเสี่ยงได้อย่างเดียว		

At the bottom, there are input fields for "ชื่อผู้ใช้", "รหัสผ่าน", and "ประเภท" (with a dropdown menu), and buttons for "เพิ่มผู้ใช้งานระบบ" and "ลบผู้ใช้งานระบบ". A "เสร็จสิ้นแล้ว" button is at the very bottom.

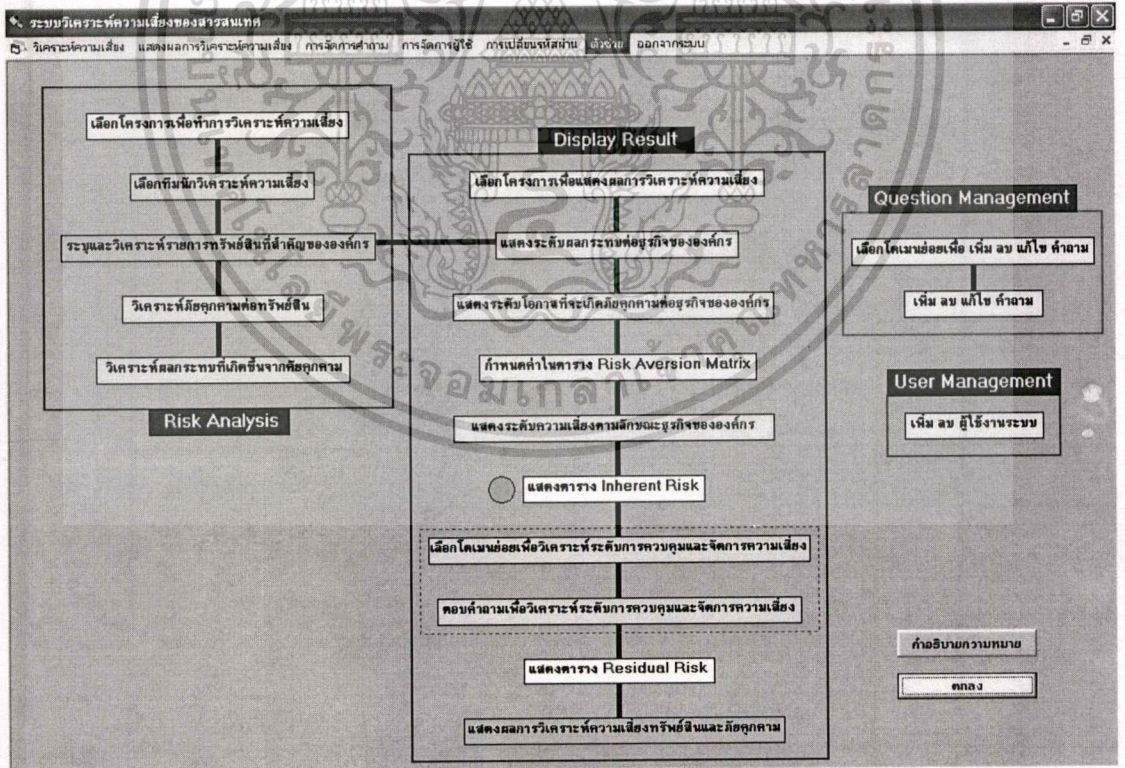
รูปที่ 4.38 หน้าจอการจัดการผู้ใช้งานระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประเภทของผู้ใช้ระบบ		
1	ผู้ดูแลระบบ	สามารถใช้งานได้ทุกส่วนของระบบ
2	นักวิเคราะห์ความเสี่ยง	สามารถใช้ระบบในส่วนวิเคราะห์ความเสี่ยงได้
3	ผู้ใช้ทั่วไป	สามารถดูผลการวิเคราะห์ความเสี่ยงได้อย่างเดียว

ระดับสิทธิในการใช้ระบบ	ประเภทของผู้ใช้ระบบ		
	1	2	3
สร้างโครงการวิเคราะห์ความเสี่ยงใหม่	●	●	
แก้ไขโครงการใดๆ ที่มีอยู่	●		
ลบโครงการใดๆ ที่มีอยู่ทิ้ง	●		
แก้ไขโครงการที่ตนเองสร้างขึ้น		●	
ลบโครงการที่ตนเองสร้างขึ้น		●	
ดูผลการวิเคราะห์ความเสี่ยง	●	●	●
เพิ่ม ลบ แก้ไข ค่าตามเกี่ยวกับการจัดการความเสี่ยง			
เพิ่ม ลบ แก้ไข เกี่ยวกับข้อมูลของผู้ใช้ระบบ			

รูปที่ 4.39 รายละเอียดเกี่ยวกับผู้ใช้ระบบ



รูปที่ 4.40 หน้าจอแสดงสถานะการใช้งานระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 4.40 เป็นหน้าจอแสดงสถานะการใช้งานระบบซึ่งสามารถเรียกใช้ได้ตลอดเวลา โดยคลิกที่เมนูตัวช่วยที่อยู่บนแท็บเมนู ประโยชน์ของหน้าจอแสดงสถานะการใช้งานระบบ คือ ช่วยให้ผู้ใช้งานระบบสามารถรู้ได้ว่าขณะนี้ตนเองกำลังอยู่ในขั้นตอนไหนและส่วนไหนของระบบ ซึ่งจะช่วยให้ผู้ใช้งานระบบไม่เกิดความสับสน จากตัวอย่างในรูปที่ 4.40 เป็นการบอกว่า ขณะนี้ผู้ใช้กำลังอยู่ในขั้นตอนแสดงตารางความเสี่ยงถาวร



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 5

### การพัฒนากระบวนการวิเคราะห์ความเสี่ยงของสารสนเทศ

#### 5.1 รูปแบบการพัฒนากระบวนการและวิธีการคำนวณที่ใช้ในการวิเคราะห์ความเสี่ยง

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ ได้ทำการพัฒนาเป็น Window GUI แอปพลิเคชัน (วินโดวส์ฟอร์ม) หรือโปรแกรมที่ทำงานบนไมโครซอฟต์วินโดวส์ โดยมี RiskAnalysis.exe เป็นโปรแกรมหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

การพัฒนากระบวนการวิเคราะห์ความเสี่ยงของสารสนเทศใช้โปรแกรม Visual Basic ในการพัฒนา และใช้ Microsoft Access เป็นระบบจัดการฐานข้อมูล โดยมีการนำแนวคิดการวิเคราะห์ความเสี่ยงต่างๆ มาประยุกต์ใช้เพื่อเป็นแนวทางในการพัฒนา

กระบวนการทำงานของระบบในการวิเคราะห์ความเสี่ยงจะประกอบด้วยการวิเคราะห์ที่สำคัญ ดังนี้

##### 5.1.1 การวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร

เป็นการวิเคราะห์ว่าในองค์กรมีทรัพย์สินอะไรบ้าง และทรัพย์สินแต่ละรายการมีระดับความสำคัญแค่ไหนและมีภัยคุกคามอะไรบ้าง โดยมีกระบวนการทำงานดังนี้

1. ทีมนักวิเคราะห์กำหนดทรัพย์สินที่สำคัญขององค์กร
2. วิเคราะห์ระดับความสำคัญของทรัพย์สิน ดังนี้

$$\text{AssetValue} = \frac{[(\text{Analyst1} \times \text{Credit1}) + (\text{Analyst2} \times \text{Credit2}) + \dots + (\text{AnalystN} \times \text{CreditN})]}{[\text{Credit1} + \text{Credit2} + \dots + \text{CreditN}]}$$

โดยที่ AssetValue คือ ค่าระดับความสำคัญของทรัพย์สิน ซึ่งมีค่าระหว่าง 0 ถึง 4

AnalystN คือ คำตอบของนักวิเคราะห์คนที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

CreditN คือ ระดับความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ N มีค่าระหว่าง 0 ถึง 4

3. วิเคราะห์ภัยคุกคามต่อทรัพย์สิน ซึ่งอธิบายไว้ในหัวข้อถัดไป

##### 5.1.2 การวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

เป็นการวิเคราะห์ว่าทรัพย์สินที่สำคัญมีภัยคุกคามอะไรบ้าง และภัยคุกคามแต่ละรายการมีโอกาสที่จะเกิดขึ้นแค่ไหนและมีผลกระทบอะไรบ้าง โดยมีกระบวนการทำงานดังนี้

1. ทีมนักวิเคราะห์กำหนดรายการภัยคุกคามต่อทรัพย์สิน

## 2. วิเคราะห์โอกาสที่จะเกิดภัยคุกคาม ดังนี้

$$\text{Likelihood} = \frac{[(\text{Analyst1} \times \text{Credit1}) + (\text{Analyst2} \times \text{Credit2}) + \dots + (\text{AnalystN} \times \text{CreditN})]}{[\text{Credit1} + \text{Credit2} + \dots + \text{CreditN}]}$$

โดยที่ Likelihood คือ ค่าโอกาสที่จะเกิดภัยคุกคาม ซึ่งมีค่าระหว่าง 0 ถึง 4

AnalystN คือ คำตอบของนักวิเคราะห์คนที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

CreditN คือ ระดับความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ N มีค่าระหว่าง 0 ถึง 4

## 3. วิเคราะห์ผลกระทบจากภัยคุกคาม ซึ่งอธิบายไว้ในหัวข้อถัดไป

### 5.1.3 การวิเคราะห์ผลกระทบจากภัยคุกคาม

เป็นการวิเคราะห์ว่าภัยคุกคามส่งผลกระทบต่อการทำงานขององค์กรในระดับไหน โดยมีกระบวนการทำงานดังนี้

วิเคราะห์ระดับผลกระทบจากภัยคุกคาม ดังนี้

$$\text{ImpactValue} = \frac{[(\text{Analyst1} \times \text{Credit1}) + (\text{Analyst2} \times \text{Credit2}) + \dots + (\text{AnalystN} \times \text{CreditN})]}{[\text{Credit1} + \text{Credit2} + \dots + \text{CreditN}]}$$

โดยที่ ImpactValue คือ ค่าผลกระทบจากภัยคุกคาม ซึ่งมีค่าระหว่าง 0 ถึง 4

AnalystN คือ คำตอบของนักวิเคราะห์คนที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

CreditN คือ ระดับความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ N มีค่าระหว่าง 0 ถึง 4

### 5.1.4 การวิเคราะห์ผลกระทบต่อองค์กร

เป็นการวิเคราะห์ว่าจากภัยคุกคามทั้งหมดมีผลกระทบต่อองค์กรในระดับไหน โดยมีวิธีการคำนวณดังนี้

$$\text{AssetImpact} = (\text{ImpactValue1} + \text{ImpactValue2} + \dots + \text{ImpactValueN}) / (\text{TotalThreat})$$

$$\text{BusinessImpact} = \frac{[(\text{AssetImpact1} \times \text{AssetValue1}) + \dots + (\text{AssetImpactN} \times \text{AssetValueN})]}{[\text{AssetValue1} + \text{AssetValue2} + \dots + \text{AssetValueN}]}$$

โดยที่ BusinessImpact คือ ระดับผลกระทบต่อองค์กร ซึ่งมีค่าระหว่าง 0 ถึง 4

AssetImpactN คือ ค่าผลกระทบเฉลี่ยต่อทรัพย์สินรายการที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

ImpactValueN คือ ค่าผลกระทบจากภัยคุกคามรายการที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

TotalThreat คือ จำนวนของภัยคุกคามทั้งหมดที่มีต่อทรัพย์สินนั้น

AssetValueN คือ ค่าระดับความสำคัญของทรัพย์สินรายการที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

### 5.1.5 การวิเคราะห์โอกาสที่จะเกิดภัยคุกคามต่อองค์กร

เป็นการวิเคราะห์ว่าจากภัยคุกคามทั้งหมดมีโอกาสที่จะเกิดขึ้นกับองค์กรในระดับไหน โดยมีวิธีการคำนวณดังนี้

$$\text{BusinessLikelihood} = \frac{[(\text{Likelihood1} \times \text{ImpactValue1}) + \dots + (\text{LikelihoodN} \times \text{ImpactValueN})]}{[\text{Likelihood1} + \text{Likelihood2} + \dots + \text{LikelihoodN}]}$$

โดยที่ BusinessLikelihood คือ ระดับโอกาสที่จะเกิดภัยคุกคามต่อองค์กร ซึ่งมีค่าระหว่าง 0 ถึง 4

LikelihoodN คือ ค่าโอกาสที่จะเกิดภัยคุกคามรายการที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

ImpactValueN คือ ค่าผลกระทบจากภัยคุกคามรายการที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

### 5.1.6 การวิเคราะห์ความระดับเสี่ยงขององค์กร

เป็นการวิเคราะห์ความว่าองค์กรมีความเสี่ยงในระดับไหน โดยคำนวณจากโอกาสที่จะเกิดภัยคุกคามกับผลกระทบต่อองค์กร โดยคำนวณจากการกำหนดค่าในตาราง Risk Aversion Table ซึ่งแสดงไว้ในบทที่ 4 รูปที่ 4.22

### 5.1.7 การวิเคราะห์การควบคุมและจัดการความเสี่ยง

เป็นการวิเคราะห์ว่าองค์กรมีการควบคุมและจัดการความเสี่ยงไปแล้วในระดับไหน โดยมีวิธีการคำนวณดังนี้

$$\text{Answer} = \frac{[(\text{Analyst1} \times \text{Credit1}) + (\text{Analyst2} \times \text{Credit2}) + \dots + (\text{AnalystN} \times \text{CreditN})]}{[\text{Credit1} + \text{Credit2} + \dots + \text{CreditN}]}$$

$$\text{SubDomain} = \frac{[\text{Answer1} + \text{Answer2} + \dots + \text{AnswerN}]}{[\text{TotalAnswer}]}$$

โดยที่ Answer คือ คำตอบเกี่ยวกับการควบคุมความเสี่ยง ซึ่งมีค่าระหว่าง 0 ถึง 4

AnalystN คือ คำตอบของนักวิเคราะห์คนที่ N ซึ่งมีค่าระหว่าง 0 ถึง 4

CreditN คือ ระดับความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ N มีค่าระหว่าง 0 ถึง 4

SubDomain คือ ค่าระดับการควบคุมความเสี่ยงของโดเมนย่อย ซึ่งมีค่าระหว่าง 0 ถึง 4

TotalAnswer คือ จำนวนคำถามทั้งหมดในโดเมนย่อยที่ตอบไป

### 5.1.8 การวิเคราะห์ความเสี่ยงของทรัพย์สินในองค์กร

เป็นการวิเคราะห์ว่าในองค์กรมีทรัพย์สินที่มีความเสี่ยงในระดับไหน โดยมีวิธีการคำนวณดังนี้

$$\text{AssetRisk} = \text{AssetValue} \times (\text{Likelihood1} + \text{Likelihood2} + \dots + \text{LikelihoodN}) \times (\text{ImpactValue1} + \text{ImpactValue} + \dots + \text{ImpactValueN})$$

โดยที่ AssetRisk คือ ค่าระดับความเสี่ยงของทรัพย์สิน

AssetValue คือ ค่าระดับความสำคัญของทรัพย์สิน ซึ่งมีค่าระหว่าง 0 ถึง 4

Likelihood คือ ค่าโอกาสที่จะเกิดภัยคุกคามต่อทรัพย์สิน ซึ่งมีค่าระหว่าง 0 ถึง 4

ImpactValue คือ ค่าผลกระทบจากภัยคุกคามต่อทรัพย์สิน ซึ่งมีค่าระหว่าง 0 ถึง 4

**5.19 การวิเคราะห์ความเสี่ยงของภัยคุกคาม**

เป็นการวิเคราะห์ว่าในองค์กรมีภัยคุกคามที่มีความเสี่ยงในระดับไหน โดยมีวิธีการคำนวณดังนี้

$$\text{ThreatRisk} = \text{Likelihood} \times (\text{ImpactValue1} + \text{ImpactValue} + \dots + \text{ImpactValueN})$$

โดยที่ ThreatRisk คือ ค่าระดับความเสี่ยงของภัยคุกคาม

Likelihood คือ ค่าโอกาสที่จะเกิดภัยคุกคาม ซึ่งมีค่าระหว่าง 0 ถึง 4

ImpactValue คือ ค่าผลกระทบจากภัยคุกคาม ซึ่งมีค่าระหว่าง 0 ถึง 4

**5.2 โครงสร้างฐานข้อมูล**

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ เลือกใช้ Microsofe Access เป็นระบบจัดการฐานข้อมูล โดยจากคลาสไดอะแกรมในรูปที่ 3.27 สามารถนำมาออกแบบตารางเพื่อให้เหมาะสมกับระบบ

จากนี้ไปจะเป็นแสดงให้เห็นถึง โครงสร้างของตารางในฐานข้อมูลทั้งหมดของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ โดยภายในแต่ละตารางแสดง ชื่อแอตทริบิวต์ แอตทริบิวต์ที่เป็น Primary Key หรือ Foreign Key ซึ่งแสดงแทนด้วย PK และ FK ตามลำดับ ถัดมาแสดงชนิดและขนาดของข้อมูล และสุดท้ายแสดงความหมายของแต่ละแอตทริบิวต์ในแต่ละตาราง

ตารางที่ 5.1 โครงสร้างของตาราง Analyst

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
AnalystID	PK	Integer	รหัสนักวิเคราะห์ความเสี่ยง
FName		String	ชื่อนักวิเคราะห์ความเสี่ยง
LName		String	นามสกุลนักวิเคราะห์ความเสี่ยง
PosID	FK	Integer	ตำแหน่งงานของนักวิเคราะห์ความเสี่ยงในองค์กร
TaskID	FK	Integer	รหัสโครงการ

ตารางที่ 5.2 โครงสร้างของตาราง Answer

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
AnswerID	PK	Integer	รหัสคำตอบ
DomainID	FK	Integer	รหัสโดเมนของ CobiT
SubDomain		Integer	รหัสโดเมนย่อยของ CobiT
Question		String	คำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง
Status		String	สถานะการตอบคำถาม
Ans		Single	ค่าคำตอบ
TaskID	FK	Integer	รหัสโครงการ
Analyst1		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 1
Credit1		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ 1
Analyst2		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 2
Credit2		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ 2
Analyst3		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 3
Credit3		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ 3
Analyst4		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 4
Credit4		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ 4
Analyst5		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 5
Credit5		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่ 5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.3 โครงสร้างของตาราง Asset

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
AssetID	PK	Integer	รหัสทรัพย์สินที่สำคัญขององค์กร
Asset		String	ทรัพย์สินที่สำคัญขององค์กร
Status		String	สถานะการวิเคราะห์ระดับความสำคัญของทรัพย์สิน
Value		Single	ค่าการผลการวิเคราะห์ระดับความสำคัญของทรัพย์สิน
TotalTheat		Integer	จำนวนภัยคุกคามทั้งหมดของทรัพย์สิน
TotalLikelihood		Single	ผลรวมของโอกาสที่จะเกิดภัยคุกคามของทรัพย์สิน
TotalImpactAVG		Single	ผลรวมของค่าเฉลี่ยของผลกระทบ
Analyst1		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 1
Credit1		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่1
Analyst2		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 2
Credit2		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่2
Analyst3		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 3
Credit3		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่3
Analyst4		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 4
Credit4		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่4
Analyst5		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 5
Credit5		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้คัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.4 โครงสร้างของตาราง Domain

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
DomainID	PK	Integer	รหัสโดเมนของ CobiT
Domain		String	โดเมนของ CobiT
Des		String	คำอธิบายโดเมนของ CobiT

ตารางที่ 5.5 โครงสร้างของตาราง Impact

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
ImpactID	PK	Integer	รหัสผลกระทบภัยคุกคาม
Impact		String	ผลกระทบจากภัยคุกคาม
Status		String	สถานะการวิเคราะห์ผลกระทบจากภัยคุกคาม
Value		Single	ค่าผลการวิเคราะห์ผลกระทบจากภัยคุกคาม
ThreatID	FK	Integer	รหัสภัยคุกคาม
Analyst1		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 1
Credit1		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่1
Analyst2		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 2
Credit2		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่2
Analyst3		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 3
Credit3		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่3
Analyst4		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 4
Credit4		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่4
Analyst5		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 5
Credit5		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่5

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 5.6 โครงสร้างของตาราง Position

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
PosID	PK	Integer	รหัสตำแหน่งงานในองค์กร
PosName		String	ตำแหน่งงานในองค์กร

ตารางที่ 5.7 โครงสร้างของตาราง Question

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
QuestID	PK	Integer	รหัสคำถาม
DomainID	FK	Integer	รหัสโดเมนของ CobiT
SubDomain	FK	Integer	โดเมนย่อยของ CobiT
Question		String	คำถามเกี่ยวกับการควบคุมจัดการความเสี่ยง
Ans0		String	ตัวเลือกที่ 1 ของคำถามการควบคุมจัดการความเสี่ยง
Ans1		String	ตัวเลือกที่ 2 ของคำถามการควบคุมจัดการความเสี่ยง
Ans2		String	ตัวเลือกที่ 3 ของคำถามการควบคุมจัดการความเสี่ยง
Ans3		String	ตัวเลือกที่ 4 ของคำถามการควบคุมจัดการความเสี่ยง
Ans4		String	ตัวเลือกที่ 5 ของคำถามการควบคุมจัดการความเสี่ยง

ตารางที่ 5.8 โครงสร้างของตาราง Sub Domain

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
SubDomainID	PK	Integer	รหัส โดเมนย่อยของ CobiT
DomainID	FK	Integer	รหัส โดเมนของ CobiT
SubDomain		Integer	โดเมนย่อยของ CobiT
Name		String	ชื่อ โดเมนย่อย
Status		String	สถานะการวิเคราะห์การควบคุมและจัดการ ความเสี่ยง
Value		Single	ค่าผลการวิเคราะห์การควบคุมและจัดการ ความเสี่ยง
TaskID	FK	Integer	รหัส โครงการ

ตารางที่ 5.9 โครงสร้างของตาราง Threat

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
ThreatID	PK	Integer	รหัสภัยคุกคาม
Threat		String	ภัยคุกคาม
Status		String	สถานะการวิเคราะห์โอกาสที่จะเกิดภัย คุกคาม
Likelihood		Single	โอกาสที่จะเกิดภัยคุกคาม
ImpactAVG		Single	ค่าเฉลี่ยของผลกระทบจากภัยคุกคาม
AssetID	FK	Integer	รหัสทรัพย์สิน
Analyst1		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 1
Credit1		Integer	ค่าความมั่นใจในการตอบคำถามของ นักวิเคราะห์คนที่ 1
Analyst2		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 2
Credit2		Integer	ค่าความมั่นใจในการตอบคำถามของ นักวิเคราะห์คนที่ 2
Analyst3		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 3

ตารางที่ 5.9 โครงสร้างของตาราง Theat (ต่อ)

ชื่อแอตทริบิวต์	ชนิดข้อมูล	ความหมาย
Credit3	Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่3
Analyst4	Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 4
Credit4	Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่4
Analyst5	Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 5
Credit5	Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่5

ตารางที่ 5.10 โครงสร้างของตาราง Title

ชื่อแอตทริบิวต์	ชนิดข้อมูล	ความหมาย
TaskID	PK Integer	รหัส โครงการ
TaskName	String	ชื่อ โครงการ
Organization	String	ชื่อองค์กร
TotalAssetValue	Single	ผลรวมของระดับความสำคัญของทรัพย์สิน
TotalLikelihood	Single	ผลรวมของ โอกาสภัยคุกคามที่จะเกิดขึ้น
UserID	FK Integer	รหัสผู้ใช้ที่สร้างโครงการ

ตารางที่ 5.11 โครงสร้างของตาราง User

ชื่อแอตทริบิวต์	ชนิดข้อมูล	ความหมาย
UserID	PK Integer	รหัสผู้ใช้งานระบบ
UserName	String	ชื่อผู้ใช้งานระบบ
Password	String	รหัสผ่านผู้ใช้งานระบบ
UserType	FK Integer	ประเภทของผู้ใช้งานระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

## บทที่ 6

### สรุป

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศเป็นระบบที่นำเอาระบบคอมพิวเตอร์เข้ามาช่วยในการวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กร เพื่ออำนวยความสะดวกให้นักวิเคราะห์ความเสี่ยงสามารถวิเคราะห์ความเสี่ยงได้อย่างรวดเร็วและเป็นระบบ เพื่อช่วยวิเคราะห์และประเมินความเสี่ยง ซึ่งผลการวิเคราะห์ความเสี่ยงสามารถนำมาใช้เป็นแนวทางในการแก้ไขความเสี่ยงได้

การพัฒนาาระบบวิเคราะห์ความเสี่ยงของสารสนเทศ มีการศึกษาแนวคิดและวิธีการวิเคราะห์และประเมินความเสี่ยงหลายๆแนวคิดมาใช้เป็นแนวทางในการพัฒนาระบบ โดยแนวคิดต่างๆที่ศึกษาเพื่อนำมาเป็นแนวทางในการพัฒนา ได้แก่ OCTAVE ,CobiT ,FRAP และ BIA ส่วนแนวคิดหลักที่นำมาใช้เป็นมาตรฐานในการพัฒนาระบบ คือ CobiT ซึ่งเป็นแนวคิดและแนวทางการปฏิบัติเพื่อการควบคุมด้านเทคโนโลยีสารสนเทศสำหรับองค์กร โดยโครงสร้างของ CobiT ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศใช้ UML ช่วยในการออกแบบ ซึ่งมีการใช้โมเดลต่างๆมาช่วยอธิบายระบบงานนั้นๆ ทำให้สามารถแสดงภาพรวมของระบบทั้งหมดได้อย่างชัดเจน และช่วยให้นักวิเคราะห์ระบบ นักพัฒนาและผู้ใช้ มีมุมมองที่เข้าใจตรงกัน ทำให้การพัฒนากระบวนการเป็นไปอย่างรวดเร็ว

ผลการวิเคราะห์ความเสี่ยงที่ได้จากการวิเคราะห์จะสามารถบอกได้ว่าทรัพย์สินใดในองค์กรมีความเสี่ยงในระดับใดบ้าง องค์กรมีความเสี่ยงจากภัยคุกคามอะไรบ้าง ในระดับไหน ทำให้ช่วยตัดสินใจได้ว่าควรพิจารณาทรัพย์สินใดและภัยคุกคามใดเป็นอันดับแรก นอกจากนั้นยังให้คำแนะนำว่าควรมีการเพิ่มหรือลดการควบคุมและจัดการความเสี่ยงในแต่ละโดเมนย่อยของ CobiT แต่อย่างไรก็ตาม ระบบวิเคราะห์ความเสี่ยงของสารสนเทศไม่สามารถช่วยแก้ไขความเสี่ยงที่เกิดขึ้นได้ เพียงแต่เป็นระบบที่ช่วยในการวิเคราะห์ความเสี่ยงและช่วยแนะนำว่าควรทำอย่างไร จึงเป็นหน้าที่ของผู้ดูแลระบบและผู้ที่เกี่ยวข้อง ในการวางแผนแก้ไขและจัดการความเสี่ยงเหล่านั้นต่อไป

## บรรณานุกรม

- ชาติ วรกุลพิพัฒน์ และเทพฤทธิ์ บัณฑิตพัฒน์. 2544. **UML ภาษามาตรฐานเพื่อผู้พัฒนาซอฟต์แวร์**. กรุงเทพฯ: ซีเอ็ดยูเคชั่น.
- วุฒิพงษ์ พงศ์สุวรรณ. 2543. **How to learn Visual Basic**. กรุงเทพฯ: ซอร์ฟแวร์ ปาร์ค.
- วรรณวิภา ติตละสิริ. 2545. **คู่มือเรียน SQL ด้วยตัวเอง**. กรุงเทพฯ: โปรวิชั่น.
- ศุภชัย สมพรนิช. 2543. **Database Programming ด้วย Visual Basic ฉบับมืออาชีพ**. กรุงเทพฯ: อินโฟเพรส.
- Audrey Dorofee and Christopher Albert. 2002. **Managing Information Security Risks : The OCTAVE Approach**. New Jersey: Addison Wesley.
- Harold F. Tipton and Micki Krause. 2000. **Information Security Management Handbook, Fourth Edition, Volume 2**. New York: Auerbach Publications.
- Leah Jenczewski. 2002. **Internet and Intranet Security Management : Risk and Solutions**. California: Idea Group Publishing.
- Linda McCarthy. 2003. **IT Security : Risking the Coperation**. San Francisco: Pearson Education Inc.
- Thomas R. Peltier. 2002. **Information Security Risk Analysis**. New York: Auerbach Publications.

## ประวัติผู้เขียน

ชื่อผู้เขียน	นายคชพงศ์ เพ็ชรราช
วันเดือนปีเกิด	1 กันยายน 2521
สถานที่เกิด	อ.เมือง จ.แพร่
ที่อยู่ปัจจุบัน	12/19 ถ.เกษฎาบดีนทร์เหนือ ต.ท่าอิฐ อ.เมือง จ.อุตรดิตถ์ 53000
วุฒิการศึกษาปริญญาตรี	วศ.บ. (วิศวกรรมคอมพิวเตอร์)
สถานที่สำเร็จการศึกษาระดับปริญญาตรี	คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร
ปีที่สำเร็จการศึกษา	ปีการศึกษา 2544



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า  
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้