การพัฒนาระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

DEVELOPMENT OF RISK MANAGEMENT SYSTEM IN INFORMATION SYSTEM

บุญเรือง สีดาพันธ์

BOONRUANG SEEDAPUNT

อาจารย์ที่ปรึกษา

ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2550

DEVELOPMENT OF RISK MANAGEMENT SYSTEM IN INFORMATION SYSTEM

BOONRUANG SEEDAPUNT

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF SCIENCE

PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2007

หัวข้อ	การพัฒนาระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ
นักศึกษา	นายบุญเรือง สีดาพันธ์
รหัสนักศึกษา	47066615
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2550
อาจารย์ที่ปรึกษา	ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

ปัจจุบันมีแนวทางการบริหารจัดการระบบสารสนเทศหลายวิธีการด้วยกัน ทั้งมาตรฐานสากล และกรอบการปฏิบัติงานที่ได้ผลดีเพื่อสนับสนุนให้องค์กรมีระบบการบริหารจัดการที่ดี เพื่อให้ได้มาซึ่งวิธีการ และมาตรฐานเหล่านี้ระบบสารสนเทศจำเป็นต้องมีวิธีการบริหารจัดการความเสี่ยง ซึ่งแนวทางการบริหารจัดการความเสี่ยงมีอยู่หลายวิธีการด้วยกัน โดยโครงการพัฒนาระบบงานนี้ได้เลือกนำแนวทางการบริหารจัดการความเสี่ยงในระบบสารสนเทศของ NIST SP800-30 เป็นแนวทางในการวิเคราะห์และออกแบบระบบ ซึ่งได้เสนอวิธีการวิเคราะห์ ประเมินความเสี่ยง และสร้างแผนในการควบคุมและป้องกันความเสี่ยง ที่เน้นมุมมองถึงปัญหาความปลอดภัยในระบบสารสนเทศ โดยการแสดงถึงภัยคุกคาม จุดอ่อน และระดับผลกระทบที่มีโอกาสเกิดขึ้น โดยการวิเคราะห์และออกแบบระบบใช้แนวทางเชิงวัตถุด้วยภาษา UML

Title	Development of Risk Management System in Information System
Student	Mr. Boonruang Seedapunt
Student ID.	47066615
Degree	Master of Science
Programme	Information Science
Academic Year	2007
Advisor	Asst.Prof. Dr.Chanboon Sathitwiriyawong

ABSTRACT

Nowadays, there are several ways of the management standard of information system, two of them are standard and best practice frameworks for high quality of services in IT services. To accomplish and compliance with these standard and framework, the information system needs the appropriate way of risk management for implementation. This Development Project is aim to take the NIST SP800-30 approach to analyses and design the system. This approach is object to guide the risk assessment methodology and to prepare for create the mitigation plan or treatment plan from the impact of information security system. The approach guide to identify threat, vulnerability, and level of risk impact and for this system analysis and design are using object-oriented approach with UML.

กิตติกรรมประกาศ

ในการจัดทำโครงการพัฒนาระบบระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศนี้ ได้รับการสนับสนุนเป็นอย่างดี จากหลายฝ่ายที่คอยให้คำแนะนำปรึกษา และเสียสละเวลาอันมีค่า จนทำให้ศึกษาโครงการนี้บรรลุผลตามเป้าหมายที่วางไว้ ผู้จัดทำจึงใคร่ขอขอบพระคุณ

1. บิดามารดา ที่คอยเป็นกำลังใจในการทำงาน
2. ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษาโครงการที่ได้ให้ความรู้ คำแนะนำ คำปรึกษาในการจัดทำโครงการ
3. อาจารย์ทุกๆท่าน ที่สั่งสอนให้ข้าพเจ้าคิดเป็น และปฏิบัติเป็น รวมทั้งตัดสินในในการแก้ปัญหาต่างๆจากความรู้พื้นฐานที่ได้ศึกษามา
4. เพื่อนร่วมงานบริษัท สามารถ คอร์ปอเรชั่น จำกัด มหาชน ที่ให้คำแนะนำ คำปรึกษาเป็นอย่างดีในการพัฒนาระบบ

บุญเรือง สีดาพันธ์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป(ต่อ)

บทที่ 1
บทนำ

1.1 วัตถุประสงค์ของการพัฒนาระบบ

ระบบบริหารจัดการความเสี่ยงมีความสำคัญต่อการทำให้ระบบสารสนเทศมีความมั่นคงและปลอดภัย ในขั้นตอนการบริหารจัดการ มีการวัดและประเมินความเสี่ยงของทรัพย์สินในระบบสารสนเทศที่อาจเป็นสาเหตุให้เกิดความบกพร่องแก่ทรัพย์สินในระบบสารสนเทศ ทรัพย์สินประกอบด้วยอุปกรณ์ฮาร์ดแวร์ ซอฟท์แวร์ เอกสารต่างๆ บุคลากร และบริการต่างๆ ซึ่งควรได้รับการวางแผนการเพื่อรองรับกับภัยคุกคามที่สามารถทำให้เกิดผลกระทบทางด้านความปลอดภัย มีการวางแผนเพื่อลดและบรรเทาผลกระทบที่ส่งผลต่อการดำเนินธุรกิจหรือการปฏิบัติงานขององค์กร โดยวัตถุประสงค์ของการพัฒนาระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศมีดังต่อไปนี้

1. เพื่อใช้ในการรวบรวมข้อมูลทรัพย์สินในระบบสารสนเทศภายขอบเขตที่ได้กำหนดไว้เพื่อเป็นเป้าหมายในการสร้างระบบความปลอดภัย
2. เพื่อการวิเคราะห์ความเสี่ยงภายในระบบสารสนเทศ
3. เพื่อลดขั้นตอนและความซ้ำซ้อนในการปฏิบัติงานได้
4. เพื่อให้มีระบบการบริหารจัดการความเสี่ยงที่สามารถนำผลการวิเคราะห์ที่ได้มาใช้ได้อย่างมีประสิทธิภาพ
5. เพื่อนำเสนอผลการวิเคราะห์อยู่ในรูปกราฟแบบต่างๆเพื่อให้เข้าใจถึงความเสี่ยงที่เกิดขึ้นภายในระบบสารสนเทศ

1.2 วิธีการในการพัฒนาระบบ

การพัฒนาระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ ได้นำแนวทางการจัดการตามเอกสาร NIST SP800-30 ที่กำหนดแนวทางในการวิเคราะห์ ประเมิน การวัดและประเมินผลมาเป็นแนวทางในการพัฒนาระบบ เพื่อให้สอดคล้องกับระบบความปลอดภัย ได้นำมาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานด้านการจัดการความปลอดภัยสารสนเทศ มาใช้เป็นกรอบในการพัฒนาระบบ โดยในมาตรฐานได้กำหนดเรื่องการจัดการความเสี่ยงสำหรับทรัพย์สินในระบบสารสนเทศ เพื่อสร้างและเลือกวิธีการควบคุมความเสี่ยงและแผนรองรับผลกระทบที่เกิดขึ้น

การวิเคราะห์และออกแบบระบบได้นำแนวทางการการวิเคราะห์และออกแบบเชิงวัตถุโดยใช้ UML ซึ่งเป็นเครื่องมือในการสร้างแบบจำลองเพื่ออธิบายระบบงาน โดยสามารถทำความเข้าใจกับระบบงานได้ง่ายทั้งนักวิเคราะห์และผู้พัฒนาระบบ

บทที่ 2
ความรู้และทฤษฎีที่เกี่ยวข้อง

2.1 การบริหารจัดการความเสี่ยงในระบบสารสนเทศ

ระบบสารสนเทศในองค์กร ควรมีวิธีการวัดและประเมิน มีการบริหารจัดการความเสี่ยงที่เหมาะสม ทั้งทรัพย์ยากรและบุคคลากรในระบบสารสนเทศ จำเป็นต้องมีการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้น เพื่อหาแนวทางหรือวิธีการบรรเทาความเสี่ยงหรือผลกระทบที่มีโอกาสเกิดขึ้น เพื่อให้ธุรกิจและบริการต่างๆสามารถดำเนินงานได้อย่างต่อเนื่อง ซึ่งจำเป็นต้องมีวิธีการหรือขั้นตอนการบริหารจัดการที่มีมาตรฐานและเป็นที่ยอมรับมาใช้งาน ซึ่งแต่ละแนวทางต่างๆมีวัตถุประสงค์ ที่แตกต่างกัน ตามลักษณะของธุรกิจและประเภทของทรัพย์สิน

2.2 แนวทางการบริหารจัดการความเสี่ยงตามแนวทาง ISO/IEC 27001

กระบวนการการบริหารจัดการความเสี่ยงเป็นหนึ่งขั้นตอนในการจัดทำระบบ ISMS (Information Security Management Systems) ตามมาตราฐาน ISO/IEC 27001 ซึ่งถือว่าเป็นขั้นตอนที่มีความสำคัญมาก ความสำเร็จจากการจัดการความเสี่ยงต้องมาจากประเมินที่ถูกต้องและครบถ้วน ในมาตราฐานได้กล่าวถึงวิธีการบริหารจัดการอย่างกว้างๆ โดยไม่ระบุถึงวิธีการหรือแนวทางที่จะนำมาใช้ ซึ่งมีหลายแนวทางด้วยกัน แนวทางการบริหารจัดการความเสี่ยงตามมาฐาน ISC/IEC 27001 ประกอบด้วย 2 ส่วน

2.2.1 การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยงที่อาจก่อให้เกิดผลเสียหายต่อข้อมูลสำคัญ ระบบ และอุปกรณ์ต่างๆ ที่สนับสนุนการทำงานให้กับข้อมูล โดยในขั้นตอนเป็นการประเมินระดับความเสี่ยง (Risk Level) ที่มีทั้งหมดต่อข้อมูลและทรัพย์สินต่างๆ ขององค์กร เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยง

ระดับของความเสี่ยงจะพิจารณาจาก 2 ปัจจัย คือ

- ความน่าจะเป็น (Probability) ในการที่จะเกิดภัยคุกคามใดๆ ขึ้น และก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สิน ขององค์กร ซึ่งโดยปกติจะคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคาม / จุดอ่อน (Threat / Vulnerability Assessment) ที่มีต่อข้อมูลและทรัพย์สินขององค์กร ร่วมกับการพิจารณาถึงวิธีการควบคุม / แก้ไขความเสี่ยง ที่มีอยู่ในปัจจุบัน (Existing Control)

- ความรุนแรง (Severity) ของความเสียหายที่อาจเกิดขึ้น ซึ่งโดยปกติจะคำนวณค่าโดยการพิจารณาจาก ระดับความสำคัญ ของข้อมูลหรือทรัพย์สินนั้นๆ ที่มีต่อองค์กร

2.2.2 การควบคุมและแก้ไขความเสี่ยง (Risk Mitigation)

ทางเลือกในการควบคุมและแก้ไขความเสี่ยงที่ได้แนะนำไว้ในมาตรฐาน ISO/IEC 27001 นั้นมีอยู่ 4 ทาง ดังนี้

- การลดความเสี่ยง (Risk Reduction) คือ การพิจารณาหาวิธีในการควบคุม / แก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับ ที่องค์กรสามารถยอมรับได้ ซึ่งในมาตรฐานได้แนะนำ ไว้ทั้งหมด 133 Controls ใน 11 Domains ให้สามารถเลือกใช้ได้
- การยอมรับความเสี่ยง (Risk Acceptance) คือ การที่องค์กรพิจารณาแล้วพบว่า การดำเนินการแก้ไข / ควบคุมความเสี่ยง นั้น ไม่เหมาะสม, ไม่สามารถกระทำได้ในทางปฏิบัติ หรือ ไม่คุ้มค่า เช่น ค่าใช้จ่ายในการดำเนินการแก้ไข / ควบคุม มีมูลค่า สูงกว่ามูลค่าของข้อมูลและทรัพย์สินที่จะทำการปกป้อง ทั้งนี้ ขึ้นอยู่กับดุลยพินิจของผู้บริหาร
- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยงโดยยกเลิกกระบวนการทำงาน หรือทรัพย์สิน ที่ก่อให้เกิดความเสี่ยงขึ้น ซึ่งมักจะกระทำเมื่อการแก้ไขความเสี่ยงด้วยวิธีการอื่นนั้น ไม่คุ้มกับผลประโยชน์ที่ได้ จากการทำงานด้วยกระบวนการหรือทรัพย์สินนั้นๆ
- การโอนความเสี่ยง (Risk Transfer) คือ การพิจารณาถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย เป็นต้น

2.3 การบริหารจัดการความเสี่ยงในระบบสารสนเทศตามแนวทาง NIST SP800-30

การบริหารจัดการความเสี่ยงตามแนวทางของ NIST Special Publication 800-30 เป็นเอกสารที่นำเสนอแนวทางในการบริหารจัดการความเสี่ยงในระบบสารสนเทศโดย NIST National Institute of Standard and Technology เป็นสถาบันด้านการกำหนดมาตรฐานและเทคโนโลยี ของสหรัฐอเมริกา ซึ่งแนวทางนี้ได้เน้นถึงการระบุภัยคุกคาม จุดอ่อน การกำหนดวิธีการประเมิน และคำแนะนำในการป้องกันความเสี่ยง รวมทั้งการกำหนดแผนการวัดและประเมินผลตามระยะเวลา

ตามคำแนะนำของ NIST sp800-30 ได้กำหนดขั้นตอนในการบริหารจัดการความเสี่ยงไว้ 3 ขั้นตอน

2.3.1 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นกระบวนการแรกในการบริหารจัดการความเสี่ยง ซึ่งองค์กรควรมีการประเมินความเสี่ยงที่มีโอกาสเกิดขึ้น โดยผลลัพธ์ที่ได้จากขั้นตอนนี้ จะสามารถระบุถึงวิธีการควบคุม ลด หรือกำจัดความเสี่ยง เพื่อเป็นการบรรเทาความเสี่ยงดังจะกล่าวในหัวข้อถัดไป

2.3.1.1 ขั้นตอนการประเมินความเสี่ยงมี 9 ขั้นตอน ดังต่อไปนี้

ขั้นตอนที่ 1 การกำหนดคุณลักษณะ (Risk Characterization)
ขั้นตอนที่ 2 การระบุภัยคุกคาม (Threat Identification)
ขั้นตอนที่ 3 การระบุจุดอ่อน (Vulnerability Identification)
ขั้นตอนที่ 4 การวิเคราะห์การควบคุม (Control Analysis)
ขั้นตอนที่ 5 การให้น้ำหนัก (Likelihood Determination)
ขั้นตอนที่ 6 การวิเคราะห์ผลกระทบ (Impact Analysis)
ขั้นตอนที่ 7 การกำหนดความเสี่ยง (Risk Determination)
ขั้นตอนที่ 8 การควบคุม (Control Recommendations)
ขั้นตอนที่ 9 การสร้างเอกสาร (Results Documentation)

ขั้นตอนที่ 1 การกำหนดคุณลักษณะ (Risk Characterization)

เป็นการตอบคำถามว่าระบบของเรามีอะไร มีทรัพย์สินอะไรที่ต้องการวิเคราะห์ความเสี่ยและสิ่งเหล่านั่นมีความเกี่ยวโยงหรือสัมพันธ์กับระบบสารเทศ หรือหน่วยให้บริการอย่างไร

ขั้นตอนที่ 2 การระบุภัยคุกคาม (Threat Identification)

ระบุแหล่งที่มาของภัยคุกคามว่ามีอะไรทั้งภายในภายนอก ที่มีโอกาสสร้างความเสียหายต่อระบบสารสนเทศ

ขั้นตอนที่ 3 ระบุจุดอ่อน (Vulnerability Identification)

ระบุจุดอ่อนและช่องโหว่ที่มีในระบบสารสนเทศเพื่อนำไปสู่ขั้นตอนการประเมิน

ขั้นตอนที่ 4 การวิเคราะห์การควบคุม (Control Analysis)

มีแผนที่ใช้ในการควบคุมและป้องกันในปัจจุบันมีอะไรบ้าง

ขั้นตอนที่ 5 การให้น้ำหนัก (Likelihood Determination)

น้ำหนักผลกระทบแบ่งตามแหล่ง โอกาสและความเป็นไปได้ของภัยคุกคามดังตาราง

ตารางที่ 2.1 การให้น้ำหนักผลกระทบ และโอกาสที่เกิดขึ้น

High	แหล่งภัยคุกคาม มีโอกาสเกิดขึ้นได้สูง ควรมีวิธีควบคุมป้องกันไม่ให้เกิดขึ้น
Medium	แหล่งภัยคุกคาม มีโอกาสเกิดขึ้น ควรมีวิธีควบคุมป้องกันเพื่อไม่ให้เกิด
Low	แหล่งภัยคุกคาม มีโอกาสเกิดขึ้นได้น้อย หรือแทบไม่มี

ขั้นตอนที่ 6 การวิเคราะห์ผลกระทบ (Impact Analysis)

โดยผลกระทบมีการแบ่งระดับความรุนแรงที่สร้างความเสียหายให้แก่ทรัพย์สินดังตาราง

ตารางที่ 2.2 ผลกระทบที่เกิดจากจุดอ่อนหรือช่องโหว่

High	1. สูญเสียทรัพย์สินหรือทรัพยากรที่คิดมูลค่าเป็นตัวเงินสูง หรือ 2. สร้างความเสียหาย ละเมิดหรือขัดขวาง ภารกิจ และชื่อเสียงขององค์กร หรือ 3. ทำให้บุคคลถึงแก่ชีวิตและเป็นอันตราย
Medium	1. สูญเสียทรัพย์สินหรือทรัพยากรที่คิดมูลค่าเป็นตัวเงิน หรือ 2. สร้างความเสียหาย ละเมิดหรือขัดขวาง ภารกิจ และชื่อเสียงขององค์กร หรือ 3. ทำให้บุคคลเป็นอันตราย
Low	1. สูญเสียทรัพย์สินหรือทรัพยากรบางอย่างที่คิดมูลค่าเป็นตัวเงิน หรือ 2. สังเกตได้ว่ามีความเสียหาย ละเมิดหรือขัดขวาง ภารกิจ และชื่อเสียงของ

ขั้นตอนที่ 7 การกำหนดความเสี่ยง (Risk Determination)

เป็นการกำหนดระดับความเสี่ยงในระบบสารสนเทศ แสดงให้เห็นภัยคุกคาม และจุดอ่อน โดยแสดงออกเป็นระดับของผลกระทบคือ สูง ปานกลาง และต่ำ

ตารางที่ 2.3 การให้น้ำหนักภัยคุกคามและระดับผลกระทบ

Threat Likelihood	Impact		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10
Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)			

ตารางที่ 2.4 รายละเอียดความเสี่ยงแต่ละระดับ

ระดับความเสี่ยง	รายละเอียดความเสี่ยง และแผนที่จำเป็น
High	ถ้ามีการสังเกตหรือคำวินิจฉัยที่ได้จากการประเมินว่ามีความเสี่ยงสูง มีความจำเป็นที่ต้องได้รับการวัดที่เหมาะสม ระบบที่มีอยู่อาจต้องทำงานได้อย่างต่อเนื่อง แผนการปฏิบัติงานที่ต้องเหมาะสมต้องถูกนำมาใช้โดยเร็วที่สุด
Medium	ถ้ามีการสังเกตได้ว่ามีความเสี่ยงอยู่ในระดับปานกลาง การทำงานที่เหมาะสมมีความจำเป็นต้องนำเอาแผนที่มีมาพัฒนาเพื่อให้สามารถใช้งานกับแผนการปฏิบัติงานภายในระยะเวลาที่กำหนด
Low	ถ้ามีการสังเกตได้ว่ามีความเสี่ยงอยู่ในระดับต่ำ อำนาจการอนุมัติที่วางไว้ต้องถูกนำมาใช้เพื่อการตัดสินใจยอมรับความเสี่ยง

ขั้นตอนที่ 8 การควบคุม (Control Recommendations)

เป้าหมายคือ ใช้การวิธีการควบคุมที่จำเป็นโดยมีค่าใช้จ่ายที่เหมาะสม เพื่อให้สามารถบรรลุเป้าหมายที่วางไว้ได้ โดยมีข้อที่ต้องพิจารณาดังต่อไปนี้

- มีวิธีการควบคุมที่มีประสิทธิภาพ
- มีกฎ ระเบียบ ข้อบังคับ และนโยบายขององค์กร
- มีการแผนการป้องกันผลกระทบ
- มีความปลอดภัย และความน่าเชื่อถือ

ขั้นตอนที่ 9 การสร้างเอกสาร (Results Documentation)

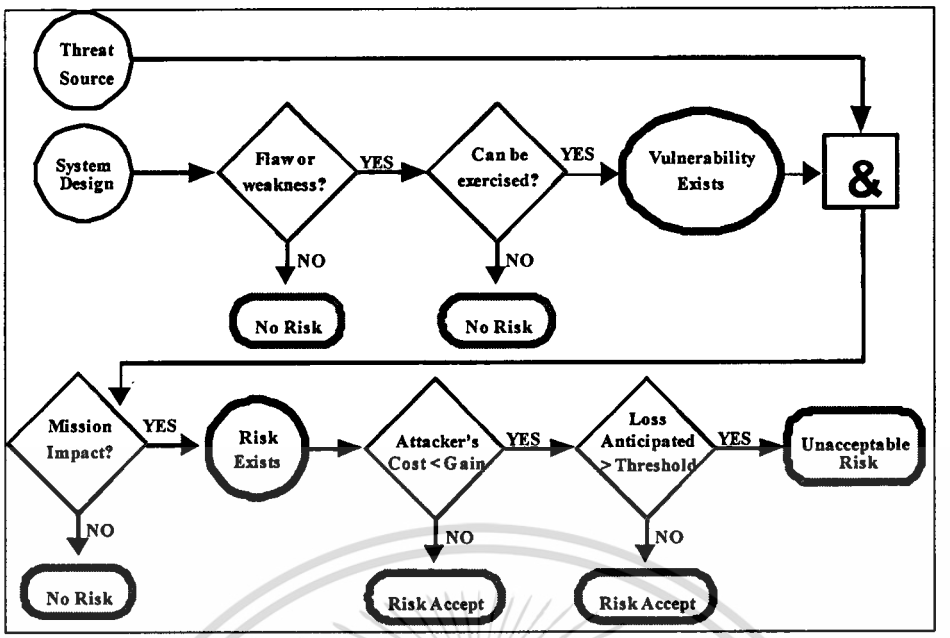
ขั้นตอนการประเมินความเสี่ยงเสร็จเรียบร้อย ได้ผลลัพธ์ออกมาในรูปแบบเอกสารรายงาน ซึ่งเป็นรายงานการบริหารจัดการความเสี่ยงเป็นบทสรุปสำหรับผู้บริหาร เพื่อนำไปเพื่อช่วยในการกำหนดวิสัยทัศน์ นโยบาย กระบวนการขั้นตอน กำหนดงบประมาณ ปรับปรุงเปลี่ยนแปลงการบริหารจัดการและระบบการปฏิบัติงานขององค์กร

2.3.2 การบรรเทาความเสี่ยง (Risk Mitigation)

การบรรเทาความเสี่ยงเป็นกระบวนการลำดับที่สองของการบริหารจัดการความเสี่ยง ซึ่งได้รวมการให้ลำดับความสำคัญ การวัด และการนำไปใช้เป็นข้อแนะนำการควบคุม เพื่อลดระดับความเสี่ยงจากกระบวนการประเมินความเสี่ยง .

2.3.2.1 ทางเลือกในการบรรเทาความเสี่ยง

- Risk Assumption สมติฐานทางด้านความเสี่ยง เพื่อยอมรับความเสี่ยงนั้นและดำเนินระบบต่อไป หรือมีการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- Risk Avoidance เพื่อหลีกเลี่ยงความเสี่ยงโดยการกำจัดต้นเหตุของความเสี่ยง หรือผลที่เกิดภายหลัง
- Risk Limitation เพื่อจำกัดความเสี่ยงโดยการนำการควบคุมไปใช้เพื่อลดผลกระทบที่เกิดจากภัยคุกคามให้เหลือน้อยที่สุด
- Risk Planning เพื่อจัดการความเสี่ยงโดยพัฒนาแผนการบรรเทาความเสี่ยงตามลำดับความสำคัญ การนำไปใช้ และดูแลรักษาแผนการควบคุม
- Research and Acknowledgment เพื่อลดความเสี่ยงและความสูญเสียโดยการหาความรู้เรื่องจุดอ่อน หรือช่องโหว่ และศึกษาวิจัยเพื่อหาวิธีการควบคุมที่ถูกต้องเหมาะสม
- Risk Transference เพื่อโอนความเสี่ยงโดยใช้ทางเลือกอื่นเพื่อทดแทนความเสียหาย เช่น การซื้อประกันภัยต่างๆ



รูปที่ 2.1 กลยุทธการบรรเทาความเสี่ยง

กลยุทธ์ที่กระทำต่อเนื่องตามกฎที่ได้รับยอมรับ โดยได้ให้แนวทางในการปฏิบัติเพื่อบรรเทาความเสี่ยงจากภัยคุกคามหรือความจงใจของมนุษย์ โดยเมื่อมีจุดอ่อนหรือช่องโหว่ในระบบ จะต้องมีแผนในการควบคุมความเสี่ยง โดยคำนึงค่าใช้จ่ายและความเสียหายที่เกิดขึ้น

2.3.2.2 แนวทางสำหรับการใช้การควบคุม

ขั้นตอนที่ 1 การกำหนดลำดับความสำคัญ

บนพื้นฐานของระดับความเสี่ยงที่กำหนดไว้ในรายงานการประเมินความเสี่ยงในขั้นตอนแรก แผนการนำไปใช้ได้กำหนดระดับความสำคัญไว้แล้ว ในการจัดสรรทรัพยากรส่วนที่มีลำดับความสำคัญสูงสุดจะถูกกำหนดให้ไม่อยู่ในระดับที่ยอมรับได้และกำหนดไว้ให้เป็นระดับความเสี่ยงสูง และจุดอ่อนหรือภัยคุกคามที่เป็นคู่กันนั้นจะต้องได้รับแผนการปฏิบัติเพื่อป้องกันการเกิดขึ้น ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือ ระดับการปฏิบัติจาก สูงไปต่ำ

ขั้นตอนที่ 2 ประเมินตัวเลือกคำแนะนำการควบคุม

คำแนะนำการควบคุมในขั้นตอนการประเมินความเสี่ยงอาจไม่เหมาะสมหรือความเป็นไปได้ในระบบสารสนเทศ ในขั้นตอนนี้คือความเป็นไปได้ ความมีประสิทธิภาพ ของตัวเลือกคำแนะนำการควบคุมจะถูกวิเคราะห์ วัตถุประสงค์คือเลือกทางเลือกที่เหมาะสมเพื่อลดระดับความเสี่ยงให้เหลือน้อยที่สุด ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือ รายการการควบคุมที่เป็นไปได้

ขั้นตอนที่ 3 ทำ Cost-Benefit Analysis

เพื่อวิเคราะห์ค่าใช้จ่ายและผลลัพธ์ที่ได้เพื่อนำเสนอการตัดสินใจในระดับจัดการ เพื่อแสดงค่าใช้จ่ายในการควบคุมความเสี่ยง ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือ รายละเอียดค่าใช้จ่ายสำหรับการนำแผนการควบคุมไปใช้

ขั้นตอนที่ 4 เลือกการควบคุม

จากผลลัพธ์การวิเคราะห์ CBA ผู้บริหารตัดสินใจเลือกทางเลือกที่มีค่าใช้จ่ายเหมาะสมและได้ผลลัพธ์ได้คุ้มค่ามากที่สุด สำหรับลดความเสียง การควบคุมที่ถูกเลือกจะเชื่อมเข้าทางด้านเทคนิค การปฏิบัติ และการควบคุมการจัดการเพื่อให้ใจว่ามีความปลอดภัยเพียงพอ ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือ ทางเลือกการควบคุม

ขั้นตอนที่ 5 มอบหมายความรับผิดชอบ

บุคคลที่เหมาะสมทั้งบุคลากรภายใน หรือภายนอก ที่มีความชำนาญและทักษะที่เหมาะสมที่สามารถทำงานและรับผิดงานที่ได้รับมอบหมายได้ ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือ รายชื่อบุคคลที่ได้รับมอบหมาย

ขั้นตอนที่ 6 พัฒนาแผนการอิมพลีเมนท์เครื่องป้องกัน

ในขั้นตอนนี้ แผนการใช้เครื่องป้องกันได้พัฒนาขึ้นมาแล้ว โดยอย่างน้อยต้องประกอบไปด้วยข้อมูลดังนี้

- ความเสี่ยงและระดับความเสี่ยง
- คำแนะนำการควบคุมซึ่งมาจากรายงานการประเมินความเสี่ยง
- ลำดับการปฏิบัติ
- ทางเลือกแผนการควบคุม
- ทรัพย์ยากรหรืออุปกรณ์การอิมพลีเมนท์ ที่มาจากทางเลือกแผนการควบคุม
- รายชื่อทีมที่ได้รับมอบหมายและสมาชิก
- วันเริ่มต้นการอิมพลีเมนท์
- เป้าหมายวันสำเร็จของการอิมพลีเมนท์
- ความต้องการการบำรุงรักษา

ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือ แผนการป้องกันเพื่อนำไปปฏิบัติ

ขั้นตอนที่ 7 การอิมพลีเมนท์ทางเลือกการควบคุม

การอิมพลีเมนท์ทางเลือกการควบคุมขึ้นอยู่กับความเหมาะสม การนำไปใช้และปฏิบัติเพื่อลดระดับความเสี่ยง แต่ไม่ได้กำจัดความเสี่ยงให้หายไป ผลลัพธ์ที่ออกมาจากขั้นตอนนี้คือการยอมรับระดับความเสี่ยงที่เหลืออยู่

2.3.3 การวัดและประเมินผล (Evaluation and Assessment)

เวลาผ่านไปเทคโนโลยีและวิธีการต่างๆมีการเปลี่ยนแปลง แผนการและวิธีการป้องกันความเสี่ยงในองค์กร ควรได้รับการวัดและประเมินตามระยะเวลาที่เหมาะสมเพื่อตรวจสอบมีภัยคุกคามและจุดอ่อนในระบบที่อาจเกิดขึ้นได้และมีวิธีการควบคุมที่ถูกต้องเหมาะสม ควรวิเคราะห์และประเมินแผนการควบคุมเพื่อให้ประสบความสำเร็จในการบริหารจัดการความเสี่ยง

บทที่ 3
การวิเคราะห์ระบบปัจจุบัน

3.1 การทำงานของระบบปัจจุบัน

การทำงานในการบริหารจัดการความเสี่ยงของบริษัทในปัจจุบัน มีการเก็บข้อมูลต่างๆไว้ในโปรแกรมสเปรสซีท ซึ่งไม่สะดวกในการจัดเก็บข้อมูลในปริมาณมาก อีกทั้งไม่มีระบบป้องกันการเข้าถึงที่ดีพอ ซึ่งเอกสารการประเมินความเสี่ยงปรากฏในรูปที่ 3.1

RISK ASSESSMENT WORKSHEET / REPORT

Version
Date
Completed by

Asset Information
Asset P590 I
Type Physical
Owner Email Service

Location Data Center
Ref. Baseline Mail v13
Ref. Inven Remedy

Criticality (value from Baseline)

C	I	A	L
VH 3	H 2	H 2	N/A 0

Total Extreme Risks	0
Total High Risks	6
Total Medium Risks	2
Total Low Risks	3

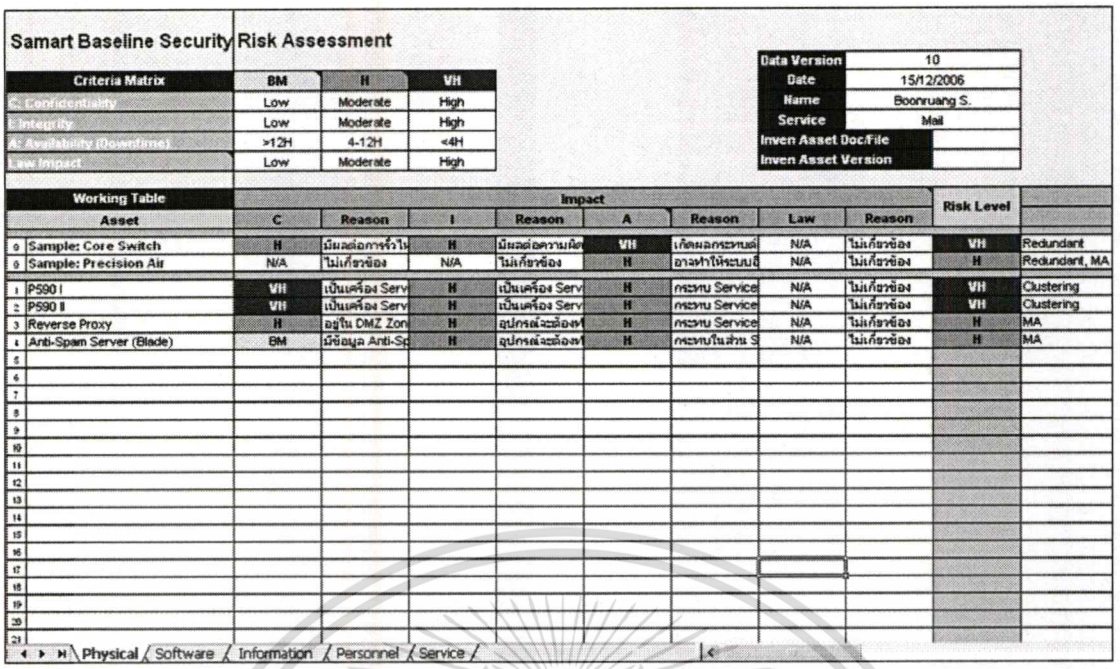
Risk Assessment

Threat Assessment | *Vulnerability Assessment* | *Risk*

ID #	Threat (what can happen?)	Possibility (Y / N)	Impact (based on threat capability) C	I	A	L	Vulnerability (how can it happen?)	Existing Safeguard(s) (what protection do you have?)	Probability	Risk Level
1	Masquerading of User Identity	Y	Moderate 3	Moderate 3	Moderate 3		Too many users	Fingerscan access control	Unlikely 2	C High 18
							Management does not review and monitor their employees			
							Lack of or inappropriate third party services reviewing and monitoring			
							Lack of access control policy	System Access Control Policy (SAP) is being implemented		
							Lack of system access control	Technical restriction is implemented in accordance with SAP		
							Lack of or inappropriate network segegration	Network is segregrated using VLAN		
							Lack of system security monitoring	System is monitored by Data Center personnel		
							Lack of identification of sender and receiver	N/A		
							System is available to public	Only for Samart's personnel with Acceptable Use Policy		
2	Misuse of System Resource	Y			Moderate 3		No acceptable use policy	Acceptable Use Policy is being implemented	Moderate 3	
							Lack of or inappropriate segegration of duties			
							Lack of disciplinary process	Disciplinary process exists in accordance with Compliance Policy		

รูปที่ 3.1 Risk Assessment worksheet

ผลลัพธ์จากการประเมินความเสี่ยงจะถูกเก็บไว้ในโปรแกรมสเปรสซีทเช่นเดียวกันในรูปที่ 3.2 ซึ่งผลลัพธ์เหล่านี้ถือว่าเป็นเอกสารที่มีความสำคัญควรมีการป้องกันการแก้ไข มีการควบคุมการปรับปรุงและเปลี่ยนแปลง ประวัติการปรับปรุงแก้ไขต่างๆควรได้รับการบันทึกและจัดเก็บให้ปลอดภัย มีการป้องกันการเข้าถึงตามสิทธิการใช้งานอย่างเป็นระบบ



Samart Baseline Security Risk Assessment

Criteria Matrix	BM	H	VH
C: Confidentiality	Low	Moderate	High
I: Integrity	Low	Moderate	High
A: Availability (Downtime)	>12H	4-12H	<4H
Law Impact	Low	Moderate	High

Data Version	10
Date	15/12/2006
Name	Boonruang S.
Service	Mail
Inven Asset Doc/File	
Inven Asset Version	

Working Table		Impact								Risk Level	
	Asset	C	Reason	I	Reason	A	Reason	Law	Reason		
0	Sample: Core Switch	H	มีผลต่อการทำงา	H	มีผลต่อความถู	VH	เกิดผลกระทบต่	N/A	ไม่เกี่ยวข้อง	VH	Redundant
0	Sample: Precision Air	N/A	ไม่เกี่ยวข้อง	N/A	ไม่เกี่ยวข้อง	H	อาจทำให้ระบบอื่	N/A	ไม่เกี่ยวข้อง	H	Redundant, MA
1	P590 I	VH	เป็นเครื่อง Serv	H	เป็นเครื่อง Serv	H	กระทบ Service	N/A	ไม่เกี่ยวข้อง	VH	Clustering
2	P590 II	VH	เป็นเครื่อง Serv	H	เป็นเครื่อง Serv	H	กระทบ Service	N/A	ไม่เกี่ยวข้อง	VH	Clustering
3	Reverse Proxy	H	อยู่ใน DMZ Zon	H	อุปกรณ์จะต้องท	H	กระทบ Service	N/A	ไม่เกี่ยวข้อง	H	MA
4	Anti-Spam Server (Blade)	BM	มีข้อมูล Anti-Sp	H	อุปกรณ์จะต้องท	H	กระทบในส่วน S	N/A	ไม่เกี่ยวข้อง	H	MA
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											

Physical / Software / Information / Personnel / Service /

รูปที่ 3.2 Risk Treatment worksheet

3.2 ปัญหาที่พบในระบบงานปัจจุบัน

เนื่องจากข้อมูลถูกจัดเก็บในโปรแกรมสเปรสซีท ทำให้เกิดปัญหาด้านความปลอดภัยโดยตรง เพราะเป็นเอกสารในการทำงานเกี่ยวกับทรัพย์สินของบริษัทเพื่อใช้ในการประเมินความเสี่ยงของระบบสารสนเทศ ซึ่งควรได้รับปกป้อง ด้านความลับ ความถูกต้อง และความพร้อมในการใช้งาน

โดยสิ่งที่ควรได้รับการปรับปรุงจากการทำงานเดิมในปัจจุบันมีดังนี้

1. ต้องการรวบรวมข้อมูลทรัพย์สินในระบบสารสนเทศภายขอบเขตที่ได้กำหนดไว้เพื่อเป็นเป้าหมายในการสร้างระบบความปลอดภัย
2. มีข้อมูลสำหรับการวิเคราะห์ความเสี่ยงภายในระบบสารสนเทศอย่างครบถ้วน
3. ลดขั้นตอนและความซ้ำซ้อนในการปฏิบัติงานในการวิเคราะห์และประเมินความเสี่ยงในระบบสารสนเทศ
4. ผลลัพธ์จากการบริหารจัดการความเสี่ยงสามารถนำมาวิเคราะห์ให้เห็นถึงแนวโน้มด้านต่างๆได้อย่างมีประสิทธิภาพ
5. ผลการวิเคราะห์ต้องการให้อยู่ในรูปภาพหรือแผนภาพแบบต่างๆเพื่อให้ผู้บริหารสามารถเห็นและเข้าใจถึงความเสี่ยงที่เกิดขึ้นภายในระบบสารสนเทศได้ง่ายขึ้น

บทที่ 4

การออกแบบระบบ

4.1 ลักษณะและขอบเขตของระบบ

4.1.1 กิจกรรมโดยรวมของระบบ

กิจกรรมหลักของระบบมีอยู่ 3 กิจกรรม กิจกรรมที่ 1 เป็นกิจกรรมการประเมินความเสี่ยงในระบบสารสนเทศ เป็นการวิเคราะห์และประเมินความเสี่ยงซึ่งอยู่ในขอบเขตตามที่ได้ระบุไว้ในกรอบการบริหารจัดการความปลอดภัยของระบบสารเทศ กิจกรรมที่ 2 เป็นกิจกรรมการบรรเทาความเสี่ยง โดยเมื่อทำการวิเคราะห์และประเมินความเสี่ยง ตามลำดับความสำคัญและระดับผลกระทบที่เกิดขึ้นแล้วต้องแสดงแนวทางการบรรเทาและป้องกันความเสี่ยงที่มีอยู่ และกำหนดทางเลือกในการบรรเทาความเสี่ยงให้เหลืออยู่ในระดับที่ยอมรับได้ กิจกรรมที่ 3 เป็นกิจกรรมสุดท้ายเป็นกิจกรรมการวัดและประเมินผลหลังจากการวิเคราะห์ ประเมินความเสี่ยง พร้อมทั้งกำหนดแผนบรรเทาความเสี่ยง เพื่อทบทวนกิจกรรมตามระยะเวลาเพื่อให้ระบบสารสนเทศมีความปลอดภัย เพื่อมั่นใจได้ว่ามีแผนการป้องกันและบรรเทาความเสี่ยงเพื่อให้ภารกิจขององค์กรสามารถดำเนินต่อไปได้

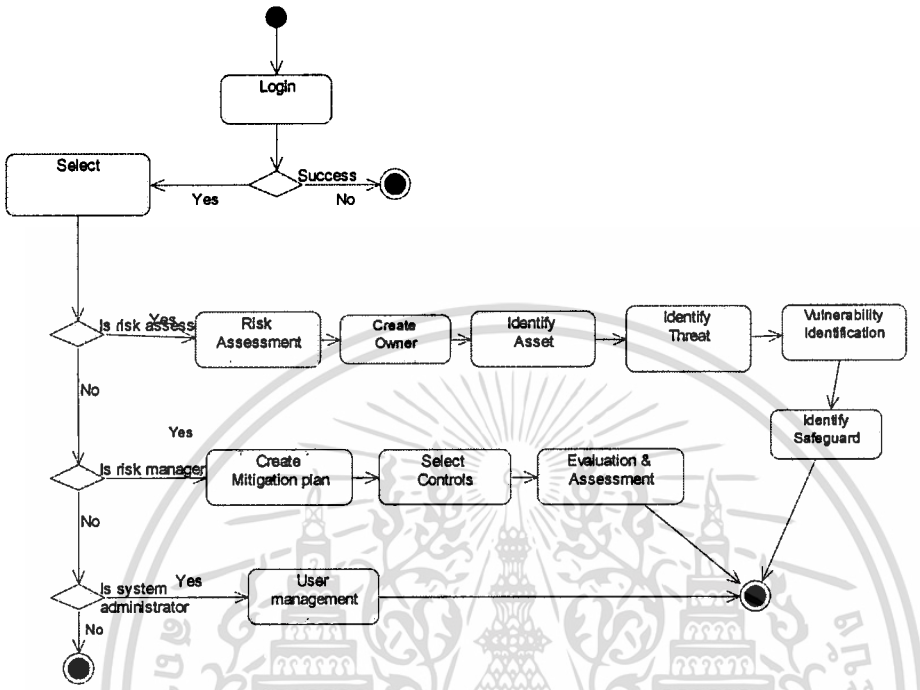
การประเมินความเสี่ยง เมื่อเข้าสู่ระบบผู้ใช้ที่มีสิทธิ์สามารถสร้าง และแก้ไขข้อมูลเกี่ยวกับการประเมินได้ โดยในกิจกรรมการประเมินความเสี่ยงมีขั้นตอนดังนี้

1. นักวิเคราะห์ความเสี่ยงเลือกแสดงโครงการและเข้าสู่ขั้นตอนการประเมินความเสี่ยง สร้างขอบเขต และให้รายละเอียดเกี่ยวกับกรอบการทำงาน
2. นักวิเคราะห์ เติมข้อมูลทรัพย์สิน ประเภท ชนิด สถานที่ตั้ง และผู้รับผิดชอบ
3. นักวิเคราะห์ แสดงภัยคุกคาม โอกาสความเป็นไปได้ และให้น้ำหนักผลกระทบที่ส่งผลด้านความปลอดภัย 4 ด้านคือ ความลับ ความถูกต้อง ความมีอยู่ และ ผลกระทบด้านกฎหมาย แสดงถึงจุดอ่อนที่มีในทรัพย์สิน และแสดงถึงแนวทางการป้องกันที่มีอยู่

การบรรเทาความเสี่ยง เมื่อเสร็จสินขั้นตอนการประเมินความเสี่ยงจะเข้าสู่ขึ้นตอนการสร้างแผนการบรรเทาความเสี่ยง

1. ผู้รับผิดชอบทรัพย์สินที่ภายใต้ขอบเขตการให้บริการที่ตนเองรับผิดชอบเข้ามาทบทวนผลการประเมินความเสี่ยง โดยผลกระทบที่เกิดจากความเสี่ยงอยู่ในระดับที่ไม่สามารถยอมรับได้จะต้องสร้างแผนการบรรเทาความเสี่ยงให้กับทรัพย์สิน
2. เลือกแผนเพื่อบรรเทาความเสี่ยง พร้อมทั้งระบุทรัพยากรที่ใช้ในแผนบรรเทาความเสี่ยง ลำดับความสำคัญ กำหนดทีมหรือบุคคลที่รับผิดชอบ พร้อมทั้งกำหนดระยะเวลา วันเริ่มต้นและวันสิ้นสุด

3. กำหนดกลุ่มความเสี่ยงและแผนการบรรเทาความเสี่ยง โดยกำหนดหัวข้อของแผนการป้องกันความเสี่ยงเพื่อให้สอดคล้องกับข้อกำหนดมาตรฐานความปลอดภัยของระบบสารสนเทศ



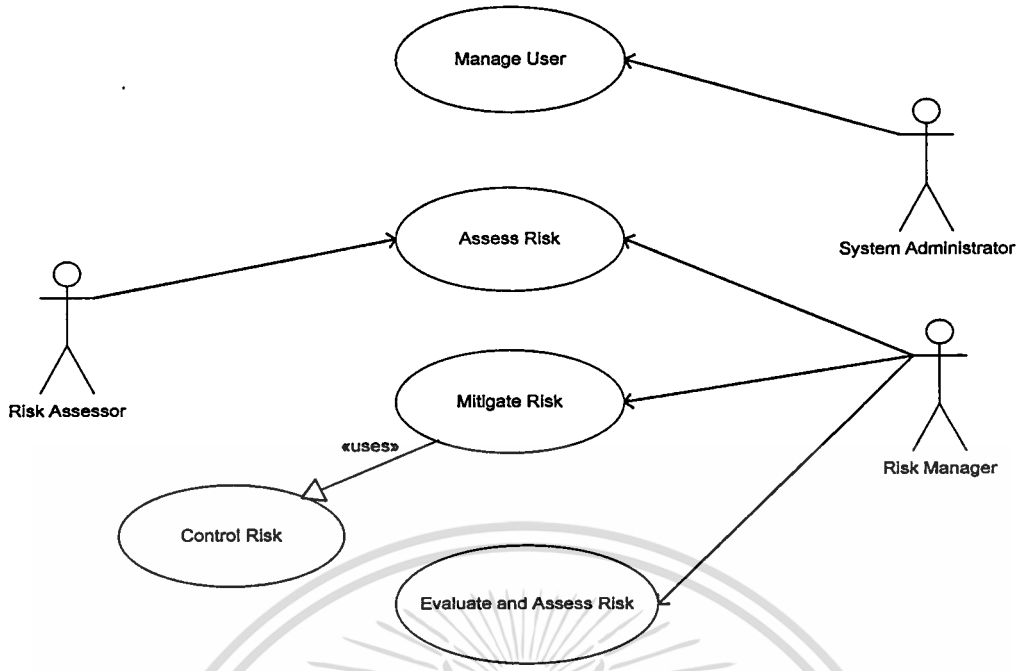
รูปที่ 4.1 Activity Diagram ระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

การวัดและประเมินผล

1. ผู้ตรวจสอบแสดงตนเพื่อเข้าเมนูการวัดและประเมินผล
2. ผู้ตรวจสอบสามารถเลือกเมนูแสดงผลการวิเคราะห์ความเสี่ยงในมุมมองต่างๆ
3. ผู้ตรวจสอบสามารถแสดงแผนบรรเทาความเสี่ยง วิธีการบรรเทาความเสี่ยง ที่สอดคล้องกับมาตรฐานความปลอดภัยในระบบสารสนเทศ

4.1.2 ภาพรวมของฟังก์ชันการทำงานในระบบ

ฟังก์ชันการทำงานของระบบนำเสนออยู่ในแผนภาพ Use-case Diagram โดยแสดงให้เห็นถึงความสัมพันธ์ของฟังก์ชันการทำงานและผู้กระทำกับระบบแสดงให้เห็นในรูปที่ 4.2



รูปที่ 4.2 Use-case Diagram ระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

ระบบการบริหารจัดการความเสี่ยงในระบบสารสนเทศประกอบไปด้วย Actor ดังต่อไปนี้

1. ผู้บริหารระบบ System administrator เป็นผู้จัดการเกี่ยวกับบัญชีผู้ใช้และสิทธิ์การเข้าใช้งานระบบ
2. ผู้ประเมินความเสี่ยง Risk assessor เป็นผู้ระบุทรัพย์สินภายในระบบ ระบุภัยคุกคามจากภายนอก ระบุจุดอ่อนของระบบ และให้คะแนนน้ำหนักกับส่วนประกอบต่างๆ ทั้งทรัพย์สิน และภัยคุกคามเพื่อการประเมินความเสี่ยง และนำส่งให้ผู้จัดการความเสี่ยงทำการทบทวน
3. ผู้จัดการความเสี่ยง Risk manager เป็นผู้ที่ดูรายการงานผลการประเมินความเสี่ยง สร้างแผนบรรเทาความเสี่ยง แผนควบคุมความเสี่ยงให้สอดคล้องกับมาตราฐานความปลอดภัย สร้างนโยบายควบคุมความเสี่ยงของระบบสารสนเทศ ตามระดับคะแนนผลกระทบที่มีค่าสูงสุด และสร้างแผนการประเมินความเสี่ยงตามรอบเวลา

ระบบการบริหารจัดการความเสี่ยงในระบบสารสนเทศประกอบไปด้วยฟังก์ชันการทำงานดังต่อไปนี้

1. การจัดการเกี่ยวกับผู้ใช้ Manage user เป็นฟังก์ชันการทำงานการจัดการเกี่ยวผู้ใช้งานระบบ
3. การประเมินความเสี่ยง Assess Risk เป็นฟังก์ชันการทำงานการประเมินความเสี่ยง
4. การบรรเทาความเสี่ยง Mitigate Risk เป็นฟังก์ชันการทำงานการสร้างแผนบรรเทาความเสี่ยง
5. การควบคุมความเสี่ยง Control Risk เป็นฟังก์ชันการทำงานเพื่อสร้างแผนให้สอดคล้องกับมาตราฐานความปลอดภัย และมีนโยบายควบคุม

6. การวัดและประเมินผล Evaluation and assessment เป็นฟังก์ชันการทำงานการนำเสนอระดับความเสี่ยงและแผนการบรรเทาความเสี่ยง

4.2 การวิเคราะห์และออกแบบระบบ

ขั้นตอนการวิเคราะห์และออกแบบระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ ใน Use-case diagram ได้นำเสนอฟังก์ชันการทำงานและแสดงความสัมพันธ์กับผู้ใช้ระบบ โดยนำมาแสดงรายละเอียดในกิจกรรมการทำงาน และลำดับการทำงานในแต่ละฟังก์ชัน โดยใน Activity diagram จะอธิบายขั้นตอนการทำงานและกิจกรรมต่างๆที่เกิดขึ้นภาย use-case ส่วน Sequence diagram จะอธิบายขั้นตอนการทำงานและการติดต่อสื่อสารกันภายในแต่ละ use-case

- **Use-case diagram ของระบบบริหารจัดการความเสี่ยงภายในระบบสารสนเทศ**

Use-case diagram ของระบบบริหารจัดการความเสี่ยงภายในระบบสารสนเทศมีดังต่อไปนี้

1. Use-case diagram: Manage User แสดงดังรูปที่ 4.3
2. Use-case diagram: Assess Risk แสดงดังรูปที่ 4.6
3. Use-case diagram: Mitigate Risk แสดงดังรูปที่ 4.9
4. Use-case diagram: Control Risk แสดงดังรูปที่ 4.12
5. Use-case diagram: Evaluation and assessment แสดงดังรูปที่ 4.15

- **Activity diagram ของระบบบริหารจัดการความเสี่ยงภายในระบบสารสนเทศ**

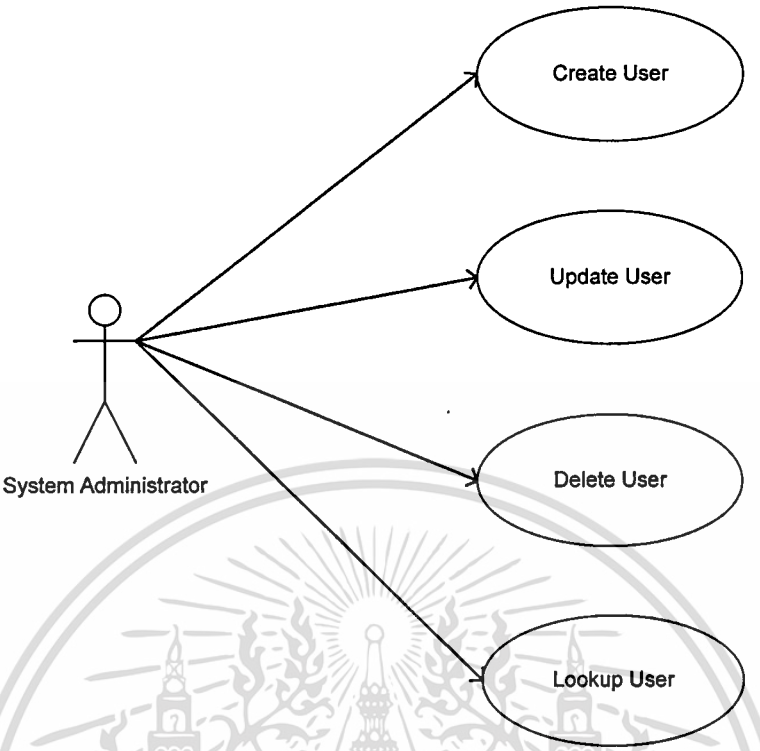
Activity diagram ของระบบบริหารจัดการความเสี่ยงภายในระบบสารสนเทศมีดังต่อไปนี้

1. Activity diagram: Manage User แสดงดังรูปที่ 4.4
2. Activity diagram: Assess Risk แสดงดังรูปที่ 4.7
3. Activity diagram: Mitigate Risk แสดงดังรูปที่ 4.10
4. Activity diagram: Control Risk แสดงดังรูปที่ 4.13
5. Activity diagram: Evaluation and assessment แสดงดังรูปที่ 4.16

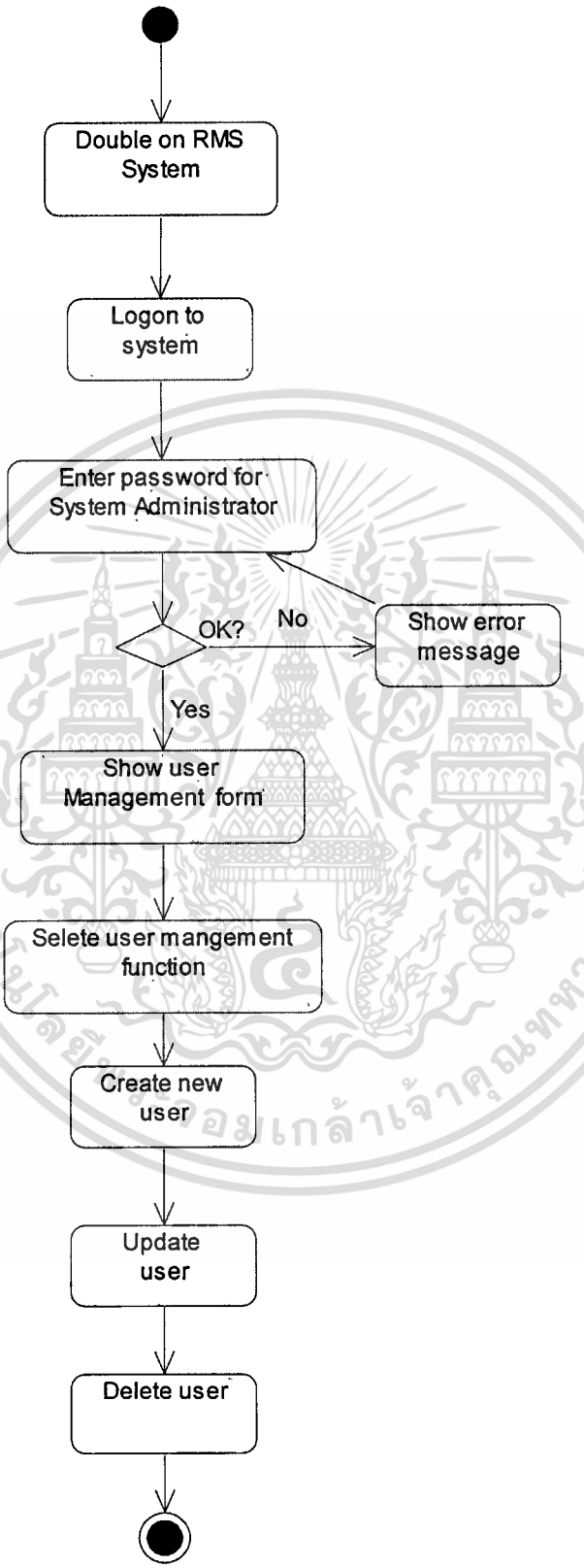
- **Sequence diagram ของระบบบริหารจัดการความเสี่ยงภายในระบบสารสนเทศ**

Sequence diagram ของระบบบริหารจัดการความเสี่ยงภายในระบบสารสนเทศมีดังต่อไปนี้

1. Sequence diagram: Manage User แสดงดังรูปที่ 4.5
2. Sequence diagram: Assess Risk แสดงดังรูปที่ 4.8
3. Sequence diagram: Mitigate Risk แสดงดังรูปที่ 4.11
4. Sequence diagram: Control Risk แสดงดังรูปที่ 4.14
5. Sequence diagram: Evaluation and assessment แสดงดังรูปที่ 4.17



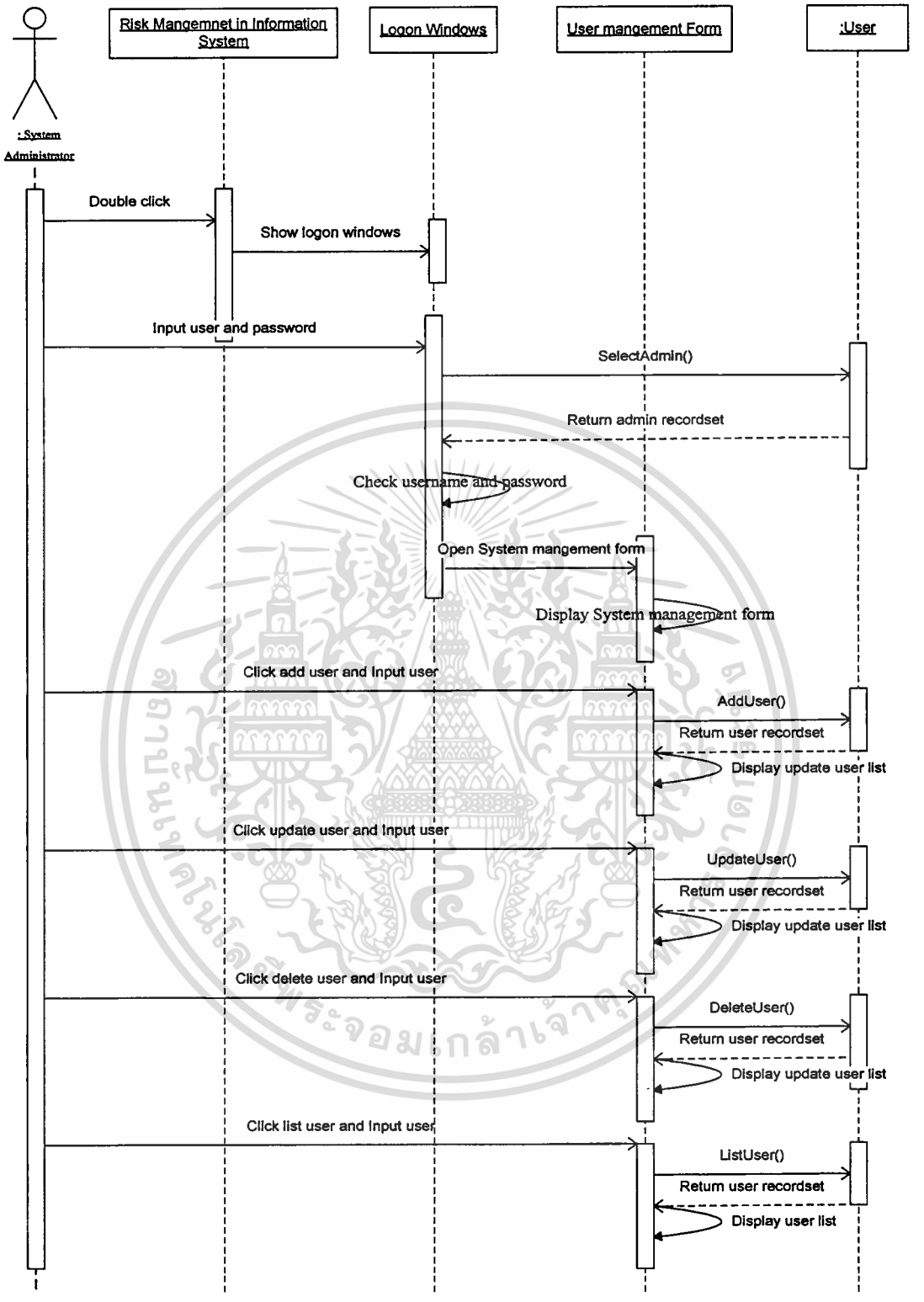
รูปที่ 4.3 Use-case Diagram: Manage User



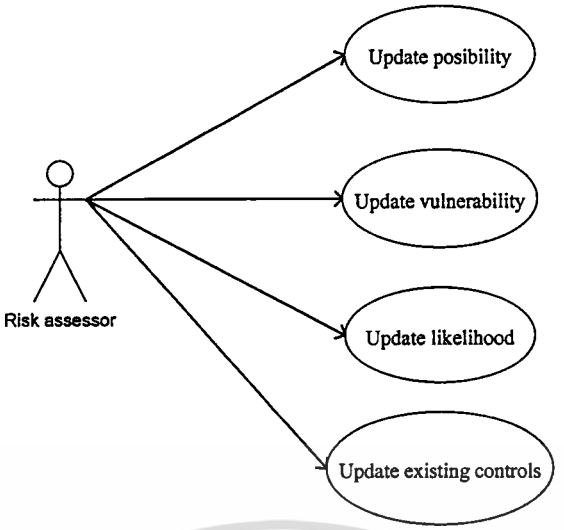
รูปที่ 4.4 Activity Diagram: Manage User

ขั้นตอนการทำงานของ Use-case: Manage User สามารถอธิบายการทำงานด้วย Activity Diagram ดังรูปที่ 4.4 โดยมีขั้นตอนดังต่อไปนี้

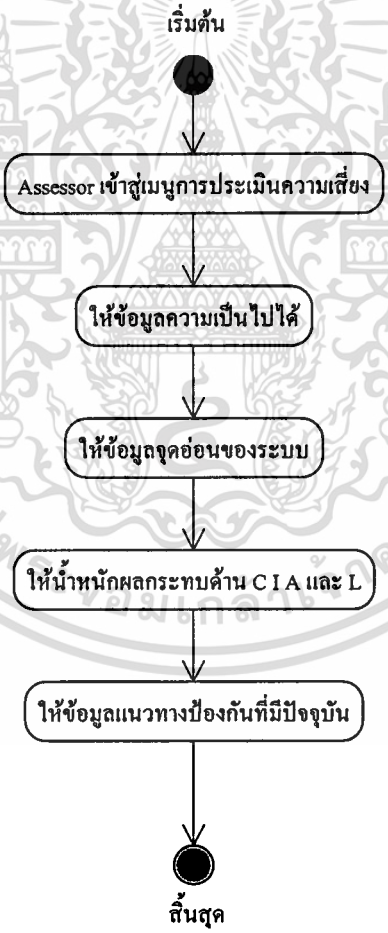
1. ผู้บริหารระบบดับเบิลคลิกที่โปรแกรม “ระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ”
2. ระบบแสดงหน้าจอล๊อกออนเข้าสู่ระบบ
3. ผู้บริหารระบบกรอกชื่อ Administrator และรหัสผ่าน และกดปุ่ม “เข้าสู่ระบบ”
4. ระบบตรวจสอบชื่อและรหัสผ่าน หากข้อมูลไม่ถูกต้องจะกลับมาที่หน้าจอล๊อกออน
5. หากระบบตรวจสอบชื่อและรหัสผ่านถูกต้อง ก็จะเข้าสู่หน้าจอจัดการระบบ
6. ระบบแสดงหน้าจอสำหรับบริหารจัดการเกี่ยวกับผู้ใช้ในระบบ



รูปที่ 4.5 Sequence Diagram: Manage User



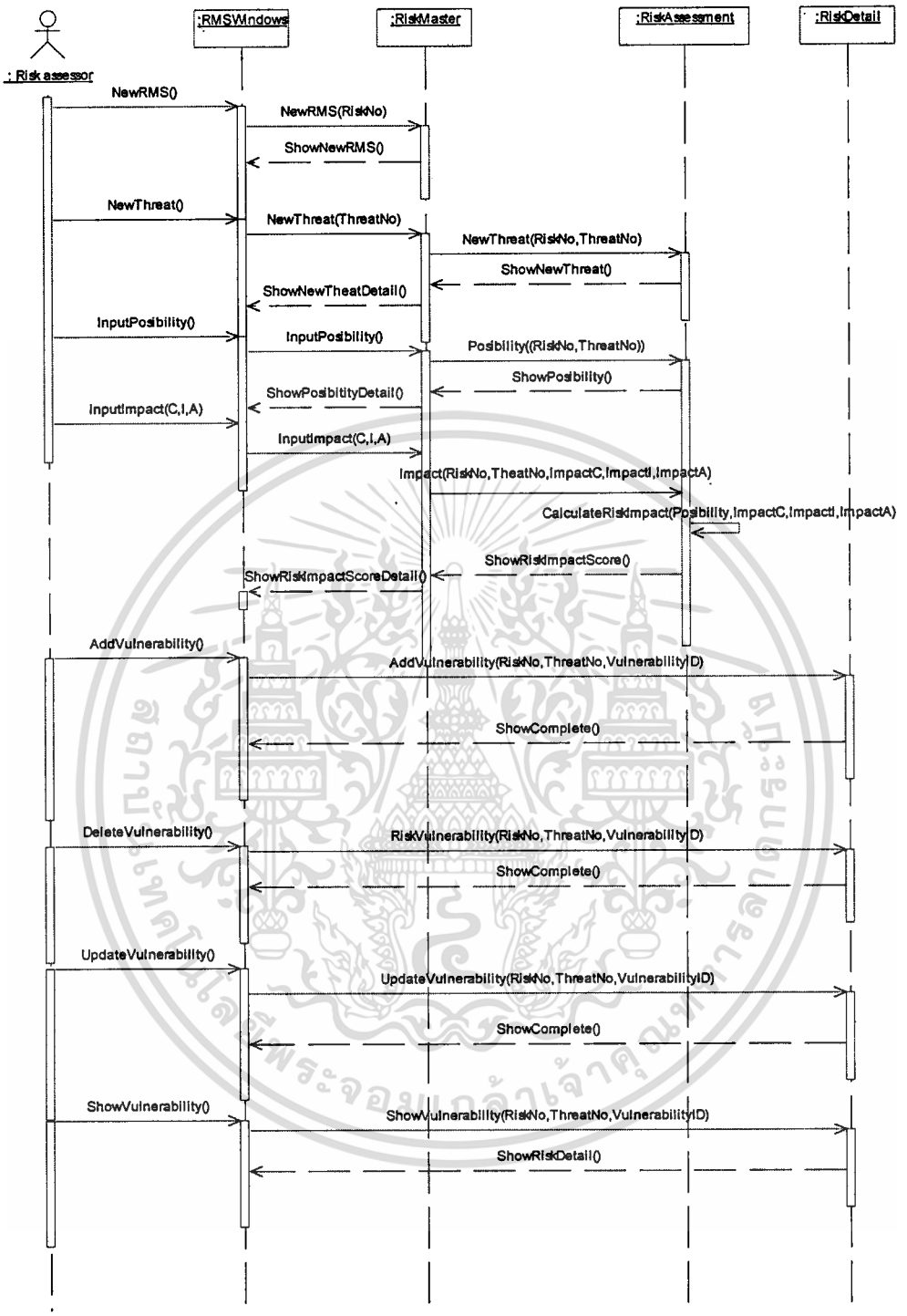
รูปที่ 4.6 Use-case Diagram: Assess Risk



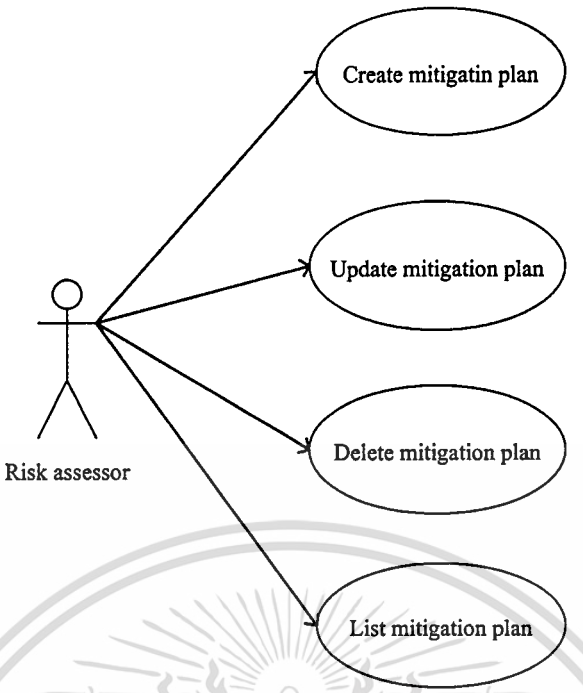
รูปที่ 4.7 Activity Diagram: Assess Risk

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use-case: Assess Risk สามารถอธิบายการทำงานด้วย Activity Diagram ดังรูปที่ 4.7 โดยมีขั้นตอนดังต่อไปนี้

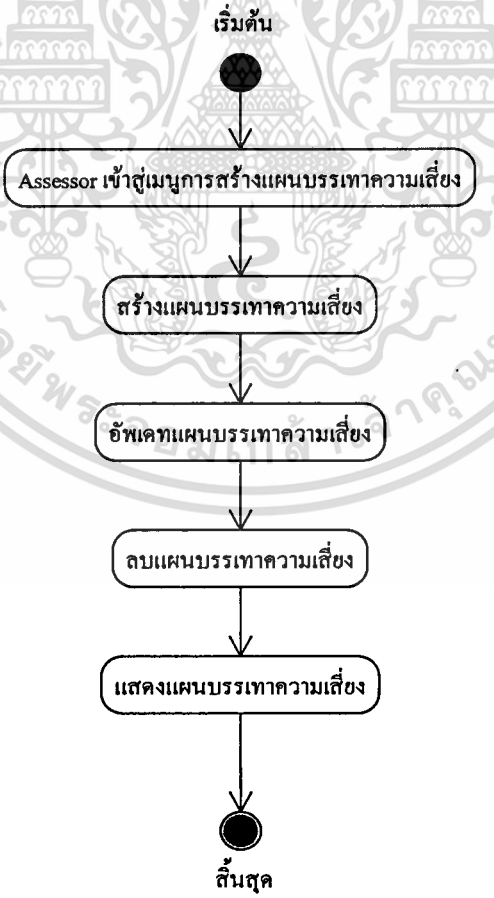
1. ระบบแสดงหน้าต่างการประเมินความเสี่ยงในระบบสารสนเทศ
2. ผู้ประเมินความเสี่ยงให้ข้อมูลความเป็นไปได้ของภัยคุกคามที่เกิดขึ้นแก่ทรัพย์สินในระบบสารสนเทศ
3. ผู้ประเมินความเสี่ยงให้ข้อมูลจุดอ่อนที่ทำให้เกิดภัยคุกคามแก่ทรัพย์สินในระบบสารสนเทศ
4. ผู้ประเมินความเสี่ยงให้ข้อมูลน้ำที่กระทบด้านความปลอดภัยแก่ทรัพย์สินในระบบสารสนเทศ
5. ระบบเข้าสู่เมนูหลักหรือออกจากระบบได้



รูปที่ 4.8 Sequence Diagram: Assess Risk



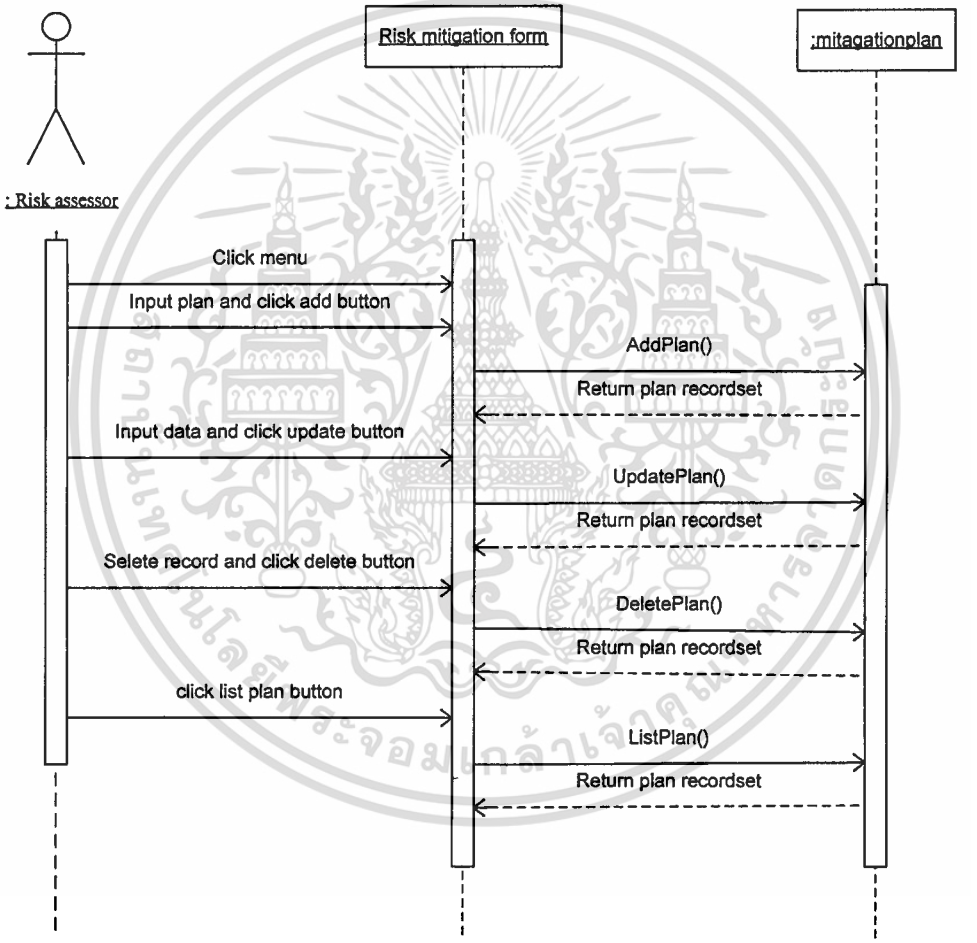
รูปที่ 4.9 Use-case Diagram: Mitigate Risk



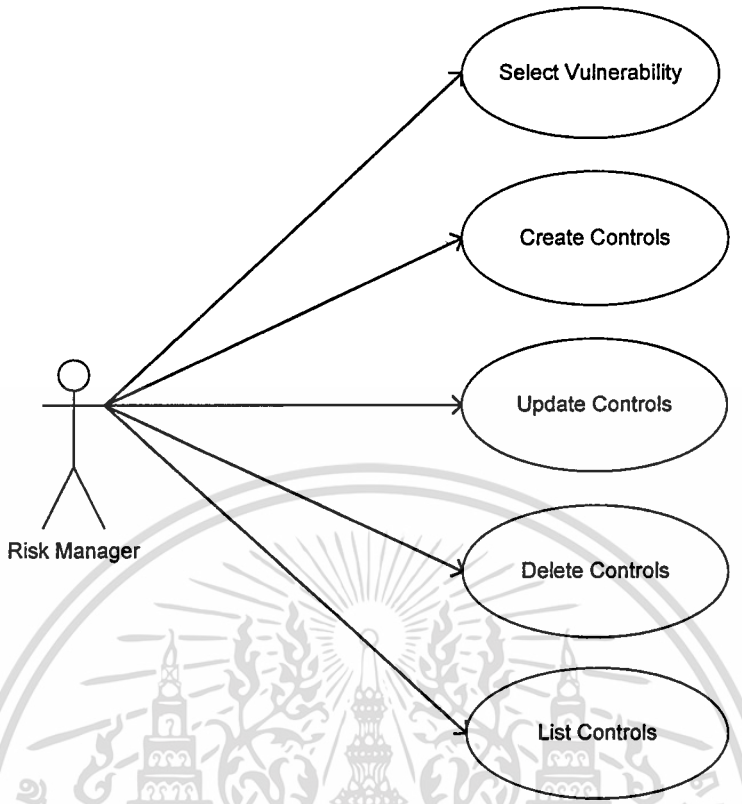
รูปที่ 4.10 Activity Diagram: Mitigate Risk

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use-case: Mitigate Risk สามารถอธิบายการทำงานด้วย Activity Diagram ดังรูปที่ 4.10 โดยมีขั้นตอนดังต่อไปนี้

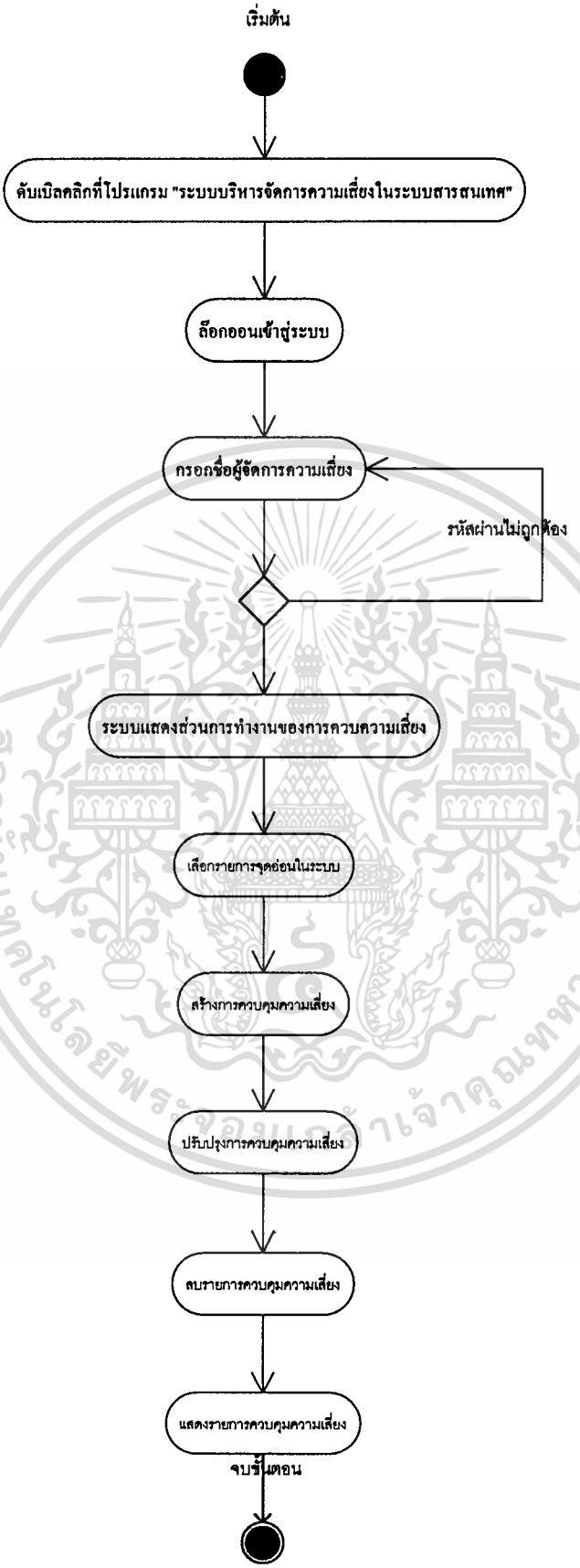
1. ระบบแสดงหน้าต่างการสร้างแผนบรรเทาความเสี่ยงในระบบสารสนเทศ
2. ผู้ประเมินสร้างแผนบรรเทาความเสี่ยงในระบบสารสนเทศตามระดับผลกระทบ
3. ผู้ประเมินอัพเดทแผนบรรเทาความเสี่ยงในระบบสารสนเทศตามระดับผลกระทบ
4. ผู้ประเมินลบแผนบรรเทาความเสี่ยงในระบบสารสนเทศตามระดับผลกระทบ
5. ผู้ประเมินแสดงแผนบรรเทาความเสี่ยงในระบบสารสนเทศตามระดับผลกระทบ
6. ระบบเข้าสู่เมนูหลักหรือออกจากระบบได้



รูปที่ 4.11 Sequence Diagram: Mitigate Risk



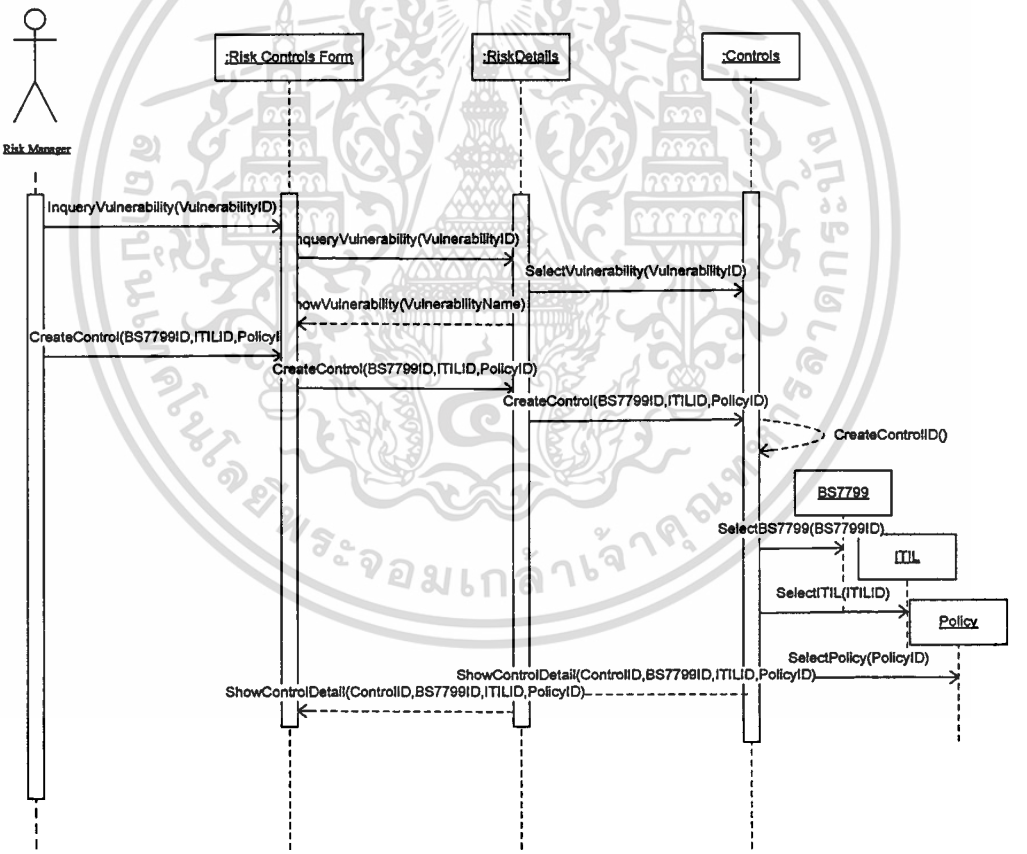
รูปที่ 4.12 Use-case Diagram: Risk Controls



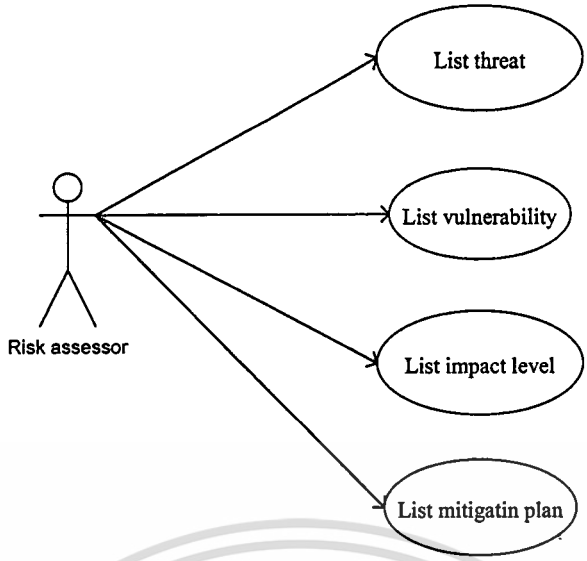
รูปที่ 4.13 Activity Diagram: Risk Controls

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use-case: Risk Controls สามารถอธิบายการทำงานด้วย Activity Diagram ดังรูปที่ 4.13 โดยมีขั้นตอนดังต่อไปนี้

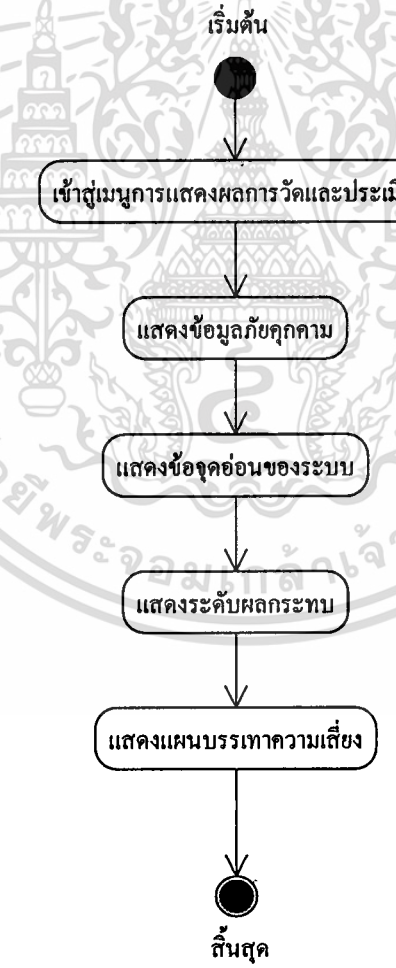
1. ระบบแสดงหน้าต่างการแสดงการควบคุมความเสี่ยง
2. ผู้จัดการความเสี่ยงสามารถเลือกรายการจุดอ่อนในระบบสารสนเทศ
3. ผู้จัดการความเสี่ยงสามารถเลือกรายการสร้างการควบคุมความเสี่ยง
4. ผู้จัดการความเสี่ยงสามารถเลือกการควบคุม ตามข้อกำหนดมาตรฐานความปลอดภัย เลือกข้อกำหนด ITIL และเลือกนโยบายการควบคุม
5. ระบบเข้าสู่เมนูหลักหรือออกจากระบบได้



รูปที่ 4.14 Sequence Diagram: Risk Controls



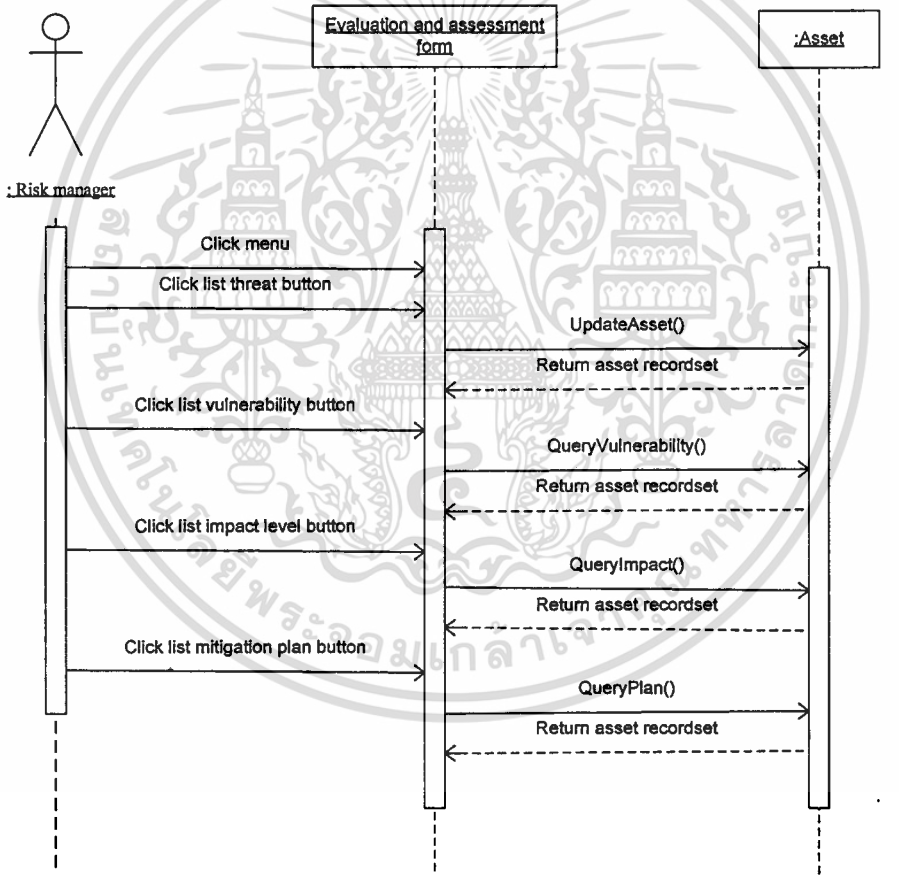
รูปที่ 4.15 Use-case Diagram: Evaluation and assessment



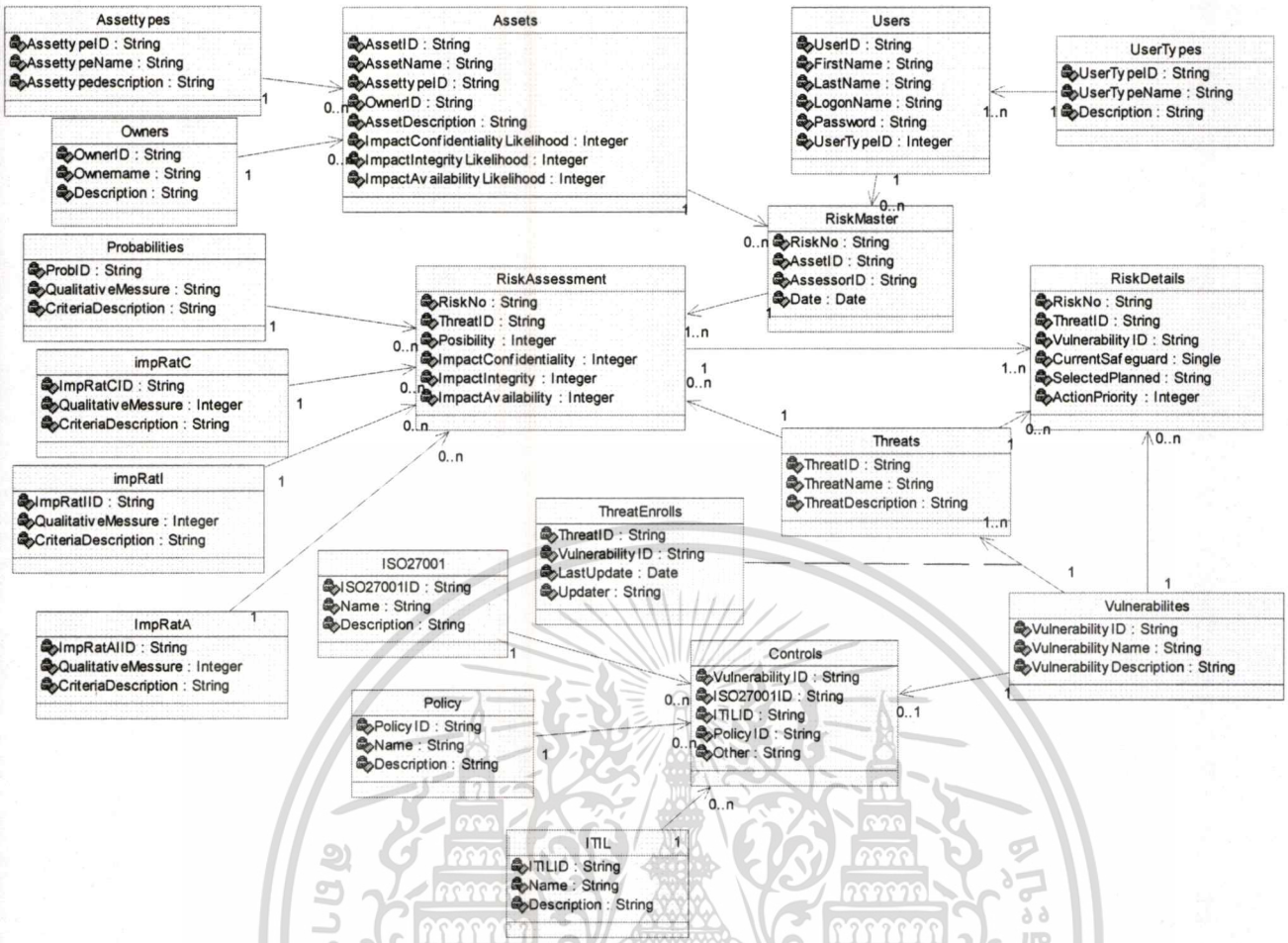
รูปที่ 4.16 Activity Diagram: Evaluation and assessment

ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use-case: Evaluation and assessment สามารถอธิบายการทำงานด้วย Activity Diagram ดังรูปที่ 4.16 โดยมีขั้นตอนดังต่อไปนี้

1. ระบบแสดงหน้าต่างการแสดงการวัดและประเมินผล
6. ผู้จัดการความเสี่ยงสามารถเลือกแสดงรายงานภัยคุกคามในระบบสารสนเทศ
7. ผู้จัดการความเสี่ยงสามารถเลือกแสดงรายงานจุดอ่อนในระบบสารสนเทศ
8. ผู้จัดการความเสี่ยงสามารถเลือกแสดงรายงานระดับผลกระทบในระบบสารสนเทศ
9. ผู้จัดการความเสี่ยงสามารถเลือกแสดงรายงานแผนบรรเทาความเสี่ยงในระบบสารสนเทศ
10. ระบบเข้าสู่เมนูหลักหรือออกจากระบบได้



รูปที่ 4.17 Sequence Diagram: Evaluation and assessment

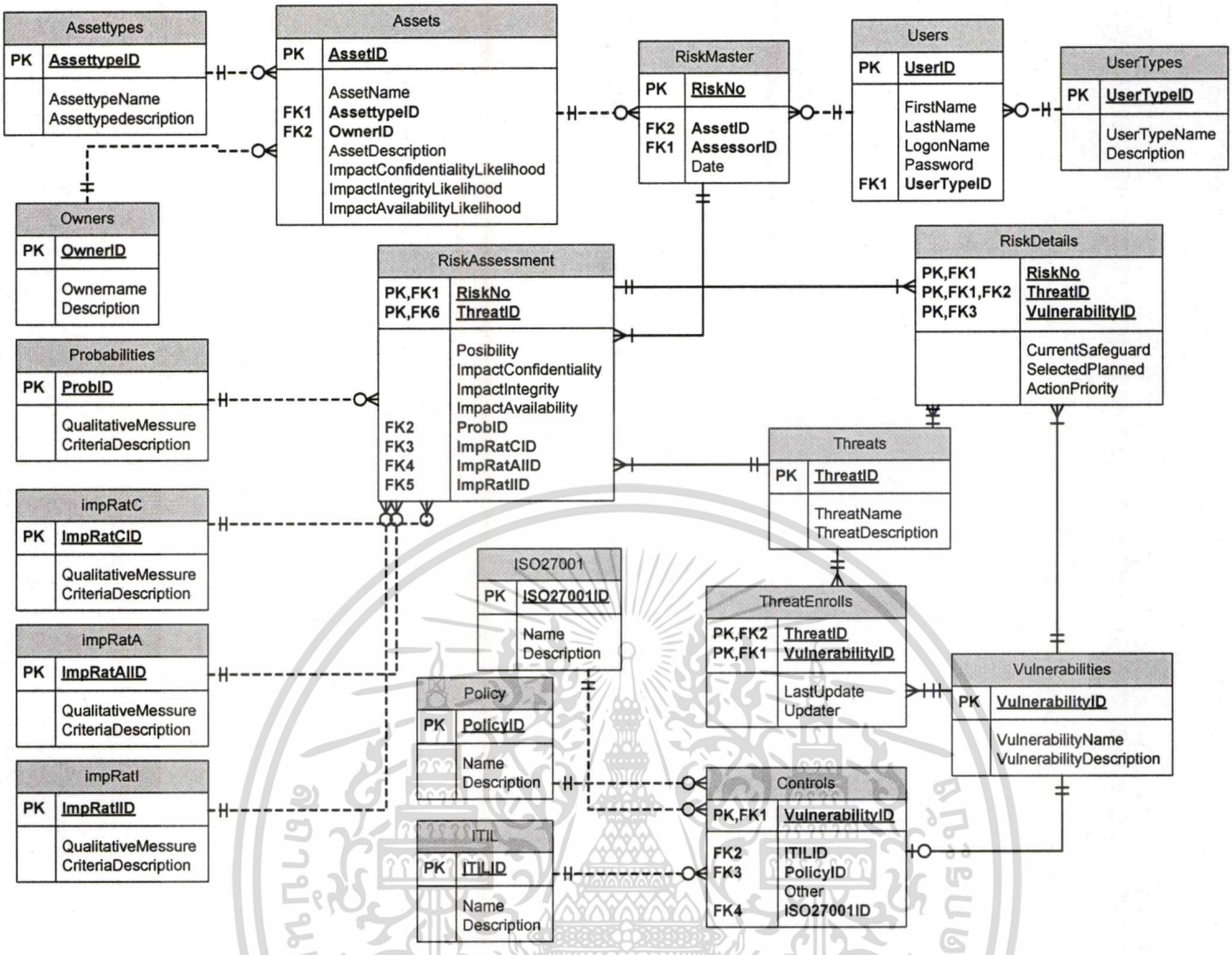


รูปที่ 4.18 Class diagram ของระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

Class diagram เป็นแผนภาพที่แสดงความสัมพันธ์ระหว่างคลาส โดยแสดงส่วนประกอบภายในคลาสทั้งแอตทริบิวต์ และตัวดำเนินการ ดังแสดงในรูปที่ 4.21 อธิบายได้ดังนี้

- คลาส RiskMaster ประกอบด้วย รหัสความเสี่ยง รหัสทรัพย์สิน รหัสผู้รับผิดชอบ รหัสภัยคุกคาม แผนการบรรเทาความเสี่ยง และข้อมูลกระทบด้านความปลอดภัย
- คลาส RiskAssessment ประกอบด้วย รหัสความเสี่ยง รหัสภัยคุกคาม เพื่อนำมาประเมินความเสี่ยงโดยใส่คะแนนใน น้ำหนักความน่าจะเป็น น้ำหนักผลกระทบด้านความลับ ด้านบูรณภาพของข้อมูล และด้านสภาพพร้อมใช้งาน
- คลาส RiskDetail ประกอบด้วย รหัสความเสี่ยง รหัสภัยคุกคาม รหัสจุดอ่อนของระบบที่สัมพันธ์กับภัยคุกคาม เพื่อนำรายการความอ่อนแอของระบบเหล่านี้ไปสร้างแผนบรรเทาป้องกัน และควบคุมตามระดับผลกระทบต่อไป
- คลาส Assets ประกอบด้วย รหัสทรัพย์สิน และข้อมูลเกี่ยวกับทรัพย์สิน
- คลาส Assettype ประกอบด้วย รหัสประเภททรัพย์สิน ชื่อประเภททรัพย์สิน
- คลาส Threats ประกอบด้วย รหัสภัยคุกคาม ข้อมูลภัยคาม
- คลาส Vulnerabilities ประกอบด้วย รหัสจุดอ่อน ข้อมูลจุดอ่อน

- คลาส ThreatEnrolls ประกอบด้วย รหัสภัยคุกคาม รหัสจุดอ่อน วันที่ปรับปรุงข้อมูล และผู้ปรับปรุงข้อมูล
- คลาส Users ประกอบด้วย รหัสผู้ใช้ และข้อมูลผู้ใช้
- คลาส Owners ประกอบด้วย รหัสเจ้าของหน่วยบริการ เพื่อแสดงความเป็นเจ้าของทรัพย์สิน เพื่อแสดงขอบเขตในการจัดการความเสี่ยงในระบบสารสนเทศ
- คลาส Probabilities ประกอบด้วย รหัสความเป็นไปได้ ระดับคะแนนความเป็นไปได้ และรายละเอียดความเป็นไปได้ในแต่ละระดับ
- คลาส ImpactC ประกอบด้วย รหัสผลกระทบด้านความลับ ระดับคะแนนผลกระทบด้านความลับ และรายละเอียดคะแนนในแต่ละระดับ
- คลาส ImpactI ประกอบด้วย รหัสผลกระทบด้านบูรณภาพ ระดับคะแนนผลกระทบด้านบูรณภาพ และรายละเอียดคะแนนในแต่ละระดับ
- คลาส ImpactA ประกอบด้วย รหัสผลกระทบด้านสภาพพร้อมใช้งาน ระดับคะแนนผลกระทบด้านสภาพพร้อมใช้งาน และรายละเอียดคะแนนในแต่ละระดับ
- คลาส Controls ประกอบด้วย รหัสการควบคุม รหัสมาตราฐานความปลอดภัย รหัส ITIL และรหัสนโยบายความคุม
- คลาส ISO27001 ประกอบด้วย รหัสมาตราฐานความปลอดภัย และข้อมูลมาตราฐานความปลอดภัย
- คลาส ITIL ประกอบด้วย รหัสกระบวนการ ITIL และข้อมูลกระบวนการ ITIL
- คลาส Policy ประกอบด้วย รหัสนโยบายควบคุมความเสี่ยงในระบบสารสนเทศ และข้อมูลนโยบายควบคุมความเสี่ยงในระบบสารสนเทศ



รูปที่ 4.19 ER diagram ของระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

บทที่ 5
การออกแบบฐานข้อมูล

5.1 แบบจำลองความสัมพันธ์ระหว่างเอนทิตี

เนื่องจากระบบฐานข้อมูลมีการอิมพลีเมนท์ด้วยระบบฐานข้อมูลเชิงสัมพันธ์ดังนั้น การสร้างตารางจึงต้องนำมาจากแบบจำลองความสัมพันธ์ระหว่างเอนทิตี โดยการออกแบบใช้แผนภาพอีอาร์แสดงความสัมพันธ์ระหว่างเอนทิตีที่เกี่ยวข้องกัน โดยการออกแบบแบบจำลองความสัมพันธ์ของข้อมูลในระบบ ประกอบด้วยข้อมูลที่มีความสัมพันธ์ดังรูปที่ 4.19 ในบทที่ 4

5.2 รายละเอียดข้อมูลที่จัดเก็บในระบบ

ฐานข้อมูลของระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ ออกแบบโดยการนำ ER diagram มาเขียนให้อยู่ในรูปตารางฐานข้อมูลพร้อมระบุแอตทริบิต ชนิดข้อมูล โดยแสดงรายละเอียดของข้อมูลในแต่ละแอตทริบิวต์ ดังตารางที่ 5.1 – 5.18

ตารางที่ 5.1 ข้อมูลระดับผลกระทบด้านความลับ (IMRATC)

Table Name : IMRATC Description : ข้อมูลระดับผลกระทบด้านความลับเพื่อให้น้ำหนักแก่ภัยคุกคาม				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ImpRatCID	รหัสผลกระทบด้านความลับ	int	PK	
QualitativeMessure	น้ำหนักผลกระทบด้านความลับ	nvarchar(20)		
CriteriaDescription	รายละเอียดผลกระทบด้านความลับ	nvarchar(MAX)		

ตารางที่ 5.2 ข้อมูลระดับผลกระทบด้านบูรณภาพ (IMRATI)

Table Name : IMRATI Description : ข้อมูลระดับผลกระทบด้านบูรณภาพเพื่อให้น้ำหนักแก่ภัยคุกคาม				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ImpRatAIID	รหัสผลกระทบด้าน	int	PK	

ตารางที่ 5.2 (ต่อ)

	บูรณภาพ			
QualitativeMessure	น้ำหนักผลกระทบด้านบูรณภาพ	nvarchar(20)		
CriteriaDescription	รายละเอียดผลกระทบด้านบูรณภาพ	nvarchar(MAX)		

ตารางที่ 5.3 ข้อมูลระดับผลกระทบด้านสภาพพร้อมใช้งาน (IMRATA)

Table Name : IMRATA Description : ข้อมูลระดับผลกระทบด้านสภาพพร้อมใช้งานเพื่อให้น้ำหนักแก่ภัยคุกคาม				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ImpRatAID	รหัสผลกระทบด้านสภาพพร้อมใช้งาน	int	PK	
QualitativeMessure	น้ำหนักผลกระทบด้านสภาพพร้อมใช้งาน	nvarchar(20)		
CriteriaDescription	รายละเอียดผลกระทบด้านสภาพพร้อมใช้งาน	nvarchar(MAX)		

ตารางที่ 5.4 ข้อมูลระดับคะแนนความเป็นไปได้ (PROBABILITIES)

Table Name : PROBABILITIES Description : ข้อมูลระดับคะแนนความเป็นไปได้ในการเกิดภัยคุกคาม				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ProbID	รหัสระดับคะแนนความเป็นไปได้	int	PK	
QualitativeMessure	น้ำหนักระดับคะแนนความเป็นไปได้	nvarchar(20)		
CriteriaDescription	รายละเอียดระดับคะแนนความเป็นไปได้	nvarchar(MAX)		

ตารางที่ 5.5 ข้อมูลเจ้าของทรัพย์สิน (OWNERS)

Table Name : OWNERS Description : ข้อมูลเจ้าของทรัพย์สิน หรือหน่วยให้บริการ กำหนดขึ้นเพื่อแสดงขอบเขตของทรัพย์สินในหน่วยบริการเพื่อการประเมินความเสี่ยง เช่น WAN SAN MAIL และ Data Center				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
OwnerID	รหัสเจ้าของทรัพย์สิน	nvarchar(5)	PK	
Ownername	ชื่อเจ้าของทรัพย์สิน	nvarchar(15)		
Description	รายละเอียดเจ้าของทรัพย์สิน	nvarchar(MAX)		

ตารางที่ 5.6 ข้อมูลผู้ใช้ (USERS)

Table Name : USERS Description : ข้อมูลผู้ใช้งาน				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
UserID	รหัสผู้ใช้	nvarchar(5)	PK	
FirstName	ชื่อผู้ใช้	nvarchar(15)		
LastName	นามสกุลผู้ใช้	nvarchar(20)		
LogonName	ชื่อเพื่อเข้าระบบ	nvarchar(10)		
Password	รหัสผ่าน	nvarchar(15)		
UserTypeID	ประเภทผู้ใช้	nvarchar(5)		

ตารางที่ 5.7 ข้อมูลความเสี่ยงหลัก (RISKMASTER)

Table Name : RISKMASTER Description : ข้อมูลความเสี่ยงหลัก				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
RiskNo	รหัสความเสี่ยง	nvarchar(5)	PK	
AssetID	รหัสทรัพย์สิน	nvarchar(5)	FK	ASSETS
AssessorID	รหัสผู้ประเมิน	nvarchar(5)	FK	USERS
Date	วันที่ประเมิน	datetime		

ตารางที่ 5.8 ข้อมูลการประเมินความเสี่ยง (RISKASSESSMENT)

Table Name : RISKASSESSMENT Description : ข้อมูลการประเมินความเสี่ยง				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
RiskNo	รหัสความเสี่ยง	nvarchar(5)	PK,FK	RISKMASTER
ThreatID	รหัสภัยคุกคาม	nvarchar(5)	PK,FK	THREATS
Posibility	คะแนนผลกระทบความเป็นไปได้	int	FK	PROBABILITIES
ImpactConfidentiality	คะแนนผลกระทบด้านความลับ	int	FK	IMPRATC
ImpactIntegrity	คะแนนผลกระทบด้านบูรณภาพ	int	FK	IMPRATI
ImpactAvailability	คะแนนผลกระทบด้านสภาพพร้อมใช้	int	FK	IMPRATA

ตารางที่ 5.9 ข้อมูลรายละเอียดความเสี่ยง (RISKDETAILS)

Table Name : RISKDETAILS Description : ข้อมูลรายละเอียดความเสี่ยง				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
RiskNo	รหัสความเสี่ยง	nvarchar(5)	PK,FK	RISKASSESSMENT
ThreatID	รหัสภัยคุกคาม	nvarchar(5)	PK,FK	THREATS
VulnerabilityID	รหัสความอ่อนแอ	nvarchar(5)	PK,FK	VULNERABILITIES
CurrentSafeguard	วิธีการป้องกันปัจจุบัน	nvarchar(50)		
SelectedPlanned	แผนการป้องกันที่ถูกเลือก	nvarchar(50)		
ActionPriority	ความเร่งด่วนในปฏิบัติ	int		

ตารางที่ 5.10 ข้อมูลภัยคุกคาม (THREATS)

Table Name : THREATS Description : ข้อมูลภัยคุกคาม				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ThreatID	รหัสภัยคุกคาม	nvarchar(5)	PK	
ThreatName	ชื่อภัยคุกคาม	nvarchar(50)		
ThreatDescription	อธิบายภัยคุกคาม	nvarchar(MAX)		

ตารางที่ 5.11 ข้อมูลคุกคามที่สัมพันธ์กับความอ่อนแอ (THREATENROLLS)

Table Name : THREATENROLLS Description : ข้อมูลภัยคุกคามที่สัมพันธ์กับความอ่อนแอของระบบ				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ThreatID	รหัสภัยคุกคาม	nvarchar(5)	PK,FK	THREATS
VulnerabilityID	รหัสความอ่อนแอ	nvarchar(5)	PK,FK	VULNERABILITIES
LastUpdate	วันที่ปรับปรุงล่าสุด	datetime		
Updater	ผู้ปรับปรุง	nvarchar(30)		

ตารางที่ 5.12 ข้อมูลความอ่อนแอ (VULNERABILITIES)

Table Name : VULNERABILITIES Description : ข้อมูลความอ่อนแอหรือจุดอ่อน				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
VulnerabilityID	รหัสความอ่อนแอ	nvarchar(5)	PK	
VulnerabilityName	ชื่อความอ่อนแอ	nvarchar(70)		
VulnerabilityDescription	อธิบายความอ่อนแอ	nvarchar(MAX)		

ตารางที่ 5.13 ข้อมูลทรัพย์สิน (ASSETS)

Table Name : ASSETS Description : ข้อมูลสินทรัพย์				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
AssetID	รหัสทรัพย์สิน	nvarchar(5)	PK	
AssetName	ชื่อทรัพย์สิน	nvarchar(60)		

ตารางที่ 5.13 (ต่อ)

AssetTypeID	รหัสประเภททรัพย์สิน	nvarchar(5)	FK	ASSETTYPE
OwnerID	รหัสเจ้าของทรัพย์สิน	nvarchar(5)	FK	OWNERS
AssetDescription	อธิบายทรัพย์สิน	nvarchar(MAX)		
ImpactConfidentialityLikelihood	คะแนนน้ำหนักผลกระทบด้านความลับ	int	FK	IMPRATC
ImpactIntegrityLikelihood	คะแนนน้ำหนักผลกระทบด้านบูรณภาพ	int	FK	IMPRATI
ImpactAvailabilityLikelihood	คะแนนน้ำหนักผลกระทบด้านสภาพพร้อมใช้	int	FK	IMPRATA

ตารางที่ 5.14 ข้อมูลประเภททรัพย์สิน (ASSETTYPES)

Table Name : ASSETTYPES

Description : ข้อมูลประเภททรัพย์สิน

ชื่อ	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างถึง
AssettypeID	รหัสประเภททรัพย์สิน	nvarchar(5)	PK	
AssettypeName	ชื่อประเภททรัพย์สิน	nvarchar(25)		
Assettypedescription	อธิบายประเภททรัพย์สิน	nvarchar(MAX)		

ตารางที่ 5.15 ข้อมูลการควบคุม (CONTROLS)

Table Name : CONTROLS

Description : ข้อมูลการควบคุม

ชื่อ	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางอ้างถึง
VulnerabilityID	รหัสความอ่อนแอ	nvarchar(5)	PK	
ISO27001ID	รหัสมาตราฐานความปลอดภัย	nvarchar(5)	FK	ISO27001

ตารางที่ 5.15 (ต่อ)

ITILID	รหัสกระบวนด้านITIL	nvarchar(5)	FK	ITIL
PolicyID	รหัสนโยบายด้านIT	nvarchar(5)	FK	POLICY
Other	การควบคุมอื่นๆ	nvarchar(60)		

ตารางที่ 5.16 ข้อมูลมาตราฐานความปลอดภัย (ISO27001)

Table Name : ISO27001 Description : ข้อมูลมาตราฐานความปลอดภัย				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ISO27001ID	รหัสมาตราฐานความปลอดภัย	nvarchar(5)	PK	
Name	ข้อกำหนดมาตราฐานความปลอดภัย	nvarchar(60)		
Description	อธิบายเกี่ยวกับข้อกำหนด	nvarchar(60)		

ตารางที่ 5.17 ข้อมูลกระบวนด้านITIL (ITIL)

Table Name : ITIL Description : ข้อมูลกระบวนด้านITIL				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
ITILID	รหัสกระบวน ITIL	nvarchar(5)	PK	
Name	ชื่อกระบวน ITIL	nvarchar(60)		
Description	อธิบายเกี่ยวกับ ITIL Process	nvarchar(60)		

ตารางที่ 5.18 ข้อมูลนโยบายควบคุม (POLICY)

Table Name : POLICY Description : ข้อมูลนโยบาย				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
PolicyID	รหัสนโยบาย	nvarchar(5)	PK	
Name	ชื่อนโยบายควบคุม	nvarchar(60)		
Description	อธิบายเกี่ยวกับ นโยบายควบคุม	nvarchar(60)		

ตารางที่ 5.19 ข้อมูลประเภทผู้ใช้ (USERTYPES)

Table Name : USERTYPES Description : ข้อมูลประเภทผู้ใช้				
ชื่อ	**คำอธิบาย**	**ชนิดข้อมูล**	**คีย์**	**ตารางอ้างถึง**
UserTypeID	รหัสประเภทผู้ใช้	nvarchar(5)	PK	
UserTypeName	ชื่อประเภทผู้ใช้	nvarchar(15)		
Description	อธิบายเกี่ยวกับ ประเภทผู้ใช้	nvarchar(60)		

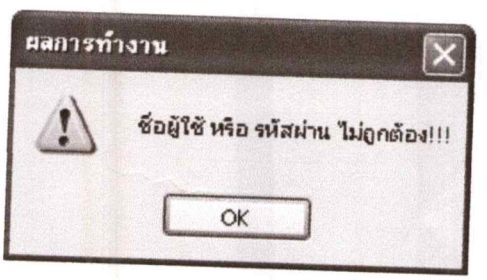
บทที่ 6
การใช้งานระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

6.1 การเข้าสู่ระบบ

คลิ๊กเพื่อเปิดโปรแกรม "ระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ" ระบบแสดงหน้าจอการเข้าสู่ระบบดังรูปที่ 6.1 โดยการใส่ชื่อผู้ใช้และรหัสผ่านเพื่อแสดงตนโดยระบบจะทำการตรวจสอบชื่อและรหัสผ่านเปรียบเทียบกับฐานข้อมูลรายชื่อผู้ใช้ในระบบ และหากชื่อหรือรหัสผ่านผิดพลาดจะแสดงหน้าจอดังรูปที่ 6.2 ถ้ารหัสผ่านถูกต้องระบบจะทำการตรวจสอบสิทธิ์การใช้งานระบบ ว่าอยู่ในระบบไหน และนำเข้าสู่หน้าจอหลัก และอนุญาตหน้าจอการทำงานตามสิทธิ์ที่ได้รับ

เมื่อเข้าสู่ระบบ หน้าจอหลักจะแสดงเมนูการทำงานหลัก 4 หน้าที่การทำงานด้วยกัน คือ การระบุส่วนประกอบของข้อมูลหลัก การประเมินความเสี่ยง การบรรเทาความเสี่ยง และการวัดและประเมินผล

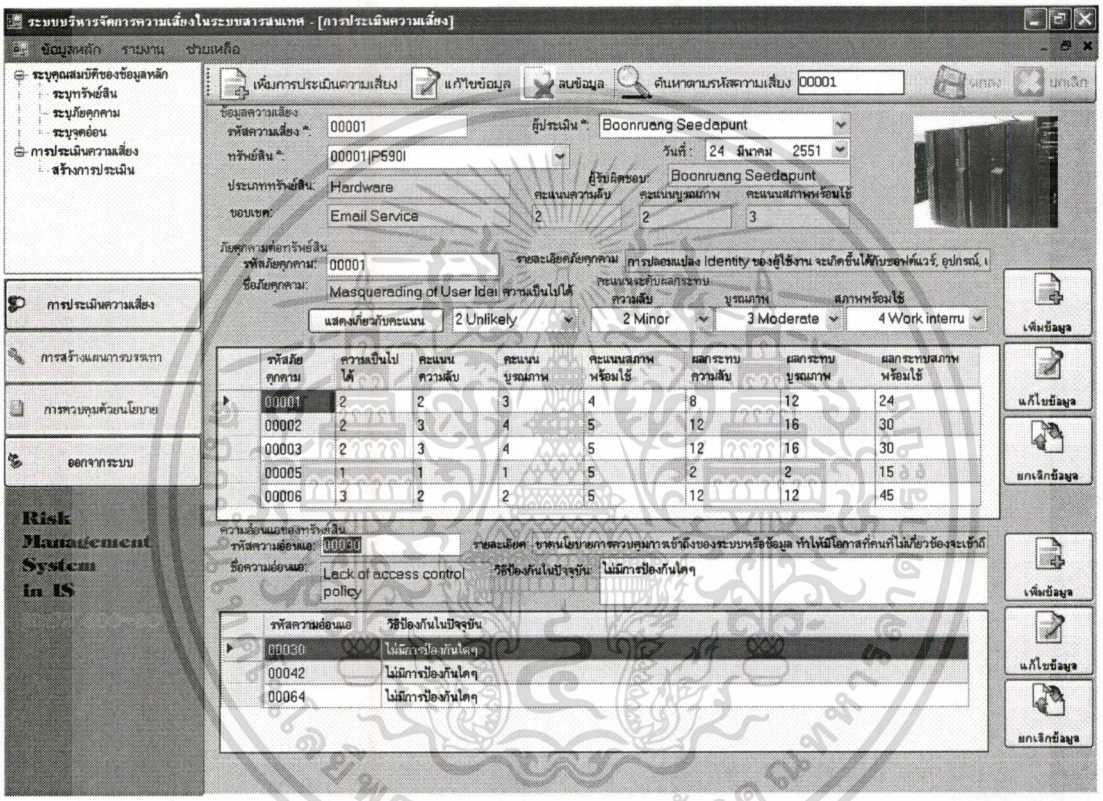
รูปที่ 6.1 หน้าจอแสดงตนเพื่อเข้าสู่ระบบ



รูปที่ 6.2 หน้าจอเข้าสู่ระบบผิดพลาด

6.2 หน้าจอหลัก

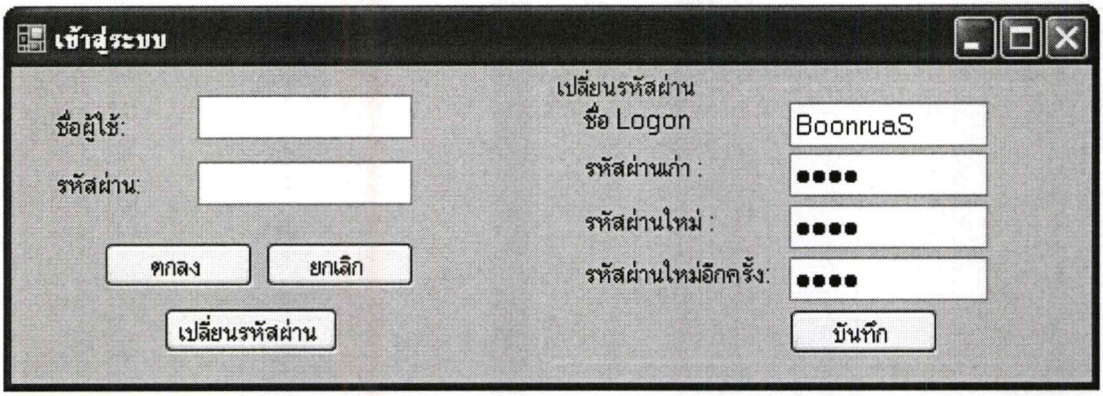
หน้าจอการทำงานหลักประกอบด้วยเมนูสั่งงานและส่วนแสดงผล โดยประกอบด้วยเมนูการเรียกโปรแกรมอยู่ 4 ประเภท คือ เมนูบาร์ ทูลบาร์ บัททอนเมนู และทรีวิวเมนู ซึ่งเมนูแต่ล่ะจะทำหน้าที่เรียนเรียกใช้โปรแกรมย่อยเหมือนกัน ซึ่งเมนูแต่ละประเภทจะให้ความสะดวกในการเรียกใช้งานแตกต่างกัน ส่วนแสดงผลจะการทำงานของโปรแกรมดังรูป 6.3



รูปที่ 6.3 หน้าจอหลักของระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

6.3 การเปลี่ยนรหัสผ่าน

เมื่อเข้าสู่ระบบดังรูปที่ 6.1 ผู้ใช้สามารถเลือกเปลี่ยนรหัสผ่านได้ด้วยตนเองโดยเลือกไปที่ปุ่มเปลี่ยนรหัสผ่าน และสามารถเปลี่ยนรหัสผ่านได้โดยการเติมชื่อรหัสผ่านเดิม และรหัสผ่านใหม่รูปที่ 6.4 หากการเปลี่ยนรหัสผ่านไม่สำเร็จหรือมีข้อผิดพลาดหน้าจอจะแสดงดังรูปที่ 6.5 และสำเร็จเรียบร้อยจะแสดงผลดังรูปที่ 6.6



รูปที่ 6.4 หน้าจอการเปลี่ยนรหัสผ่าน

รูปที่ 6.5 หน้าจอเปลี่ยนรหัสผ่านไม่ถูกต้อง

รูปที่ 6.6 หน้าจอเปลี่ยนรหัสผ่านเรียบร้อย

6.4 การจัดการบัญชีผู้ใช้

เป็นหน้าจอสำหรับผู้ดูแลระบบ เพื่อทำหน้าที่กำหนดบทบาทของผู้ใช้ในระบบ ปรับปรุงข้อมูล แก้ไขรหัสผ่านของผู้ใช้ และกำหนดระบบสิทธิ์ของผู้ใช้ ซึ่งมี 3 ระดับคือ ระดับสิทธิ์ผู้ดูแลระบบคือค่า 1 ระดับผู้ประเมินความเสี่ยงคือค่า 2 ระดับผู้จัดการความเสี่ยงคือค่า 3 แสดงรายการผู้ใช้ในระบบและระดับสิทธิ์ดังรูปที่ 6.7

รูปที่ 6.7 หน้าจอการจัดการบัญชีผู้ใช้

6.5 การระบุส่วนประกอบของข้อมูลหลัก

ข้อมูลที่อยู่ในขอบเขตการประเมินต้องได้รับการระบุเป็นข้อมูลเบื้องต้นก่อนการประเมินความเสี่ยง โดยประกอบด้วย ข้อมูลทรัพย์สินในระบบสารสนเทศ ข้อมูลภัยคุกคาม และข้อมูลจุดอ่อน โดยข้อมูลดังกล่าวหากไม่ครบถ้วนสามารถเพิ่ม หรือปรับปรุงได้ระหว่างการประเมิน

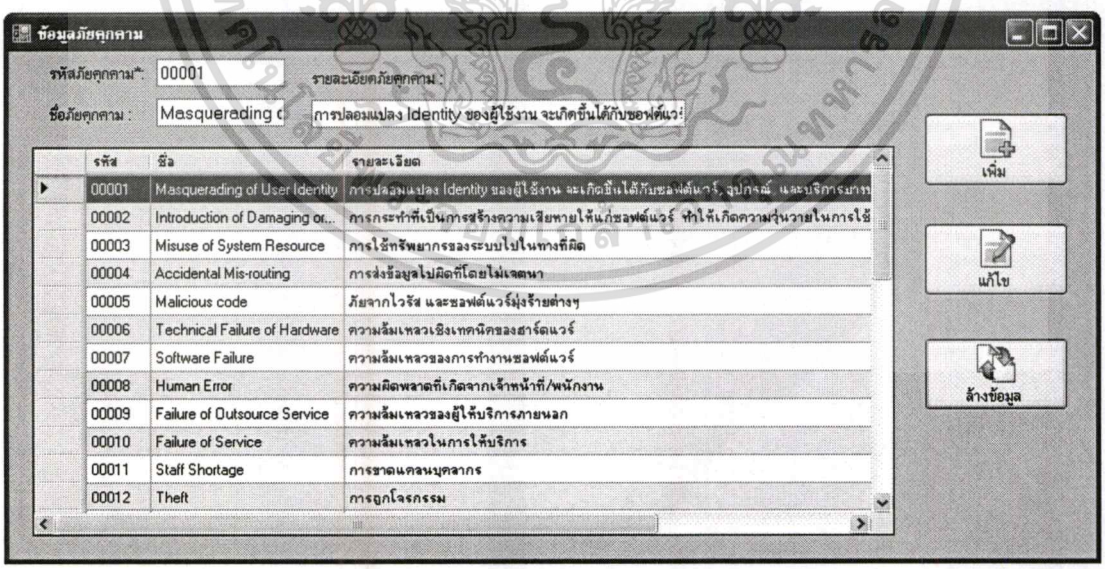
6.5.1 ข้อมูลทรัพย์สินในระบบสารสารสนเทศ

ทรัพย์สินในระบบจะถูกแสดงออกมาเพื่อการประเมินความเสี่ยง เพื่อเป้าหมายในการสร้างแผนป้องกันหรือบรรเทาและสร้างนโยบายเพื่อควบคุม โดยทรัพย์สินในการประเมินจะอยู่ภายในขอบเขตที่จะทำการจัดตั้งมาตราฐาน หรืออยู่ในขอบเขตที่ต้องการสร้างนโยบายควบคุมจะต้องระบุไว้ในส่วนของเจ้าของระบบหรือหน่วยบริการ เช่น การจัดตั้งมาตราฐานที่อยู่ในขอบเขตของ ระบบเครือข่ายแวน ระบบจัดเก็บข้อมูลส่วนกลาง หรือระบบอีเมลขององค์กร ซึ่งในขอบเขตเหล่านี้ประกอบไปด้วยทรัพย์สินต่างๆ โดยสามารถแบ่งได้ 5 ประเภทดังนี้ ฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศ บุคคล และบริการในระบบสารสนเทศ

รูปที่ 6.8 หน้าจอข้อมูลทรัพย์สินในระบบสารสนเทศ

6.5.2 ข้อมูลภัยคุกคาม

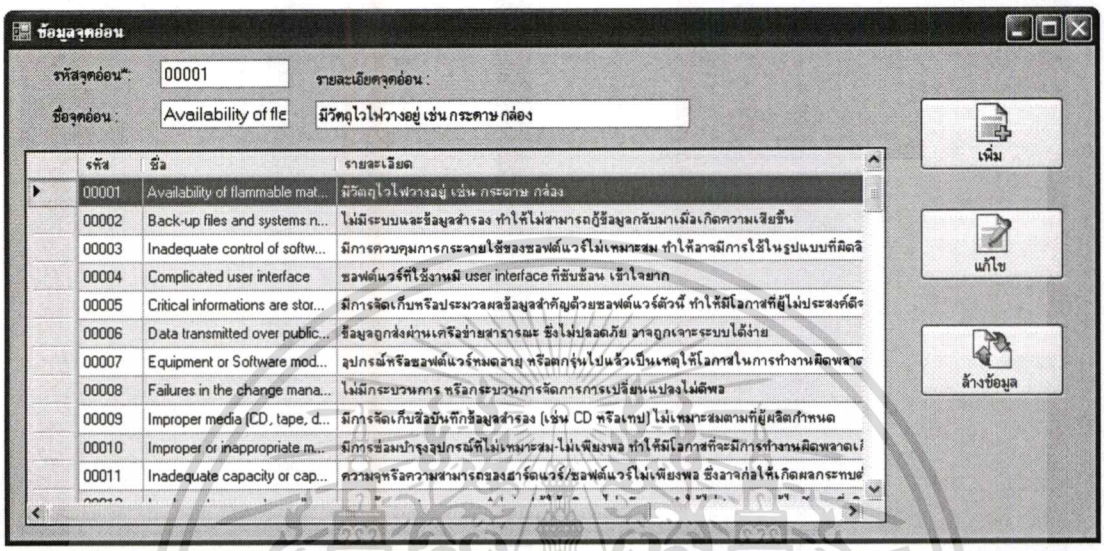
เป็นการระบุข้อมูลภัยคุกคามที่ทำให้เกิดความเสี่ยงแก่ระบบสารสนเทศ โดยให้รหัส ชื่อภัยคุกคาม และรายละเอียดภัยคุกคาม ดังรูปที่ 6.9



รูปที่ 6.9 หน้าจอข้อมูลภัยคุกคาม

6.5.3 ข้อมูลจุดอ่อน

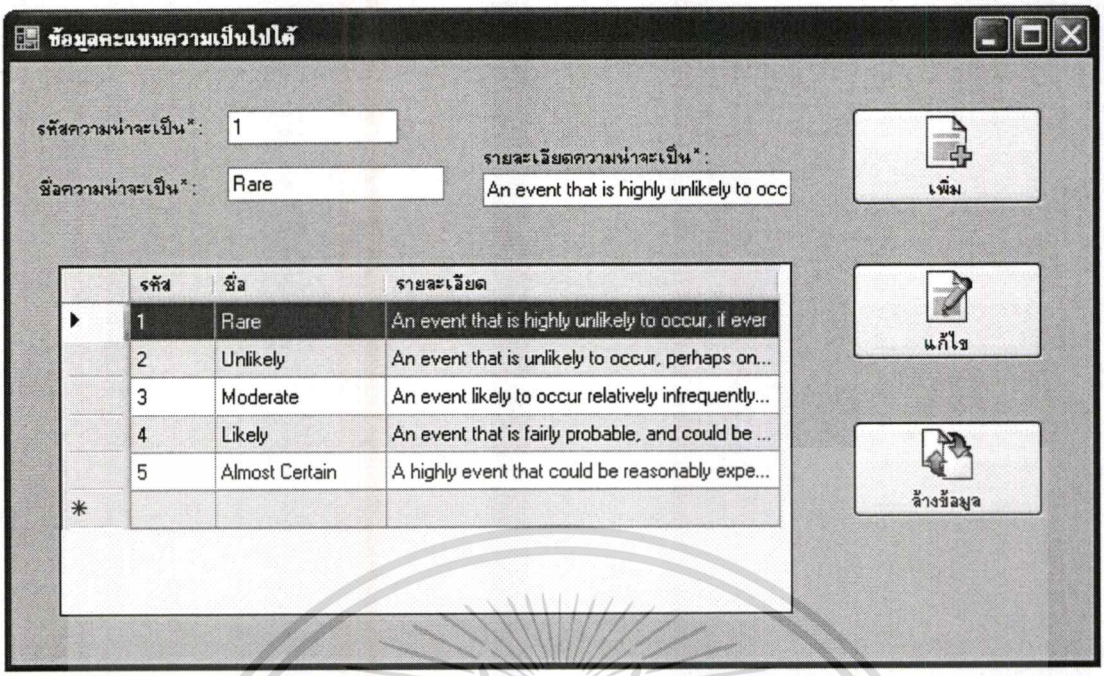
เป็นการระบุจุดอ่อนของทรัพย์สินในระบบ ที่เป็นช่องทางให้เกิดความเสียหาย และสร้างผลกระทบแก่ทรัพย์สินในมุมมองด้านความปลอดภัย 3 ด้าน ดังนี้ ด้านความลับ ด้านบูรณภาพ และด้านสภาพพร้อมใช้ ข้อมูลจุดอ่อนแสดงดังรูปที่ 6.10



รูปที่ 6.10 หน้าจอข้อมูลจุดอ่อน

6.5.4 ข้อมูลคะแนนความเป็นไปได้

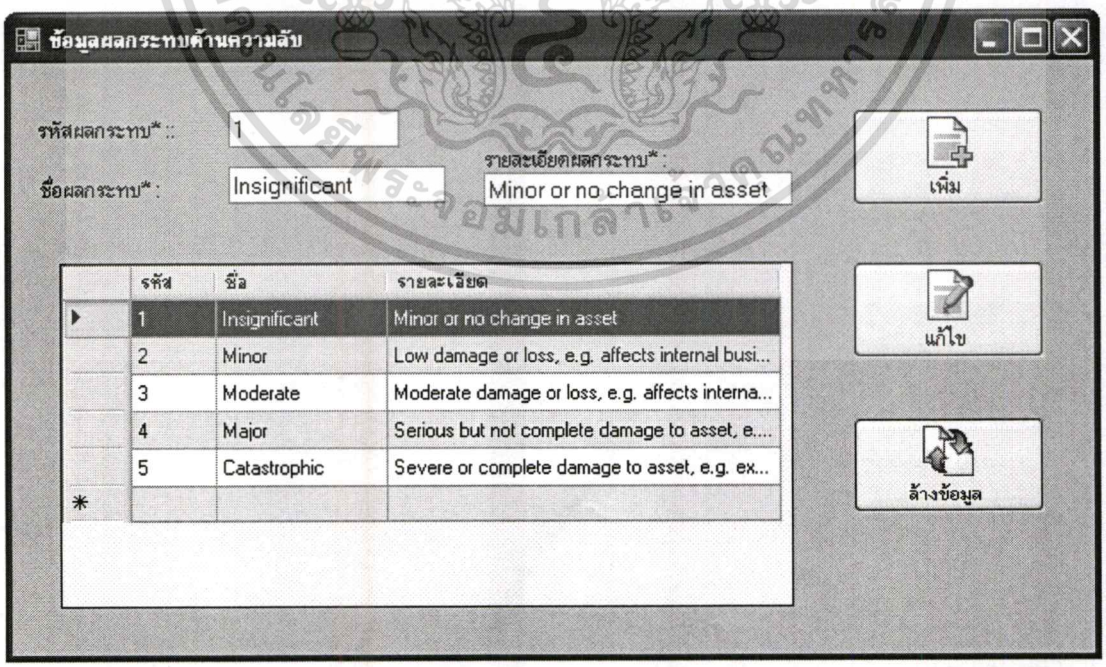
ระดับคะแนนความเป็นไปได้ในการประเมินภัยคุกคามที่เกิดขึ้นกับทรัพย์สิน ซึ่งแต่ละระดับบอกความถี่ของการเกิดเหตุการณ์ในแต่ละครั้ง ระดับที่ 1 เกิดขึ้นได้ยาก ระดับที่ 2 พบได้ไม่บ่อยอาจจะ 3 ปีต่อครั้ง ระดับที่ 3 พบได้ปานกลางปีละครั้ง ระดับที่ 4 ค่อนข้างมาก ระดับที่ 5 เกิดขึ้นถี่มาก ปีละหลายครั้ง ดังรูปที่ 6.11



รูปที่ 6.11 หน้าจอข้อมูลคะแนนความเป็นไปได้

6.5.5 ข้อมูลคะแนนผลกระทบด้านความลับ

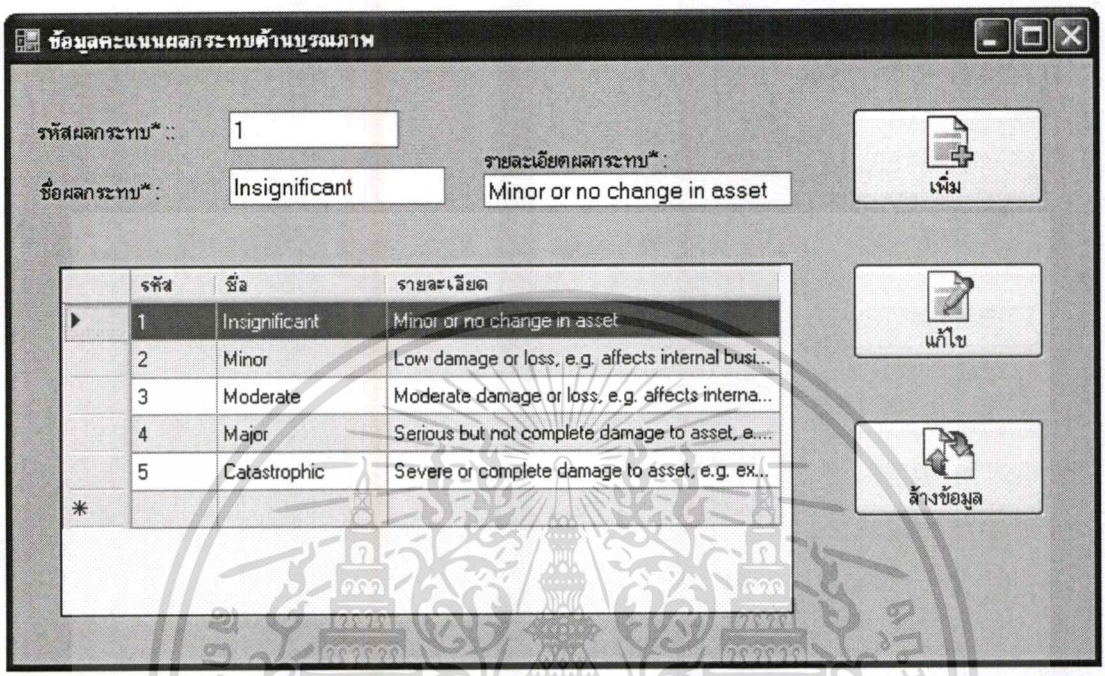
ระดับผลกระทบในมุมมองความปลอดภัยในระบบสารสนเทศในด้านความลับ ระดับผลกระทบมี 5 ระดับ เรียงตามระดับผลกระทบจากน้อยมากไปถึงระดับมากที่สุด 1-5 ดังรูปที่ 6.12



รูปที่ 6.12 หน้าจอข้อมูลคะแนนผลกระทบด้านความลับ

6.5.6 ข้อมูลคะแนนผลกระทบด้านบูรณภาพ

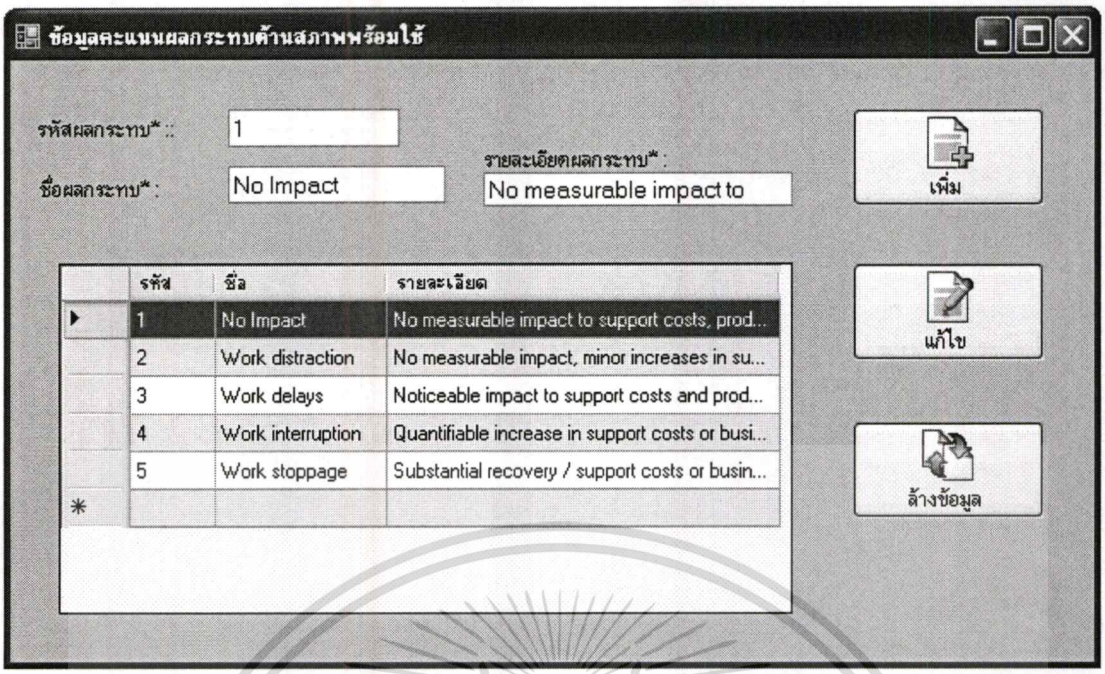
ระดับผลกระทบในมุมมองความปลอดภัยในระบบสารสนเทศในด้านบูรณภาพ ระดับผลกระทบมี 5 ระดับ เรียงตามระดับผลกระทบจากน้อยมากไปถึงระดับมากที่สุด 1-5 ดังรูปที่ 6.13



รูปที่ 6.13 หน้าจอข้อมูลคะแนนผลกระทบด้านบูรณภาพ

6.5.7 ข้อมูลคะแนนผลกระทบด้านสภาพพร้อมใช้

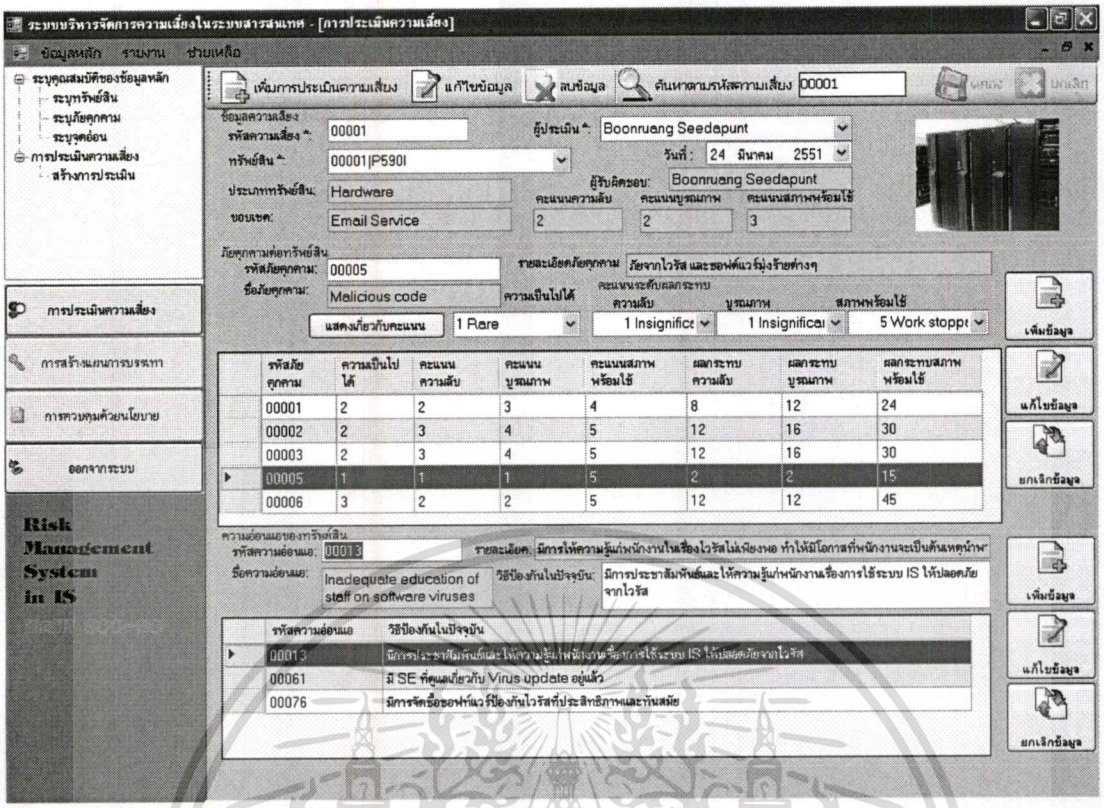
ระดับผลกระทบในมุมมองความปลอดภัยในระบบสารสนเทศในด้านสภาพพร้อมใช้ ระดับผลกระทบมี 5 ระดับ เรียงตามระดับผลกระทบจากน้อยมากไปถึงระดับมากที่สุด 1-5 ดังรูปที่ 6.14



รูปที่ 6.14 หน้าจอข้อมูลคะแนนผลกระทบด้านสภาพพร้อมใช้

6.6 การประเมินความเสี่ยง

การประเมินความเสี่ยงผู้ประเมินความเสี่ยงเลือกเพิ่มรายการประเมินความเสี่ยงเพื่อสร้างการประเมินความเสี่ยงใหม่ ขั้นตอนแรกเลือกทรัพย์สินเพื่อประเมินความเสี่ยง ตอบตกลงเพื่อเข้าสู่รายการประเมินภัยคุกคามที่มีต่อทรัพย์สินเพื่อแสดงผลกระทบ โดยให้คะแนนความเป็นไปได้ที่ภัยคุกคามนั้นจะเกิดขึ้น ซึ่งมีอยู่ 5 ระดับดังได้กล่าวในหัวข้อ 6.5.4 จากนั้นให้คะแนนน้ำหนักในมุมมองด้านความปลอดภัยทั้ง 3 ด้าน ประกอบด้วยคะแนนด้านความลับ ด้านบูรณภาพ และด้านสภาพพร้อมใช้ หลังจากนั้น โปรแกรมจะคำนวณออกมาเป็นคะแนนผลกระทบ และผู้ประเมินความเสี่ยงต้องแสดงรายการจุดอ่อนของทรัพย์สินออกมาดังรูปที่ 6.10 เพื่อนำรายการจุดอ่อนไปสร้างแผนบรรเทาและควบคุมในขั้นตอนต่อไป

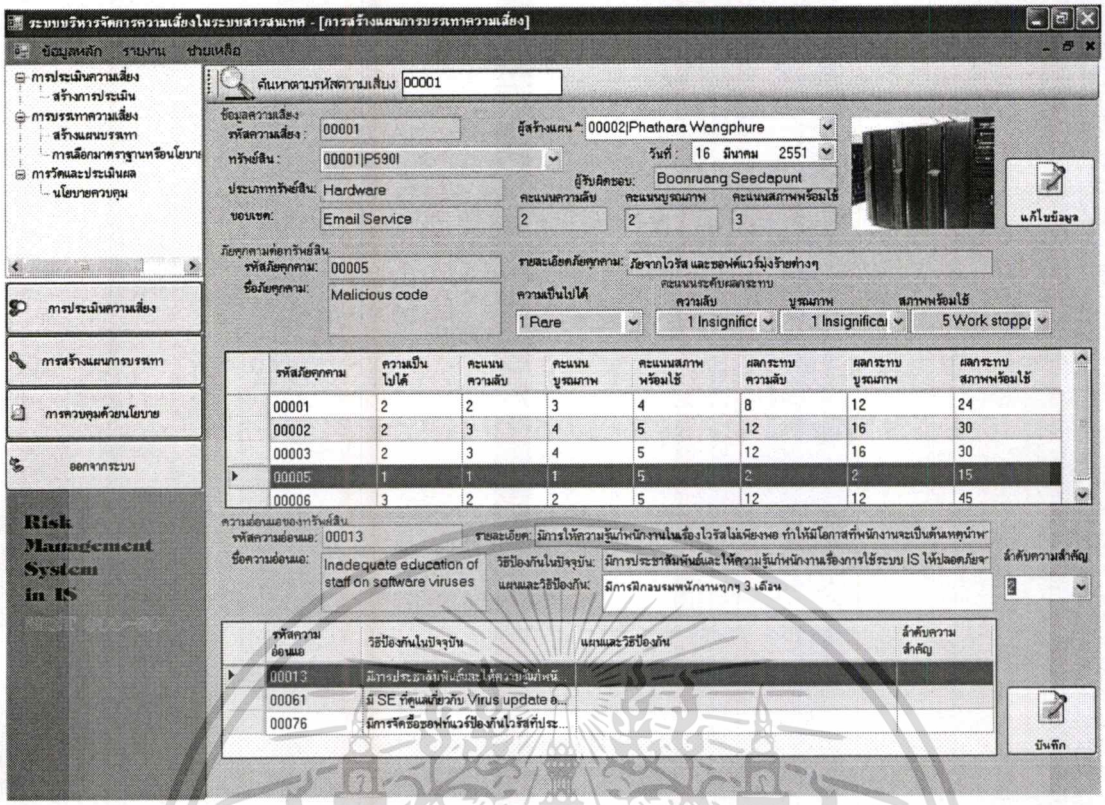


รูปที่ 6.15 หน้าจอการประเมินความเสี่ยง

6.7 การบรรเทาความเสี่ยง

6.7.1 การสร้างแผนบรรเทาความเสี่ยง

ผู้จัดการความเสี่ยงเลือกค้นหารหัสความเสี่ยงเพื่อสร้างแผนบรรเทาความเสี่ยง โดยพิมพ์รหัสความเสี่ยงแล้วกดปุ่มตกลง ในหน้าจอการสร้างแผนบรรเทาความเสี่ยงจะแสดงระผลกระทบที่เกิดจากภัยคุกคามเรียงจากมากที่สุดไปถึงระดับปานกลาง โดยระดับผลกระทบจากภัยคุกคามที่ต่ำกว่าระดับปานกลางจะไม่แสดง โดยถือว่าความเสี่ยงอยู่ระดับที่ต่ำเป็นเกณฑ์ที่ยอมรับได้และไม่ถูกนำมาแสดงเพื่อสร้างแผนบรรเทาและการควบคุมความความเสี่ยง ดังรูปที่ 6.16 โดยแผนบรรเทาจะถูกเลือกออกมาในขั้นตอนนี้ และกำหนดระดับความสำคัญหรือเร่งด่วนเพื่อนำไปใช้ ซึ่งระดับความเร่งด่วนมี 4 ระดับ เรียงจาก 1-4 ตามความเร่งด่วนจากมากที่สุดไปถึงน้อยที่สุด



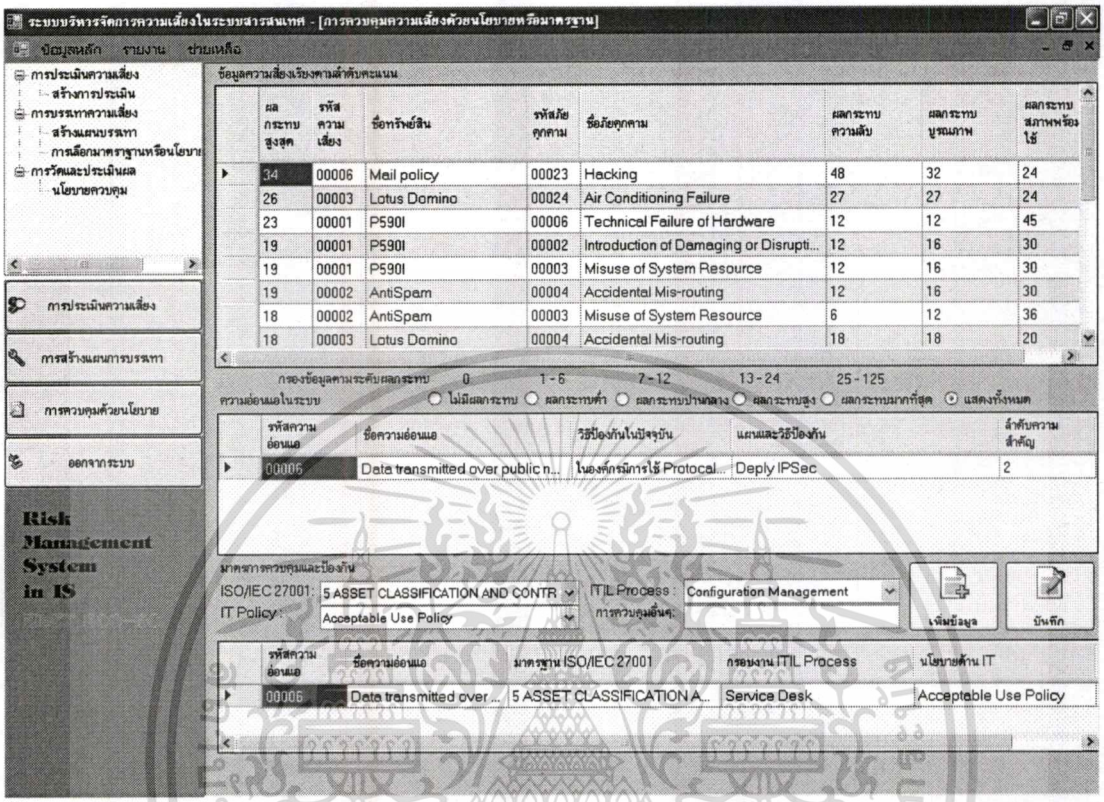
รูปที่ 6.16 หน้าจอการสร้างแผนบรรเทาความเสี่ยง

6.7.2 การเลือกมาตราฐานหรือนโยบายเพื่อควบคุมความเสี่ยง

การเลือกมาตราฐานหรือนโยบายเพื่อควบคุมความเสี่ยงเป็นขั้นตอนสุดท้ายของการบรรเทาความเสี่ยงและเป็นขั้นตอนสุดท้ายของการบริหารจัดการความเสี่ยงในระบบสารสนเทศ ผลลัพธ์ที่ได้มาจากขั้นตอนการประเมินความเสี่ยงจะถูกนำมาสร้างแผนเพื่อป้องกันและบรรเทาความเสี่ยง โดยเลือกมาตราฐานเป็นกรอบในการจัดการความเสี่ยง และมีนโยบายขึ้นเพื่อควบคุมเสี่ยง เพื่อให้มีขั้นตอนหรือเอกสารที่เป็นมาตราฐานอ้างอิงโดย สามารถทบทวนและตรวจสอบได้ ทั้งนี้กระบวนการตามมาตราฐาน หรือข้อกำหนดต่างๆ จะอยู่นอกเหนือขอบเขตของโครงการพัฒนาระบบนี้ ผู้เขียนจึงไม่ขอกล่าวในรายละเอียด เพียงแต่สิ่งที่อยากนำมาแสดงให้เห็นคือนอกเหนือจากขั้นตอนการประเมินความเสี่ยงแล้วนั้นเรายังต้องมีกระบวนการหรือวิธีการมาควบคุมความเสี่ยงตามมาตราฐาน โดยมีวิธีการควบคุมทางด้านเทคนิคที่ครบถ้วน มีวิธีการทางด้านนโยบายจากระดับบริหารที่ชัดเจน และมีการควบคุมสอดคล้องกับมาตราฐานเป็นที่ยอมรับในระดับสากล ซึ่งเป็นการสร้างความเชื่อมั่นว่าเมื่อมีเหตุการณ์ที่ได้คาดไว้แล้วเกิดขึ้นองค์กรก็มีแผนการรองรับและพร้อมรับมือ

มาตราฐานที่ถูกนำมาอ้างคือ มาตราฐานด้านความปลอดภัยในระบบสารสนเทศ ISO/IEC 17799:2000 กระบวนด้านการบริหารจัดการบริการในระบบสารสนเทศ ITIL และเอกสาร

นโยบายในระบบสารสนเทศในองค์กร IT Policy ที่อิงตามระบบจัดการความปลอดภัย ISMS ดังรูปที่ 6.17



รูปที่ 6.17 หน้าจอการเลือกมาตราฐานหรือนโยบายเพื่อควบคุมความเสี่ยง

บทที่ 7
บทสรุป

7.1 ผลการพัฒนาระบบ

การพัฒนาระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ ได้ทำการวิเคราะห์และออกแบบระบบ โดยนำเสนอในรูปไดอะแกรมเชิงวัตถุต่างๆ ซึ่งมีผลต่อการพัฒนาที่สามารถทำได้ง่ายมากขึ้น โดยการพัฒนาระบบมุ่งหวังให้ผู้ใช้งานสามารถใช้งานได้ง่ายขึ้นและสารสนเทศที่ได้สามารถนำมาวิเคราะห์และนำไปใช้ในการประมาณการได้

ระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ โดยวัตถุประสงค์ของการพัฒนาระบบมีดังต่อไปนี้

1. เพื่อใช้ในการรวบรวมข้อมูลทรัพย์สินในระบบสารสนเทศภายขอบเขตที่ได้กำหนดไว้เพื่อเป็นเป้าหมายในการสร้างระบบความปลอดภัย
2. เพื่อช่วยในการวิเคราะห์ความเสี่ยงภายในระบบสารสนเทศ
3. เพื่อช่วยลดขั้นตอนและความซ้ำซ้อนในการปฏิบัติงานได้
4. เพื่อให้มีระบบการบริหารจัดการความเสี่ยงที่สามารถนำผลการวิเคราะห์ที่ได้มาใช้ได้อย่างมีประสิทธิภาพ
5. เพื่อนำเสนอผลการวิเคราะห์อยู่ในรูปกราฟแบบต่างๆเพื่อให้ผู้บริหารสามารถเห็นและเข้าใจถึงความเสี่ยงที่เกิดขึ้นภายในระบบสารสนเทศ

7.2 ประโยชน์ที่ได้รับ

ประโยชน์ที่ได้รับจากการพัฒนาระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศ

1. ความรู้และทักษะในด้านของการวิเคราะห์ ออกแบบ และการพัฒนาระบบ
2. ได้เรียนรู้ภาษาและเครื่องมือในการพัฒนาระบบ
3. ได้ระบบบริหารจัดการความเสี่ยงในระบบสารสนเทศเพื่อทดแทนไฟล์สเปรดชีทแบบเดิม

7.3 ข้อเสนอแนะและแนวทางการพัฒนาในอนาคต

การพัฒนาระบบเพิ่มเติมต่อไปในอนาคต อาจจะเพิ่มเติมในส่วนหัวข้อการบริหารจัดการความเสี่ยงในทรัพย์สินแต่ละประเภทว่าได้สอดคล้องกับข้อกำหนดข้อไหนของมาตรฐานอะไรเพื่อให้เห็นถึงข้อกำหนดของมาตรฐาน และส่วนของรายงานที่อาจจะยังไม่สมบูรณ์ดังนี้

1. เพิ่มส่วนอ้างอิงในแผนการบรรเทาหรือป้องกันความเสี่ยงแก่ทรัพย์สิน พร้อมทั้งระบุไปยังเอกสารข้อกำหนดหรือนโยบายข้อใด
2. พัฒนารายงานสำหรับผู้ใช้งานให้ตรงความต้องการของผู้ใช้งานกลุ่มต่างๆ ให้สมบูรณ์มากขึ้น
3. พัฒนาเป็นระบบเว็บแอฟปลิเคชัน เพื่อให้ผู้ใช้สามารถใช้ผ่านระบบได้สะดวกมากขึ้น

บรรณานุกรม

ปริญญา หอมเอนก. 2006. **Information Technology Risk Management using International Standard Methodologies and Framework.** [Online]. Available: http://www.acisonline.net/article_prinya_eweek_150449.htm

ศุภชัย สมพานิช. 2549. **Database Programming ด้วย VB2005 & VC#2005 ฉบับสมบูรณ์.** กรุงเทพ : DEV Book

ศุภชัย สมพานิช. 2550. **พัฒนาระบบฐานข้อมูลด้วย VB2005 & VC#2005 ฉบับมืออาชีพ.** กรุงเทพ : DEV Book

British Standard BS7799-2. 2002. **Information security management system –Specification with guidance for use.** [Online].Available:http://www.bsi-global.com

NIST sp800-30. 2001.**Risk management Guide for Information Technology Systems.** [Online].Available:http://csrc.nist.gov/publications/nistpubs/

OCTAVE. 2003.**An introduction to OCTAVE Method.** [Online].Available: http://www.cert.org/octave/methodintro.html

ประวัติผู้เขียน

ชื่อผู้เขียน	นายบุญเรือง สีดาพันธ์
วันเกิด	24 สิงหาคม 2519
สถานที่เกิด	ร้อยเอ็ด
วุฒิการศึกษาระดับปริญญาตรี	วท.บ. (วิทยาศาสตร์สถิติ) คณะวิทยาศาสตร์ มหาวิทยาลัยมหาสารคาม
ปีที่สำเร็จการศึกษา	ปีการศึกษา 2542
การทำงานปัจจุบัน	วิศวกรระบบ บริษัท สามารถ คอร์ปอเรชั่น จำกัด มหาชน