การพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

The Development of Information Security Risk Analysis System

โดย

นายกชพงศ์ เพ็ชรราช

รหัส 45061522

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2547

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

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

บทคัดย่อ

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

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

Abstract

Recentry ,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

สารบัญ (ต่อ)

หน้า

สารบัญรูป

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

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 ข้อมูลในส่วนของคำถามได้อย่างสะดวกรวดเร็ว
8. เพื่อช่วยเก็บข้อมูลของโครงการ ข้อมูลส่วนตัวของนักวิเคราะห์ แบบสอบถาม ผลการวิเคราะห์ความเสี่ยง
9. เพื่อช่วยให้นักวิเคราะห์ความเสี่ยงสามารถพิมพ์รายงานผลการวิเคราะห์ความเสี่ยงได้ เพื่อนำมาใช้ประกอบในการวิเคราะห์ความเสี่ยงต่อไป

1.2 วิธีการในการพัฒนาระบบ

โครงการนี้เป็นการพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศโดยมีการศึกษาแนวคิดและวิธีการวิเคราะห์และประเมินความเสี่ยงหลายๆแนวคิดมาใช้เป็นแนวทางในการพัฒนาระบบ

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

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศใช้ UML ช่วยในการออกแบบ ซึ่งมีการใช้โมเดลต่างๆมาช่วยอธิบายระบบงานนั้นๆ ทำให้สามารถแสดงภาพรวมของระบบทั้งหมดได้อย่างชัดเจน และช่วยทำให้นักวิเคราะห์ระบบ นักพัฒนาและผู้ใช้ มีมุมมองที่เข้าใจตรงกัน ทำให้การพัฒนาระบบเป็นไปอย่างรวดเร็ว

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 แต่ความปลอดภัยของสารสนเทศจะเป็นการพิจารณาว่าอะไรที่จำเป็นต้องมีการปกป้อง ทำไมจึงต้องปกป้อง ปกป้องจากอะไรและจะปกป้องสิ่งนั้นอย่างไรตลอดระยะเวลาที่สิ่งนั้นยังคงอยู่

ความปลอดภัยของสารสนเทศต้องทำเป็นระบบและทำอย่างต่อเนื่องไม่มีวันจบ ระบบของเราอาจมีความปลอดภัยที่ดีในวันนี้ อีกเดือนหนึ่งหรืออีกสัปดาห์หนึ่งข้างหน้า ระบบอาจถูกบุกรุกได้ เหตุผลก็คือ ช่องโหว่ของระบบใหม่ๆ เกิดขึ้นแทบทุกวัน สังเกตได้จาก NOS ในตระกูลวินโดว์ของไมโครซอฟต์นั้น 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 หากยังไม่ปลอดภัยจะต้องทำอย่างไรบ้าง จะต้องใช้ผลิตภัณฑ์ด้านความปลอดภัยอะไร มีขั้นตอนในการดำเนินการอย่างไร ซึ่งไม่มีคำตอบมาตรฐานสำหรับคำถามข้างต้น และไม่มีคำตอบเดียวที่

สามารถใช้กับทุกสถานการณ์ได้ แต่เราสามารถประเมินความเสี่ยงและจัดการความเสี่ยงเพื่อให้ระบบมีความเสี่ยงลดลงได้ นั่นคือเพิ่มความปลอดภัยของระบบให้สูงขึ้น

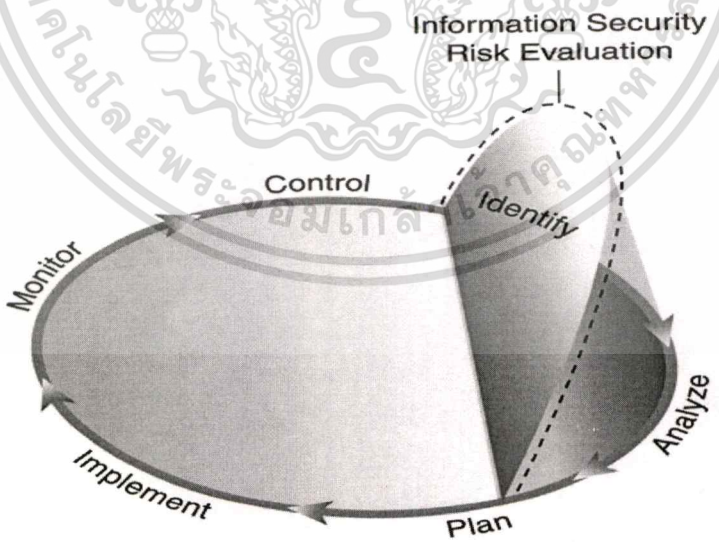
ก่อนที่เราจะสามารถดำเนินการจัดการเพื่อลดความเสี่ยงได้จะต้องมีการประเมินความเสี่ยงก่อน ซึ่งการประเมินความเสี่ยง มีขั้นตอนโดยสรุปคือ

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

หลังจากการประเมินความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อไปที่ต้องทำมีดังนี้

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

ขั้นตอนที่กล่าวมาทั้งหมดเป็นการจัดการความเสี่ยง ซึ่งประกอบด้วยขั้นตอนในการประเมินความเสี่ยงรวมกับขั้นตอนในการนำแผนกลยุทธ์ในการป้องกันมาใช้ นั่นคือ การประเมินความเสี่ยงเป็นส่วนหนึ่งในการจัดการความเสี่ยงนั่นเอง ความสัมพันธ์ระหว่างการประเมินความเสี่ยงและการจัดการความเสี่ยง แสดงในรูปที่ 2.1



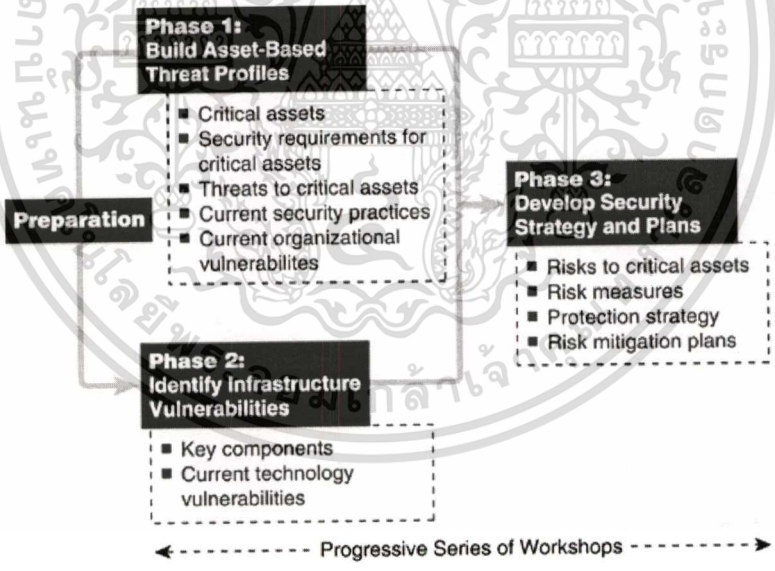
รูปที่ 2.1 ความสัมพันธ์ระหว่างการประเมินความเสี่ยงและการจัดการความเสี่ยง

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

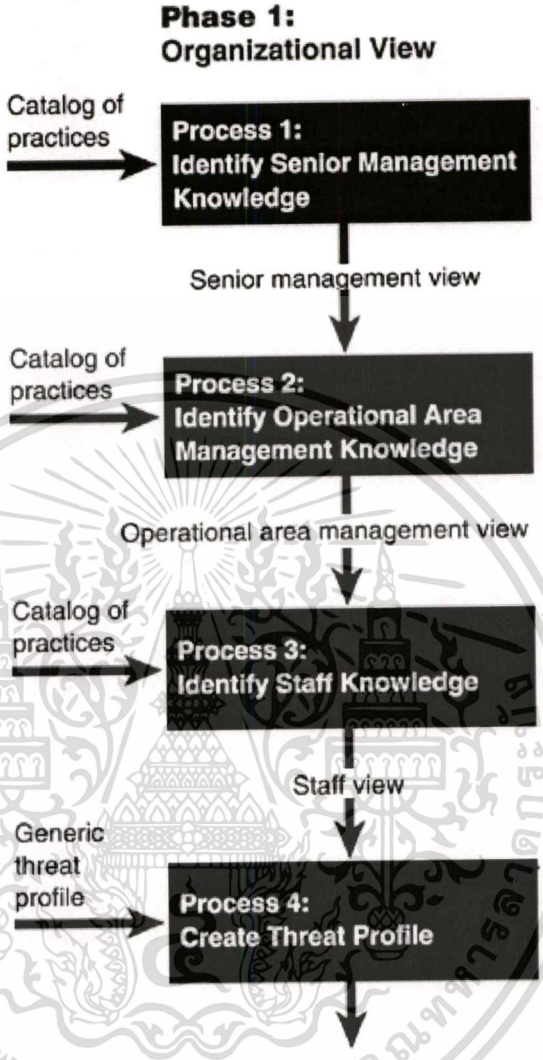
ภาพรวมวิธีการของ OCTAVE แสดงในรูปที่ 2.2



รูปที่ 2.2 วิธีการของ OCTAVE

2.2.1 ขั้นตอนที่ 1 : สร้างโครงร่างของภัยคุกคามต่อทรัพย์สิน

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



รูปที่ 2.3 ขั้นตอนที่ 1 สร้างโครงร่างของภัยคุกคามต่อทรัพย์สิน

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

- ระบุขอบเขตของภัยคุกคามที่เกี่ยวข้อง
- ระบุความต้องการความปลอดภัยสำหรับทรัพย์สินที่สำคัญ
- รวบรวมข้อมูลที่ได้จากการสำรวจเกี่ยวกับความปลอดภัยและช่องโหว่ขององค์กร

กระบวนการที่ 4 : สร้างโครงร่างของภัยคุกคาม

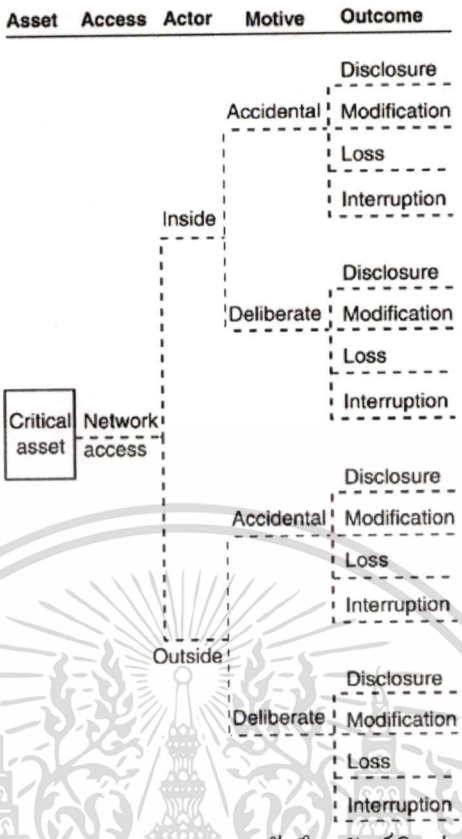
ทีมนักวิเคราะห์ (Analysis team) จะรวบรวมข้อมูลที่ได้จากกระบวนการที่ 1 ถึง 3 มาวิเคราะห์เพื่อหาทรัพย์สินที่สำคัญและมีความเสี่ยง (critical assets) และสร้างโครงร่างของภัยคุกคาม โดยทีมนักวิเคราะห์ควรมีทักษะและคุณสมบัติต่อไปนี้

- เข้าใจลักษณะและระบบธุรกิจขององค์กร
- เข้าใจเทคโนโลยีสารสนเทศขององค์กร
- มีทักษะในการติดต่อสื่อสาร
- มีทักษะในการวิเคราะห์

โครงร่างของภัยคุกคามเป็นโครงสร้างที่ใช้แสดงขอบเขตของภัยคุกคามที่มีต่อทรัพย์สินที่สำคัญ โดยจะแสดงในลักษณะโครงสร้างต้นไม้ ซึ่งวิธีการของ OCTAVE ภัยคุกคามจะถูกแสดงในโครงร่างโดยใช้คุณสมบัติต่อไปนี้

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

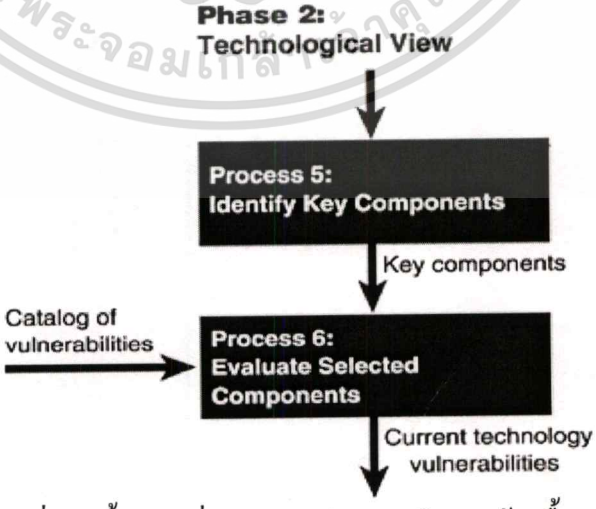
ภัยคุกคามที่เกิดขึ้นมีหลายรูปแบบ เช่น การเข้าถึงทรัพย์สินผ่านเครือข่าย การเข้าถึงทรัพย์สินทางกายภาพ ปัญหาหรือข้อผิดพลาดของระบบทั้งซอฟแวร์หรือฮาร์ดแวร์ ภัยธรรมชาติต่างๆ รวมไปถึงอุบัติเหตุที่อาจเกิดขึ้นในองค์กร เป็นต้น จากภัยคุกคามที่ได้กล่าวมา สามารถนำมาสร้างโครงร่างของภัยคุกคามได้ ดังรูปที่ 2.4



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

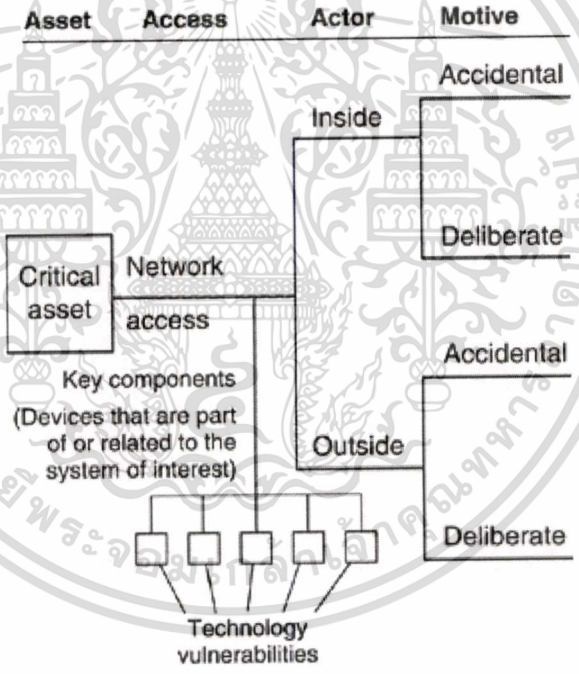


รูปที่ 2.5 ขั้นตอนที่ 2 ระบุจุดอ่อนของโครงสร้างพื้นฐาน

กระบวนการที่ 5 : ระบุส่วนประกอบที่สำคัญ

ผู้ที่เกี่ยวข้องในกระบวนการนี้คือทีมนักวิเคราะห์และพนักงานเทคโนโลยีสารสนเทศที่ได้เลือกไว้ จุดประสงค์ของกระบวนการที่ 5 คือ เลือกส่วนประกอบของโครงสร้างพื้นฐานเพื่อนำมาทดสอบหาจุดบกพร่องต่อไปในกระบวนการที่ 6

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



รูปที่ 2.6 ความสัมพันธ์ระหว่างโครงร่างของภัยคุกคามและส่วนประกอบของโครงสร้างพื้นฐาน

กระบวนการที่ 6 : การประเมินส่วนประกอบที่ถูกเลือก

ในกระบวนการที่ 6 เป็นการนำส่วนประกอบของโครงสร้างพื้นฐานที่ผ่านการคัดเลือกและพิจารณาจากกระบวนการที่ 5 แล้วมาทำการทดสอบหาจุดบกพร่องโดยในการทดสอบจุดบกพร่องของระบบในแต่ละส่วนประกอบอาจใช้เครื่องมือทดสอบที่ต่างกันตามความเหมาะสมซึ่งทีมนักวิเคราะห์จะเป็นผู้เลือกเครื่องมือและวิธีการทดสอบ ผลที่ได้จากการทดสอบเบื้องต้นแสดงในตารางที่ 2.1

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 จุดบกพร่องที่ถูกตรวจพบมีความเสี่ยงและผลกระทบสูง ต้องมีการแก้ไขทันที (ภายใน 24 ชั่วโมง) ระดับกลาง ต้องแก้ไขภายใน 1 เดือน และระดับต่ำ อาจทำการแก้ไขในภายหลังได้

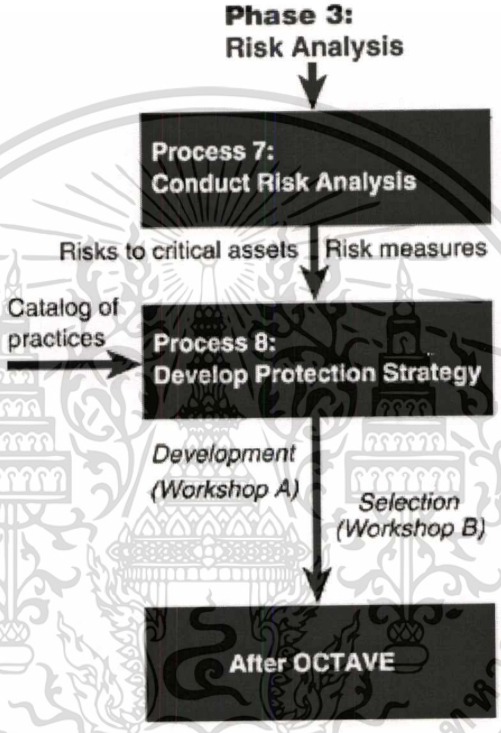
ตารางที่ 2.2 ระดับของจุดบกพร่อง

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 ซึ่งเป็นการนำข้อมูลที่ผ่านการวิเคราะห์และประเมินในขั้นตอนที่ 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 ซึ่งเป็นการแบ่งอย่างง่ายๆ แต่ทีมนักวิเคราะห์อาจกำหนดระดับของภัยคุกคามที่แตกต่างไปจากนี้ได้ตามความเหมาะสม

การวิเคราะห์ผลกระทบของภัยคุกคามที่มีต่อทรัพย์สินทำให้สามารถบอกได้ว่าภัยคุกคามอะไรมีผลกระทบมากน้อยเท่าใด แต่ภัยคุกคามแต่ละอย่างมีโอกาสเกิดขึ้นไม่เท่ากันเช่น ภัยคุกคามที่มีผลกระทบทำให้ระบบเสียหายอย่างมากแต่มีโอกาสเกิดน้อยมากๆ เป็นต้น ทำให้เราไม่สามารถสรุปได้ว่า ภัยคุกคามที่มีผลกระทบสูงมากจะมีความเสี่ยงสูงมากเสมอไป

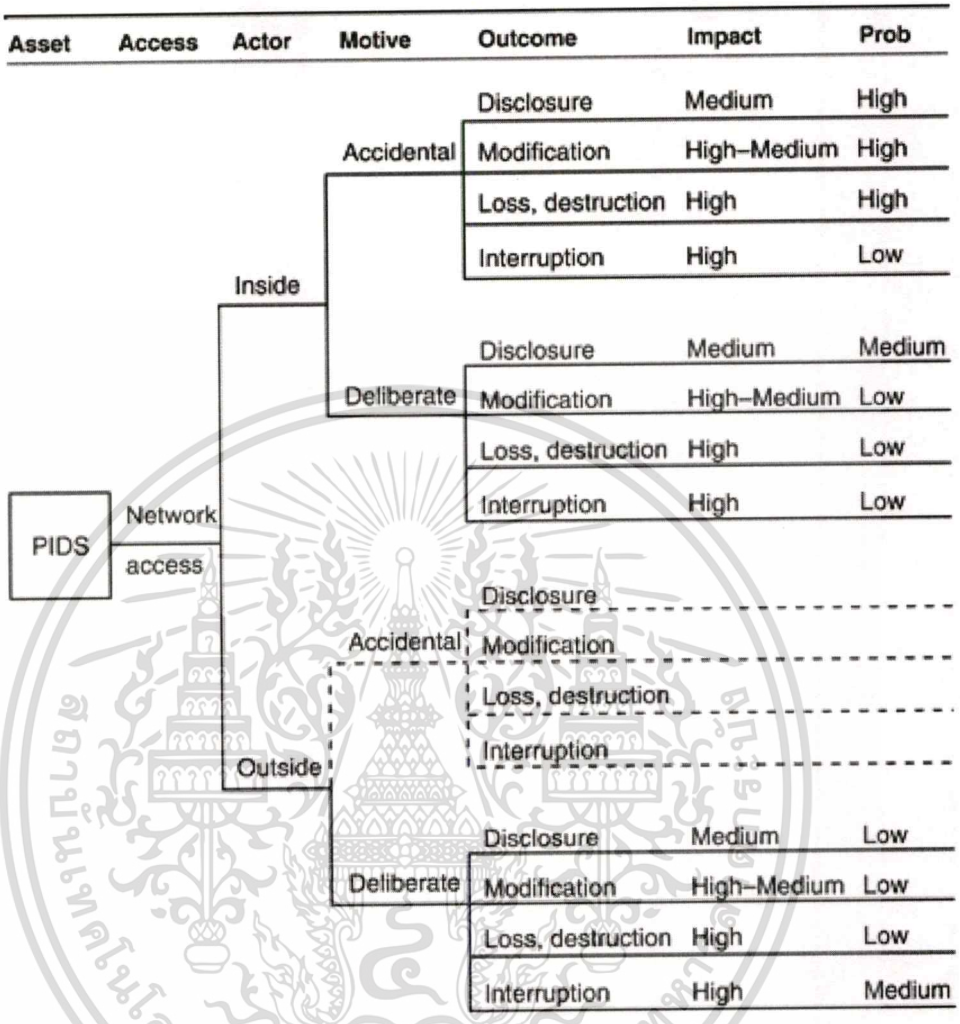
ความน่าจะเป็นของภัยคุกคามที่จะเกิดขึ้นเป็นปัจจัยสำคัญที่ต้องนำมาใช้ร่วมกับผลกระทบของภัยคุกคามในการวิเคราะห์และประเมินความเสี่ยง โดยความน่าจะเป็นของภัยคุกคาม คือ โอกาสของภัยคุกคามที่จะเกิดขึ้นซึ่งพิจารณาจากความถี่ของภัยคุกคามที่เกิดขึ้นในช่วงระยะเวลาหนึ่ง ทีมนักวิเคราะห์จะทำหน้าที่กำหนดมาตรฐานสำหรับใช้ในการประเมินความน่าจะเป็นของภัยคุกคามขึ้นมา ตัวอย่างของการการการประเมินความน่าจะเป็นของภัยคุกคามที่จะเกิดขึ้นสำหรับองค์กรแสดงในตารางที่ 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 มาแสดงในโครงร่างภัยคุกคามจากการเข้าถึงทรัพย์สินผ่านเครือข่ายได้

โครงร่างภัยคุกคามแสดงให้เห็นว่าผลลัพธ์ที่เกิดขึ้นจากภัยคุกคามของการเข้าถึงทรัพย์สินผ่านเครือข่ายจะมีผลกระทบและความเป็นไปได้ในระดับใดบ้าง เช่น ภัยคุกคามจากภายในเครือข่ายโดยไม่เจตนาซึ่งส่งผลให้เกิดความเสียหายกับข้อมูลจะมีผลกระทบสูงและมีความน่าจะเป็นสูง ส่วนภัยคุกคามจากภายในเครือข่ายโดยไม่เจตนาซึ่งส่งผลให้เกิดการขัดจังหวะหรือขัดขวางการทำงานของระบบจะมีผลกระทบสูงแต่มีความน่าจะเป็นต่ำ เป็นต้น



รูปที่ 2.8 โครงร่างภัยคุกคามการเข้าถึงทรัพย์สินผ่านเครือข่าย

กระบวนการที่ 8 : พัฒนากลยุทธ์การป้องกัน

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

กระบวนการที่ 8A

ในกระบวนการที่ 8A จะเป็นการสร้างกลยุทธ์ในการป้องกัน โดยก่อนเริ่มกระบวนการนี้จะต้องทำการรวบรวมข้อมูลและสารสนเทศที่ได้มาจากกระบวนการที่ 1 ถึง 3 มาพิจารณาใหม่อีกครั้ง แล้วทำการสร้างกลยุทธ์ในการป้องกันขึ้นมา จากนั้นการวางแผนเพื่อลดความเสียหายที่เกิดขึ้น

OCTAVE มีการประเมินหาค่าความเสี่ยงโดยใช้ความน่าจะเป็นและผลกระทบมาจับคู่กันในลักษณะเมทริกซ์ซึ่งจะได้ค่าความเสี่ยงออกมาเป็น 3 ระดับ วิธีการนี้เป็นการประเมินแบบเชิง

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 มีกิจกรรมหลักๆที่สำคัญดังนี้

- การเตรียมการก่อนเข้าพบผู้บริหาร

ทำการสร้างรายงานสรุปการทำงานโดยแบ่งเป็น 2 ส่วน โดยส่วนแรกเป็นรายงานสรุปสารสนเทศเกี่ยวกับความเสี่ยงที่ได้รวบรวมระหว่างการประเมิน และส่วนที่ 2 เป็นรายงานสรุปผลลัพธ์ที่สำคัญของการประเมิน รวมถึงแผนกลยุทธ์ในการป้องกันและแผนการลดความเสี่ยง

- นำเสนอสารสนเทศเกี่ยวกับความเสี่ยง

สารสนเทศเกี่ยวกับความเสี่ยงที่เกิดขึ้นระหว่างกระบวนการของ OCTAVE ที่สำคัญที่จะนำเสนอ คือ ช่องโหว่หรือข้อบกพร่องของระบบในปัจจุบัน สารสนเทศเกี่ยวกับทรัพย์สินที่สำคัญและโครงร่างของความเสี่ยงที่มีต่อทรัพย์สินที่สำคัญ

- การทบทวนตรวจสอบ

นำเสนอแผนกลยุทธ์ในการป้องกันและแผนการลดความเสี่ยงให้ผู้บริหารพิจารณาตรวจสอบและอาจมีการแก้ไขหรือทำใหม่ตามความเหมาะสม

- ทำขั้นตอนต่อไป

สุดท้ายผู้บริหารจะเป็นคนตัดสินใจว่าจะนำแผนกลยุทธ์ในการป้องกันและแผนการลดความเสี่ยงมาประยุกต์ใช้อย่างไรโดยจะพิจารณาว่าจะทำอะไรเป็นขั้นตอนต่อไปหลังจากการ

ประเมิน ใครจะเป็นผู้รับรับผิดชอบในการทำขั้นตอนต่อไปและจะทำอย่างไรต่อไปเมื่อขั้นตอนนี้เสร็จสิ้น

2.3 การวิเคราะห์ความเสี่ยงของสารสนเทศโดยใช้แนวคิด CobiT

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

โดเมนหลักของ CobiT

1. การวางแผนและการจัดการองค์กร (Planning and Organization)

โดเมนนี้ครอบคลุมถึงกลยุทธ์และการระบุทิศทางของการนำเทคโนโลยีสารสนเทศมาช่วยในการดำเนินไปยังเป้าหมายธุรกิจขององค์กร รวมถึงการวางแผนกลยุทธ์ การติดต่อสื่อสารกัน การจัดการมุมมองที่แตกต่างกัน และความเหมาะสมของโครงสร้างพื้นฐานของเทคโนโลยีกับองค์กร

2. การจัดหาและติดตั้ง (Acquisition and Implementation)

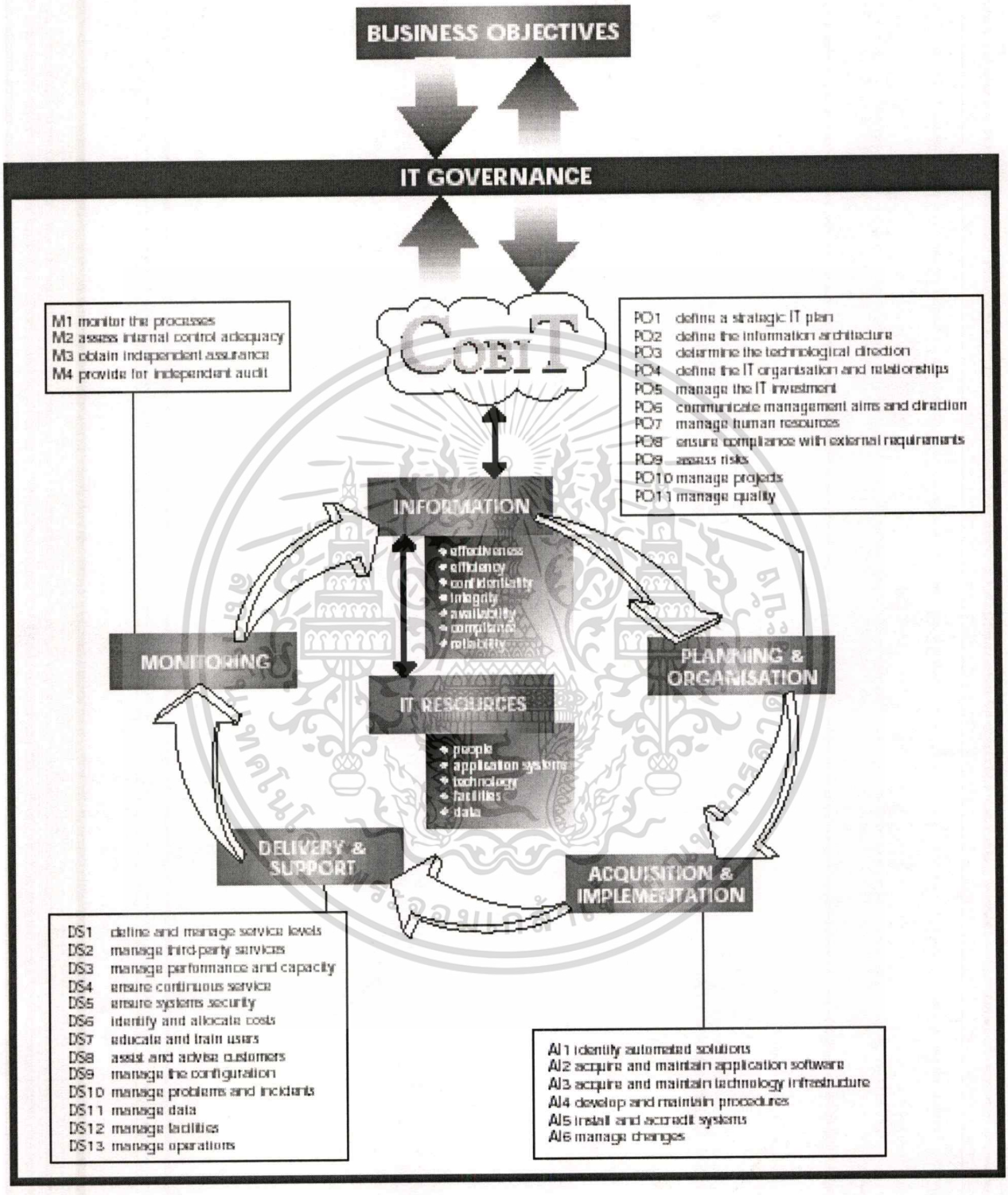
โดเมนนี้เกี่ยวกับการทำตามกลยุทธ์ที่กำหนดไว้ เป็นการนำเทคโนโลยีสารสนเทสมาติดตั้งและประยุกต์ใช้ร่วมกับกระบวนการทางธุรกิจขององค์กร รวมถึงการเปลี่ยนแปลงและการบำรุงรักษาระบบที่มีอยู่

3. การส่งมอบและบำรุงรักษา (Delivery and Support)

โดเมนนี้เกี่ยวกับการให้บริการซึ่งอยู่ในขอบเขตของความปลอดภัยและความต่อเนื่อง รวมถึงส่วนของการประมวลผลข้อมูลโดยระบบงาน

4. การติดตามผล (Monitoring)

กระบวนการทางเทคโนโลยีสารสนเทศทั้งหมดจะต้องมีการประเมินเกี่ยวกับคุณภาพและการปฏิบัติตามข้อบังคับ โดเมนนี้จะต้องแก้ไขการจัดการที่ผิดพลาดของกระบวนการควบคุมขององค์กร อาจมีการตรวจสอบจากผู้ตรวจสอบภายในองค์กรเองหรือจากบุคคลภายนอก



รูปที่ 2.9 กระบวนการทางเทคโนโลยีสารสนเทศของ CobiT ถูกกำหนดไว้ภายใต้ 4 โดเมน

จากรูปที่ 2.9 แสดงให้เห็นภาพรวมของกระบวนการดำเนินงานทางเทคโนโลยีสารสนเทศในองค์กร ซึ่งในการวิเคราะห์ความเสี่ยงตามแนวคิดของ CobiT จะมีองค์ประกอบที่สำคัญ คือ

โดเมนหลักทั้ง 4 โดเมน คุณภาพหรือมาตรฐานของระบบสารสนเทศ 7 ประการ และทรัพยากรด้านเทคโนโลยีสารสนเทศ 5 ประเภท ซึ่งมีรายละเอียดดังนี้

คุณภาพของระบบสารสนเทศ 7 ประการ (Information Criteria)

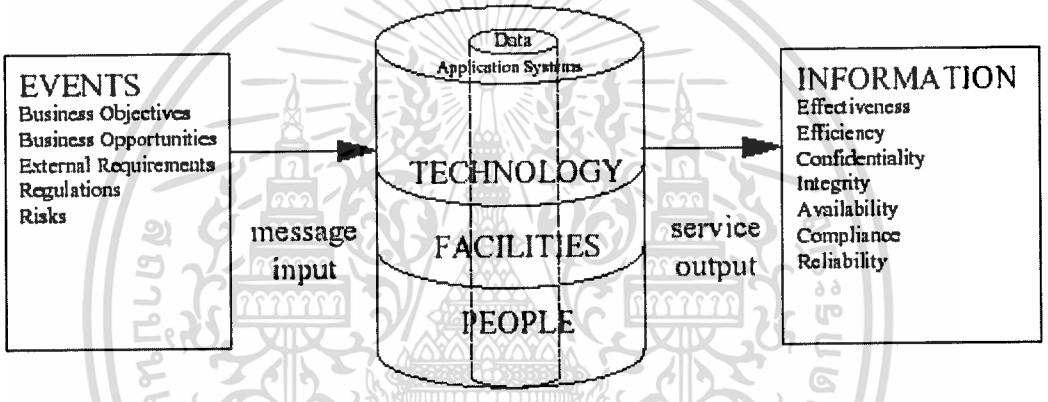
- ประสิทธิภาพ (Effectiveness) หมายถึงข้อมูลที่ใช้เกี่ยวข้องกับกระบวนการทางธุรกิจ รวมทั้งมีการส่งมอบข้อมูลแก่ผู้ใช้อย่าง ถูกต้อง ตรงเวลา สม่ำเสมอ และใช้ประโยชน์ได้
- ประสิทธิผล (Efficiency) หมายถึง มีการใช้ประโยชน์จากทรัพยากรอย่างเต็มที่เพื่อให้ได้มาซึ่งข้อมูลสารสนเทศ
- ความลับ (Confidentiality) หมายถึง การป้องกันการเปิดเผยข้อมูลที่สำคัญต่อบุคคลหรือหน่วยงานที่ไม่ได้รับอนุญาต
- ความสมบูรณ์และถูกต้อง (Integrity) หมายถึงความครบถ้วนถูกต้องของข้อมูล ตลอดจนเป็นข้อมูลใช้ได้ ในแง่ของความคาดหมายและการให้ความสำคัญของธุรกิจ (business values and expections)
- การมีใช้เมื่อต้องการ (Availability) หมายถึง เป็นข้อมูลที่เรียกใช้ได้เมื่อต้องการและจำเป็นใช้ทั้งในปัจจุบันและอนาคต และรวมทั้งการป้องกันภัยให้กับทรัพยากรต่างๆที่จำเป็นและการรักษาระดับความสามารถในการทำงานของทรัพยากรเหล่านั้น
- การปฏิบัติตามระบบ (Compliance) หมายถึง การที่ข้อมูลได้จัดทำขึ้นตามกฎ ระเบียบ ข้อบังคับ หลักเกณฑ์ ข้อตกลง หรือกฎหมาย ที่มีขึ้นเพื่อบังคับใช้ทั้งจากหน่วยงานภายในและภายนอกองค์กร เช่น ข้อบังคับของตลาดหลักทรัพย์ ประมวลกฎหมายภาษีอากร หลักการบัญชีที่ยอมรับโดยทั่วไป เป็นต้น
- ความน่าเชื่อถือของข้อมูล (Reliability of Information) หมายถึงความสามารถในการจัดหาข้อมูลที่เหมาะสมให้แก่ผู้บริหารของกิจการเพื่อสามารถดำเนินธุรกิจและเพื่อให้สามารถจัดทำรายงานทางการเงินและรายงานที่จำเป็นอื่นๆภายใต้ความรับผิดชอบของผู้บริหาร

ทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resources) 5 ประเภท

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

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

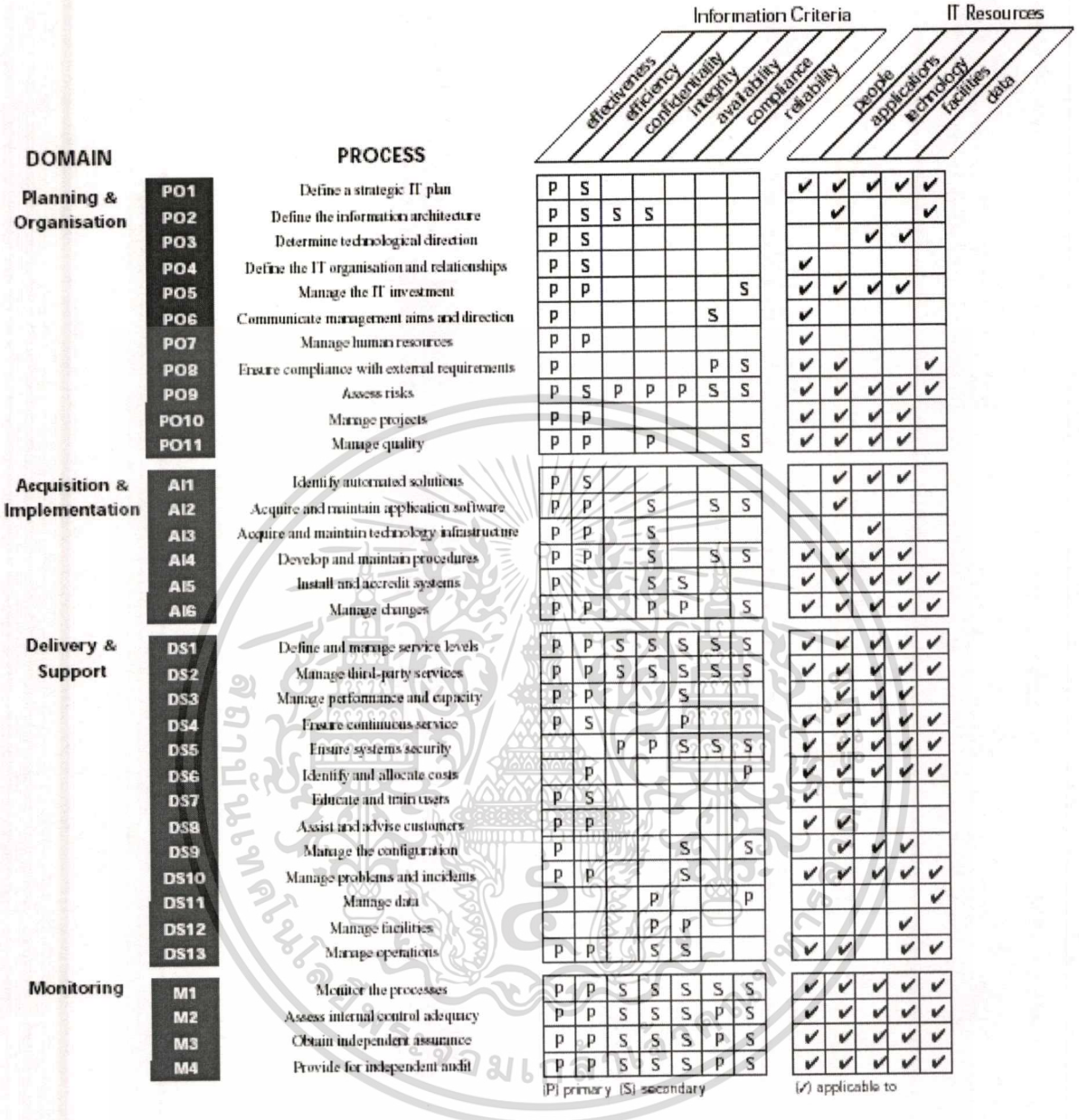
จากมาตรฐานของระบบสารสนเทศ 7 ประการ และทรัพยากรด้านเทคโนโลยีสารสนเทศ 5 ประเภท สามารถนำมาแสดงความสัมพันธ์ในการดำเนินงานของระบบสารสนเทศในองค์กรร่วมกับความต้องการตามกระบวนการธุรกิจขององค์กรได้ดังรูปที่ 2.10



รูปที่ 2.10 โครงสร้างการดำเนินงานของธุรกิจและเทคโนโลยีสารสนเทศ

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

การวิเคราะห์ความเสี่ยงของ CobiT ได้กำหนดโครงสร้างและขอบเขตไว้โดยพิจารณาจากองค์ประกอบที่สำคัญที่ได้กล่าวไปแล้ว ดังรูปที่ 2.11



รูปที่ 2.11 สรุป Control Objectives ของ CobiT

จากรูปที่ 2.11 เป็นการแสดง Control Objective ในแต่ละโดเมนว่าใน 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

บทที่ 3

การวิเคราะห์และออกแบบระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

3.1 ลักษณะและขอบเขตของระบบ

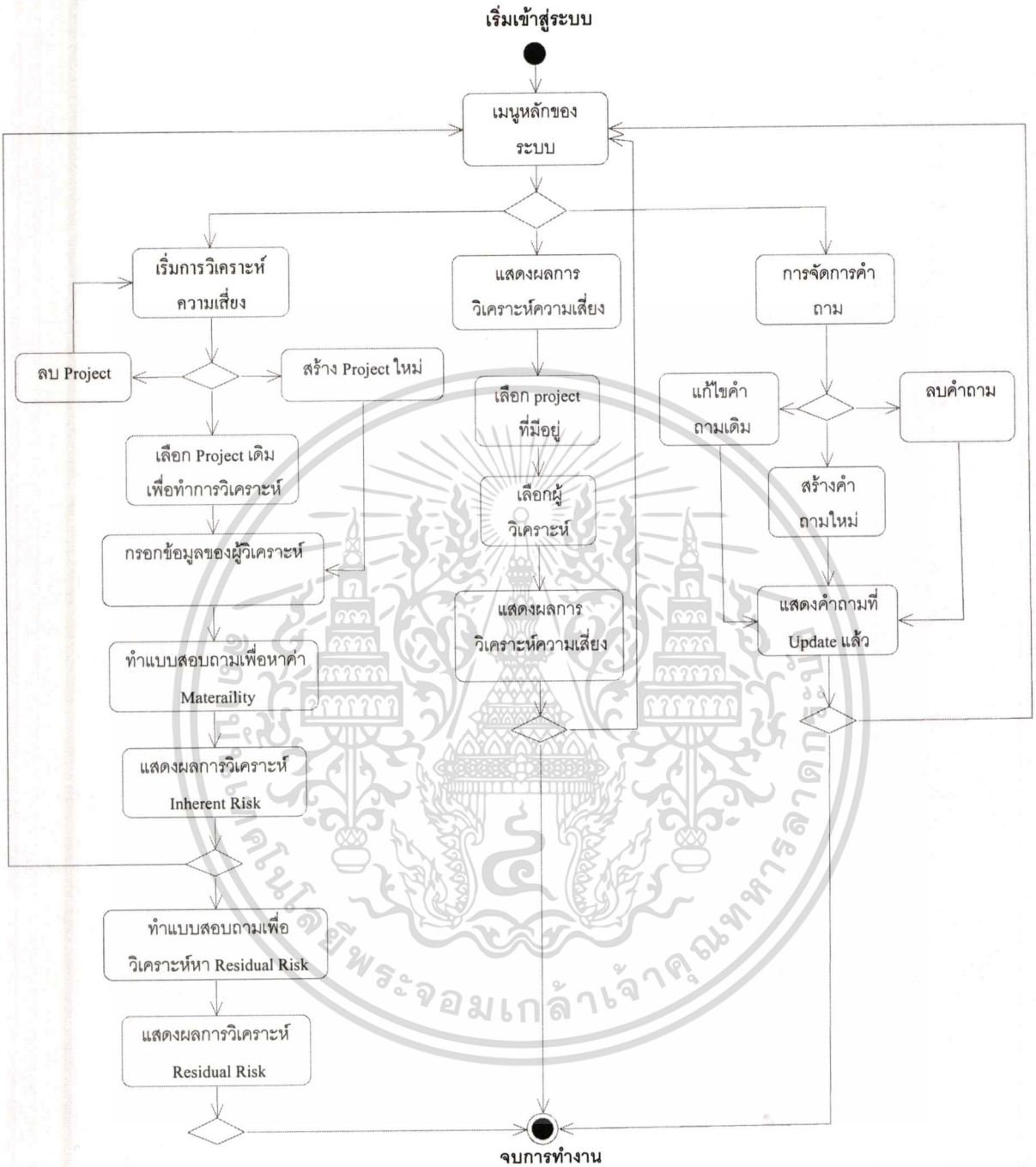
3.1.1 กิจกรรมโดยรวมของระบบ

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ เป็นการนำระบบคอมพิวเตอร์มาช่วยในการวิเคราะห์ความเสี่ยงของสารสนเทศภายในองค์กร ซึ่งกิจกรรมโดยรวมของระบบสามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.1 โดยมีขั้นตอนการทำงานดังต่อไปนี้

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

- กรณีเลือกเข้าไปในส่วน เริ่มการวิเคราะห์ความเสี่ยง จะสามารถเลือกได้ 3 อย่าง คือ สร้าง Project ใหม่ เลือก Project เดิมเพื่อทำการวิเคราะห์ หรือ ลบ Project

1. กรณีผู้วิเคราะห์ เลือกลบProject ระบบจะทำการลบProject ที่ถูกเลือกและกลับไปในส่วนเริ่มการวิเคราะห์ความเสี่ยง 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. ผู้วิเคราะห์เลือกว่าจะทำการวิเคราะห์ในส่วน Residual Risk ต่อไป หรือจะกลับไปยังเมนูหลักของระบบ
8. ระบบจะให้ผู้วิเคราะห์ตอบแบบสอบถามเพื่อนำใช้ในการวิเคราะห์หา Residual Risk
9. ระบบแสดงผลการวิเคราะห์ในส่วน residual Risk
10. ผู้วิเคราะห์เลือกว่าจะออกจากระบบ หรือจะกลับไปยังเมนูหลักของระบบ



รูปที่ 3.1 Activity Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

- กรณีเลือกเข้าไปในส่วน แสดงผลวิเคราะห์ความเสี่ยง

1. ผู้วิเคราะห์จะทำเลือก Project ที่ต้องการจะดู จากรายการของ Project ที่มีอยู่
2. ผู้วิเคราะห์จะทำเลือกว่าใน Project นี้ จะดูผลการวิเคราะห์ของใคร เพราใน 1 Project อาจมีผู้วิเคราะห์หลายคน

3. ระบบแสดงผลการวิเคราะห์ตามที่เลือกไว้
4. ผู้วิเคราะห์เลือกว่าจะออกจากระบบ หรือจะกลับไปยังเมนูหลักของระบบ

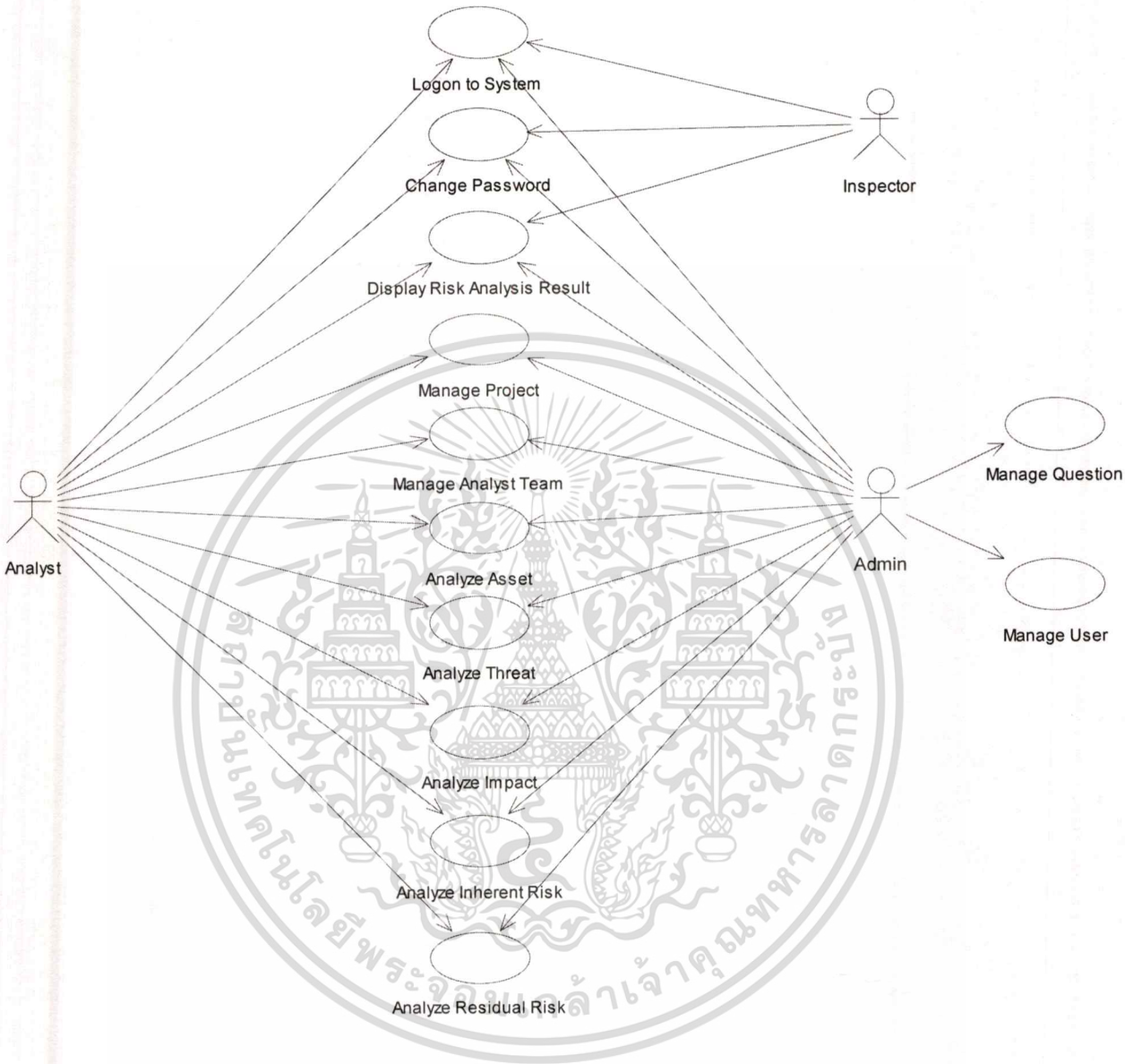
- กรณีเลือกเข้าไปในส่วน การจัดการคำถาม (ผู้ดูแลระบบเท่านั้นที่สามารถเข้าใช้ส่วนนี้ได้)

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 ซึ่งจะทำให้เห็นฟังก์ชันหลักที่เกิดขึ้นในระบบและแสดงความสัมพันธ์ระหว่างผู้ใช้กับระบบ

จาก Use Case Diagram ในรูปที่ 3.2 จะประกอบด้วย Actor ซึ่งแสดงแทนด้วยสัญลักษณ์รูปคน หมายถึง ผู้ที่เกี่ยวข้องกับระบบ จะเห็นว่าในระบบวิเคราะห์ความเสี่ยงของสารสนเทศประกอบด้วย Actor 3 ตัว ได้แก่ ผู้วิเคราะห์หรือนักวิเคราะห์(Analist) และผู้ใช้ทั่วไป (Inspector) ซึ่งเปรียบเสมือนUser 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 สร้างจัดการโครงการ
- Manage Analyst Team หมายถึง สร้างจัดการทีมนักวิเคราะห์ความเสี่ยง

- Analyze Asset หมายถึง วิเคราะห์ทรัพย์สินที่สำคัญขององค์กร
- Analyze Threat หมายถึง วิเคราะห์ภัยคุกคามต่อทรัพย์สิน
- Analyze Impact หมายถึง วิเคราะห์ผลกระทบจากภัยคุกคาม
- Analyze Inherent Risk หมายถึง วิเคราะห์ความเสี่ยงถาวร (Inherent Risk)
- Analyze Residual Risk หมายถึง วิเคราะห์ความเสี่ยงที่เหลือ (Residual Risk)
- Manage Question หมายถึง จัดการคำถามเกี่ยวกับการควบคุมความเสี่ยง
- Manage User หมายถึง จัดการข้อมูลผู้ใช้ระบบ

3.2 การวิเคราะห์และออกแบบระบบ

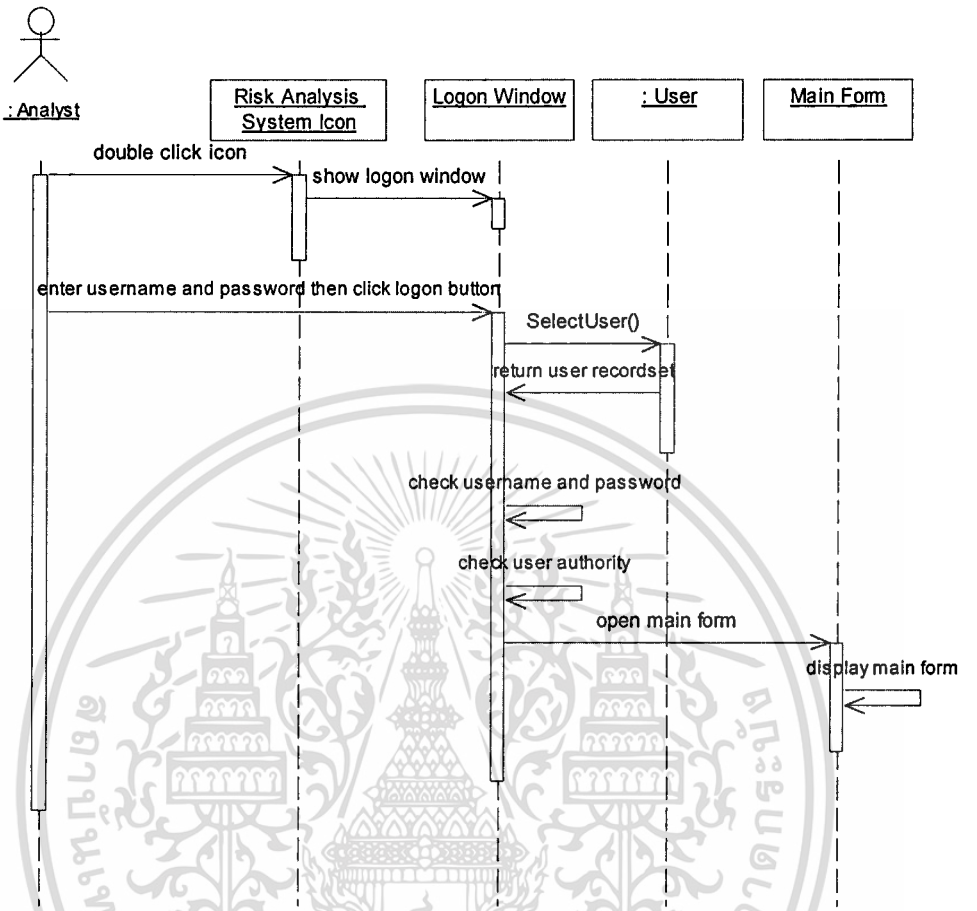
จากภาพรวมของฟังก์ชันการทำงานในระบบวิเคราะห์ความเสี่ยงของสารสนเทศที่แสดงโดยใช้ Use Case Diagram มีวัตถุประสงค์เพื่อใช้อธิบายหน้าที่ของระบบให้มีความชัดเจนยิ่งขึ้น เพื่อให้เกิดความเข้าใจตรงกันระหว่างผู้ใช้ระบบกับนักวิเคราะห์ระบบ ดังนั้น ในแต่ละ Use Case ควรมีการแสดงขั้นตอนการทำงานโดยละเอียดตั้งแต่ต้นจนจบ โดยในที่นี้จะขอเลือกนำเสนอรายละเอียดในแต่ละ Use Case ด้วย Activity Diagram และ Sequence Diagram โดย Activity Diagram จะอธิบายขั้นตอนการทำงานและกิจกรรมต่างๆที่เกิดขึ้นภายใน Use Case และ Sequence Diagram จะอธิบายขั้นตอนการทำงานและการติดต่อสื่อสารกันที่เกิดขึ้นภายใน Use Case โดยจะเน้นไปที่แกนเวลา คือ ถ้าเวลาเปลี่ยน ขั้นตอนการทำงานจะเปลี่ยนโดยมี Actor เป็นผู้กระทำเริ่มต้น

- Sequence Diagram ของระบบวิเคราะห์ความเสี่ยงของสารสนเทศในแต่ละ Use Case มีดังนี้

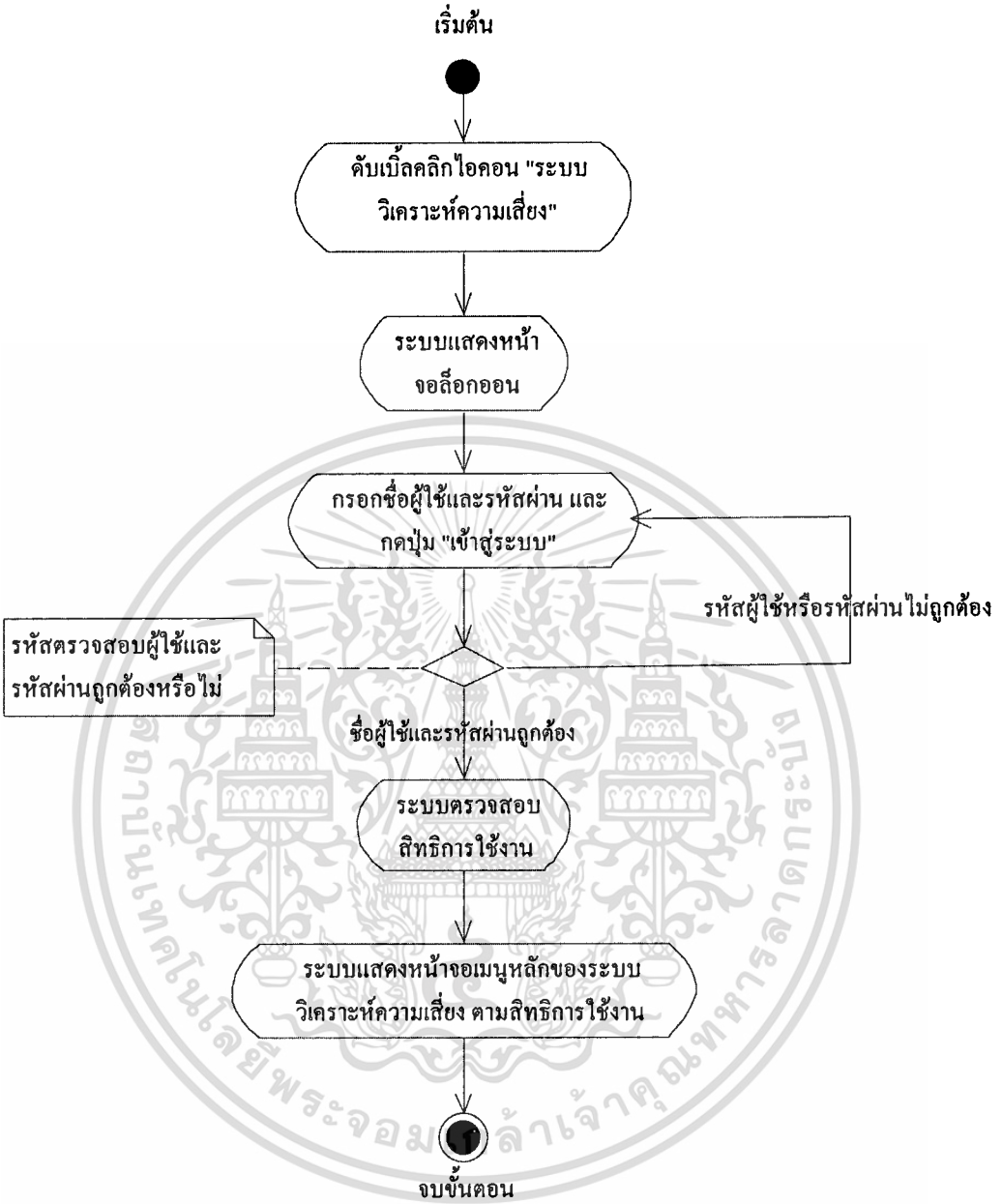
1. Sequence Diagram : Logon to System แสดงดังรูปที่ 3.3
2. Sequence Diagram : Change Password แสดงดังรูปที่ 3.5
3. Sequence Diagram : Display Risk Analysis Result แสดงดังรูปที่ 3.7
4. Sequence Diagram : Manage Project แสดงดังรูปที่ 3.9
5. Sequence Diagram : Manage Analyst Team แสดงดังรูปที่ 3.11
6. Sequence Diagram : Analyze Asset แสดงดังรูปที่ 3.13
7. Sequence Diagram : Analyze Threat แสดงดังรูปที่ 3.15
8. Sequence Diagram : Analyze Impact แสดงดังรูปที่ 3.17
9. Sequence Diagram : Analyze Inherent Risk แสดงดังรูปที่ 3.19
10. Sequence Diagram : Analyze Residual Risk แสดงดังรูปที่ 3.21
11. Sequence Diagram : Manage Question แสดงดังรูปที่ 3.23
12. Sequence Diagram : Manage User แสดงดังรูปที่ 3.25

- Activity Diagram ของระบบวิเคราะห์ความเสี่ยงของสารสนเทศในแต่ละ Use Case มีดังนี้

1. Activity Diagram : Logon to System แสดงดังรูปที่ 3.4
2. Activity Diagram : Change Password แสดงดังรูปที่ 3.6
3. Activity Diagram : Display Risk Analysis Result แสดงดังรูปที่ 3.8
4. Activity Diagram : Manage Project แสดงดังรูปที่ 3.10
5. Activity Diagram : Manage Analyst Team แสดงดังรูปที่ 3.12
6. Activity Diagram : Analyze Asset แสดงดังรูปที่ 3.14
7. Activity Diagram : Analyze Threat แสดงดังรูปที่ 3.16
8. Activity Diagram : Analyze Impact แสดงดังรูปที่ 3.18
9. Activity Diagram : Analyze Inherent Risk แสดงดังรูปที่ 3.20
10. Activity Diagram : Analyze Residual Risk แสดงดังรูปที่ 3.22
11. Activity Diagram : Manage Question แสดงดังรูปที่ 3.24
12. Activity Diagram : Manage User แสดงดังรูปที่ 3.26



รูปที่ 3.3 Sequence Diagram : Logon to System

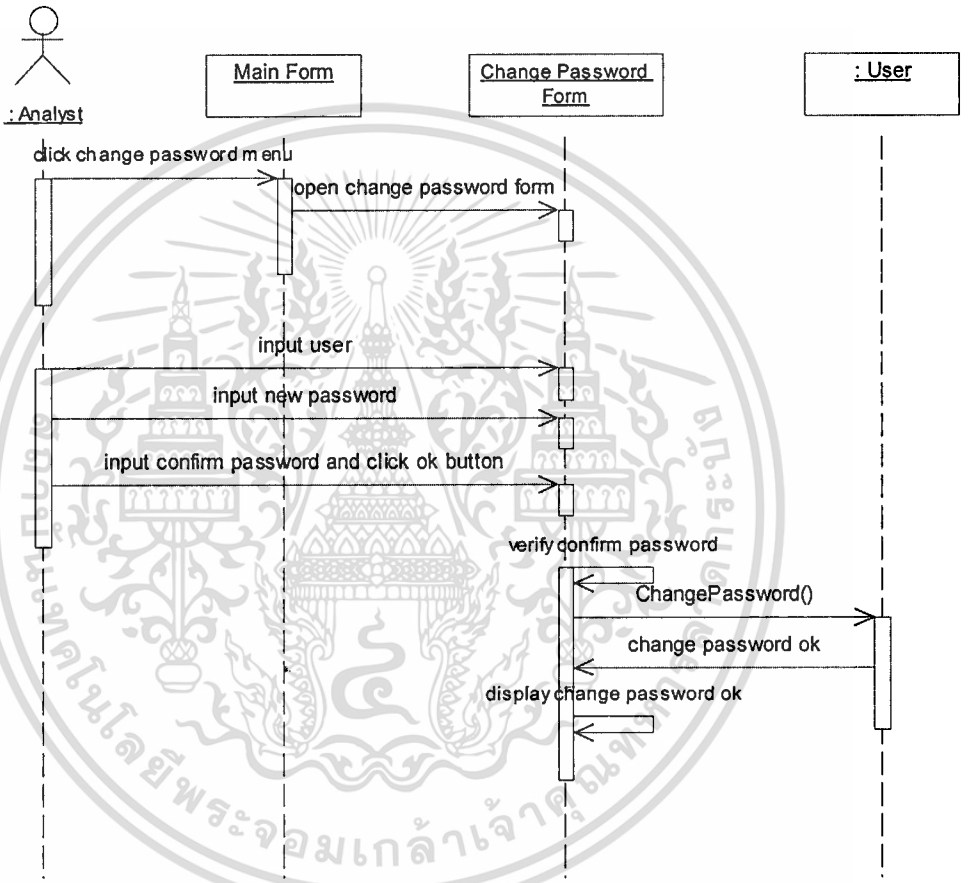


รูปที่ 3.4 Activity Diagram : Logon to System

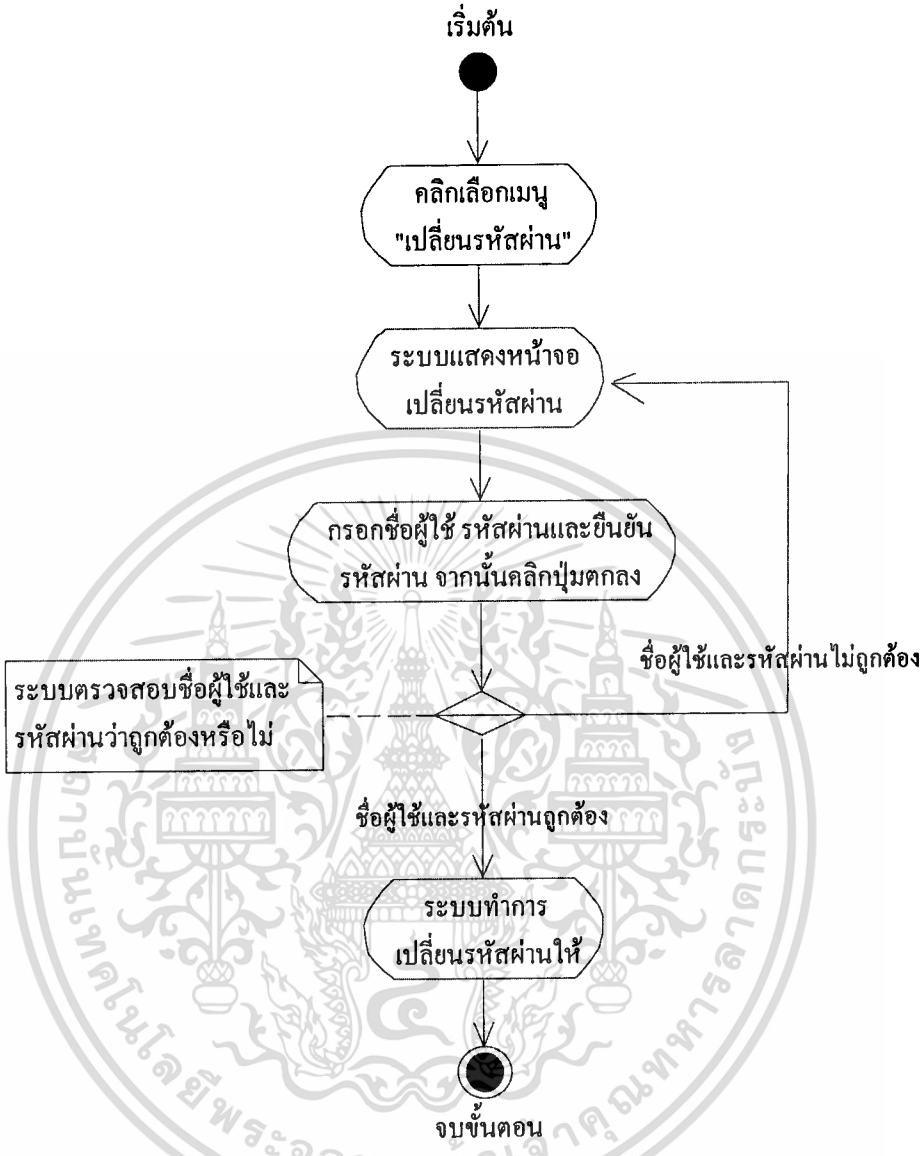
ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Logon to System สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.4 โดยมีขั้นตอนดังต่อไปนี้

1. ดับเบิ้ลคลิกไอคอน “ระบบวิเคราะห์ความเสี่ยง”
2. ระบบแสดงหน้าจอล็อกออน
3. กรอกชื่อผู้ใช้และรหัสผ่านและกดปุ่ม “เข้าสู่ระบบ”

4. ระบบตรวจสอบชื่อผู้ใช้และรหัสผ่าน ถ้าชื่อผู้ใช้และรหัสผ่านไม่ถูกต้องจะกลับไปยังหน้าจอล็อกออน
5. ถ้าชื่อผู้ใช้และรหัสผ่านถูกต้องระบบจะทำการตรวจสอบสิทธิการใช้งาน
6. ระบบแสดงหน้าจอเมนูหลักของระบบวิเคราะห์ความเสี่ยง ตามสิทธิการใช้งาน



รูปที่ 3.5 Sequence Diagram : Change Password

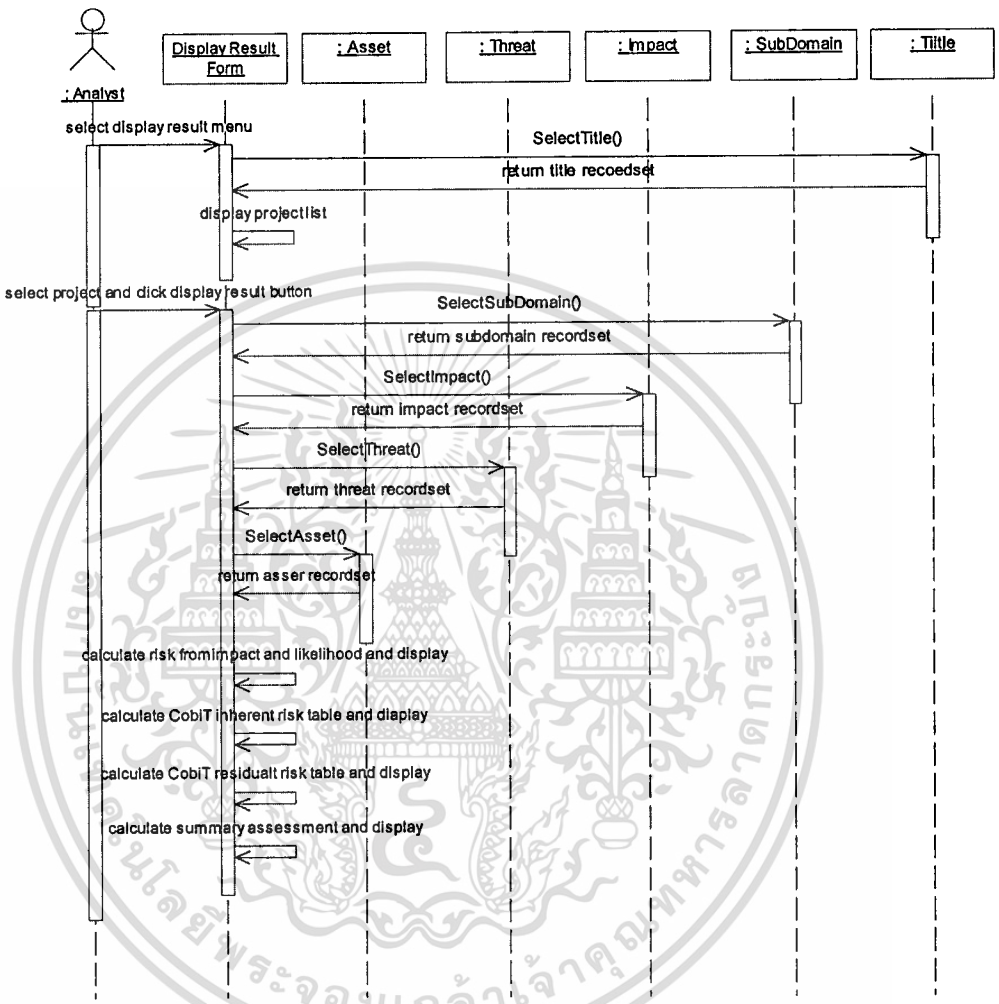


รูปที่ 3.6 Activity Diagram : Change Password

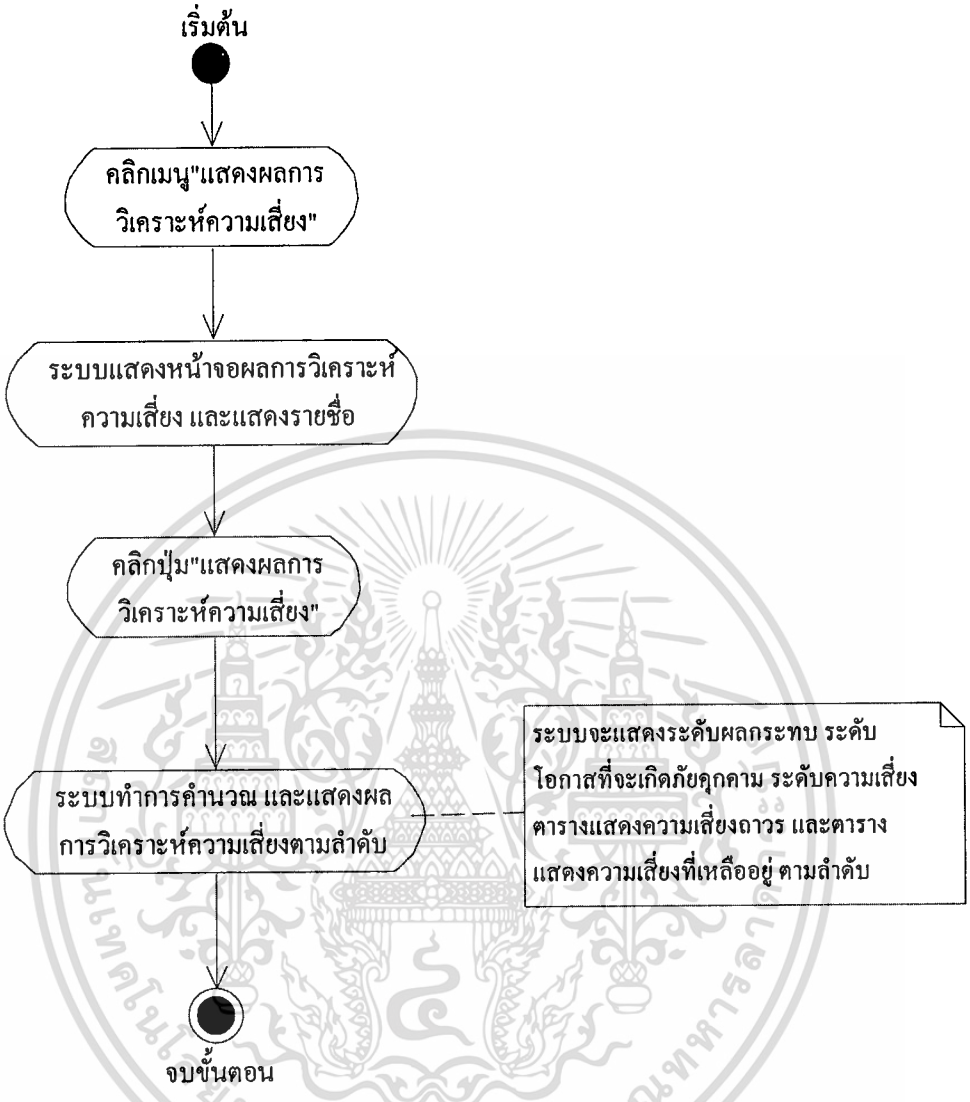
ขั้นตอนการทำงานตั้งแต่ต้นจนจบของ Use Case : Change Password สามารถอธิบายได้ด้วย Activity Diagram ดังรูปที่ 3.6 โดยมีขั้นตอนดังต่อไปนี้

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

5. ถ้าชื่อผู้ใช้และรหัสผ่านถูกต้องระบบจะทำการเปลี่ยนรหัสผ่านให้



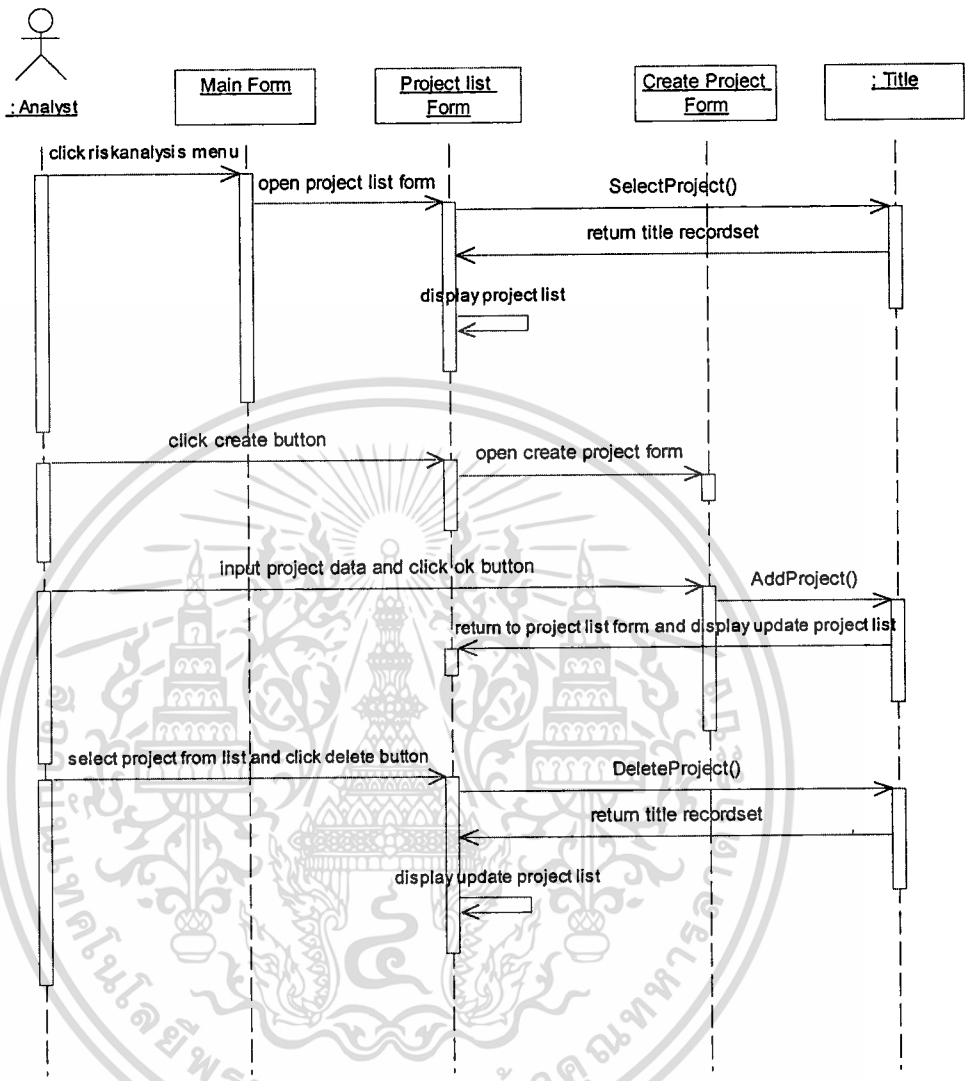
รูปที่ 3.7 Sequence Diagram : Display Risk Analysis Result



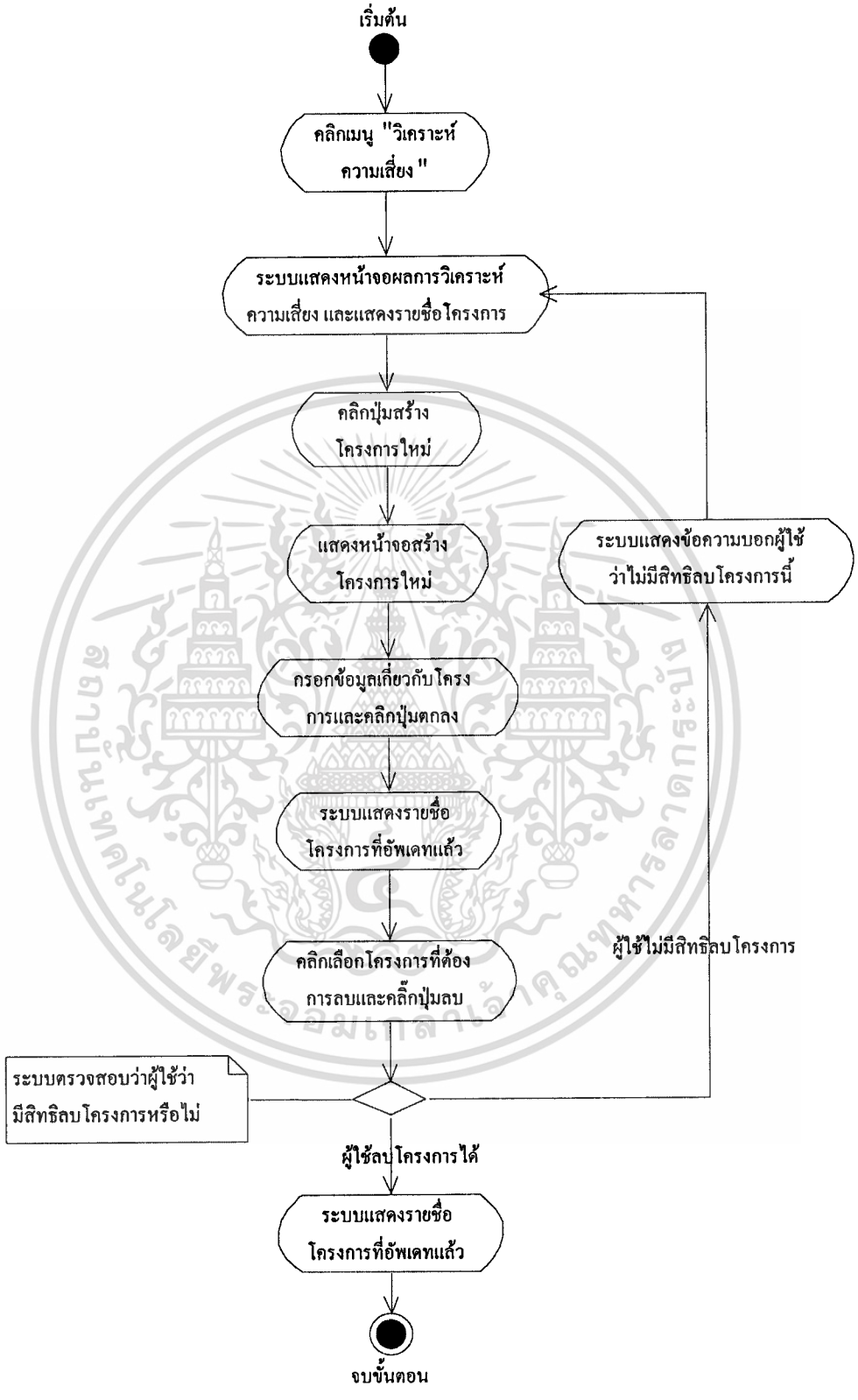
รูปที่ 3.8 Activity Diagram : Display Risk Analysis Result

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



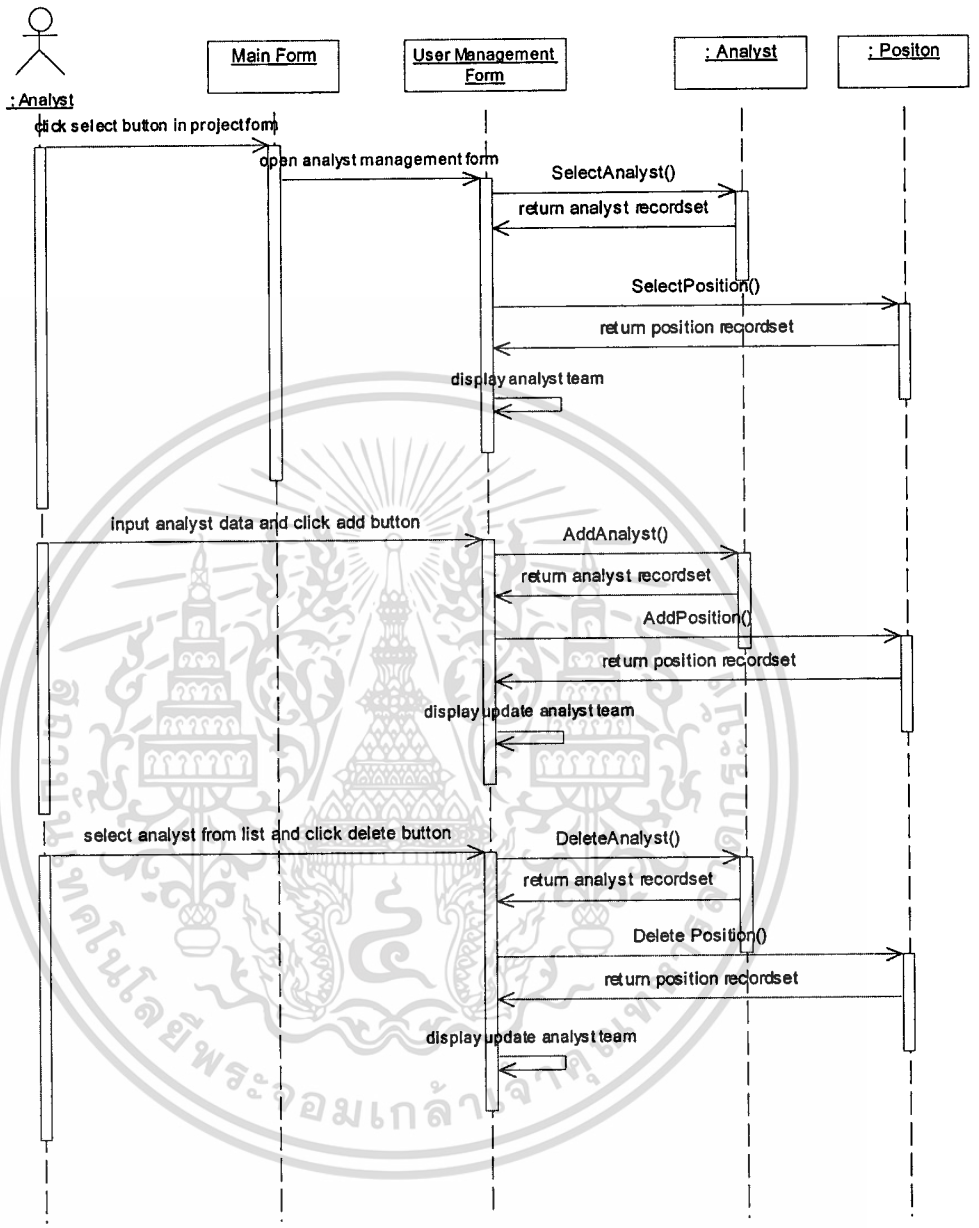
รูปที่ 3.9 Sequence Diagram : Manage Project



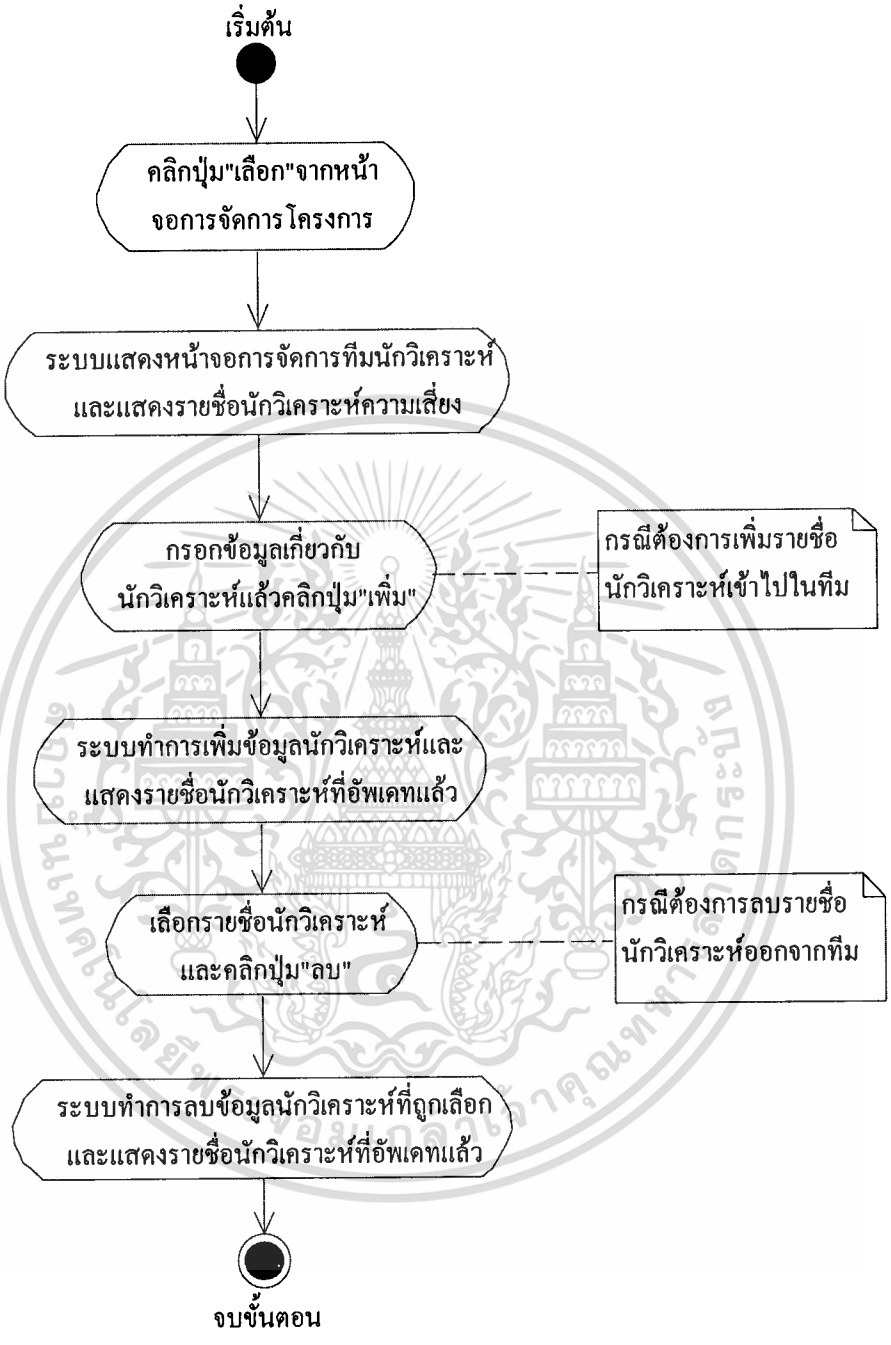
รูปที่ 3.10 Activity Diagram : Manage Project

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. ระบบตรวจสอบผู้ใช้ว่ามีสิทธิลบโครงการหรือไม่ ถ้าผู้ใช้ไม่มีสิทธิลบโครงการจะมีข้อความแจ้งเตือนว่าไม่มีสิทธิในการลบจ้างนั้นระบบจะกลับไปยังหน้าจอการวิเคราะห์ความเสี่ยงและแสดงรายชื่อโครงการ



รูปที่ 3.11 Sequence Diagram : Manage Analyst Team



รูปที่ 3.12 Activity Diagram : Manage Analyst Team

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

1. คลิกปุ่ม “เลือก” จากหน้าจอการจัดการโครงการ

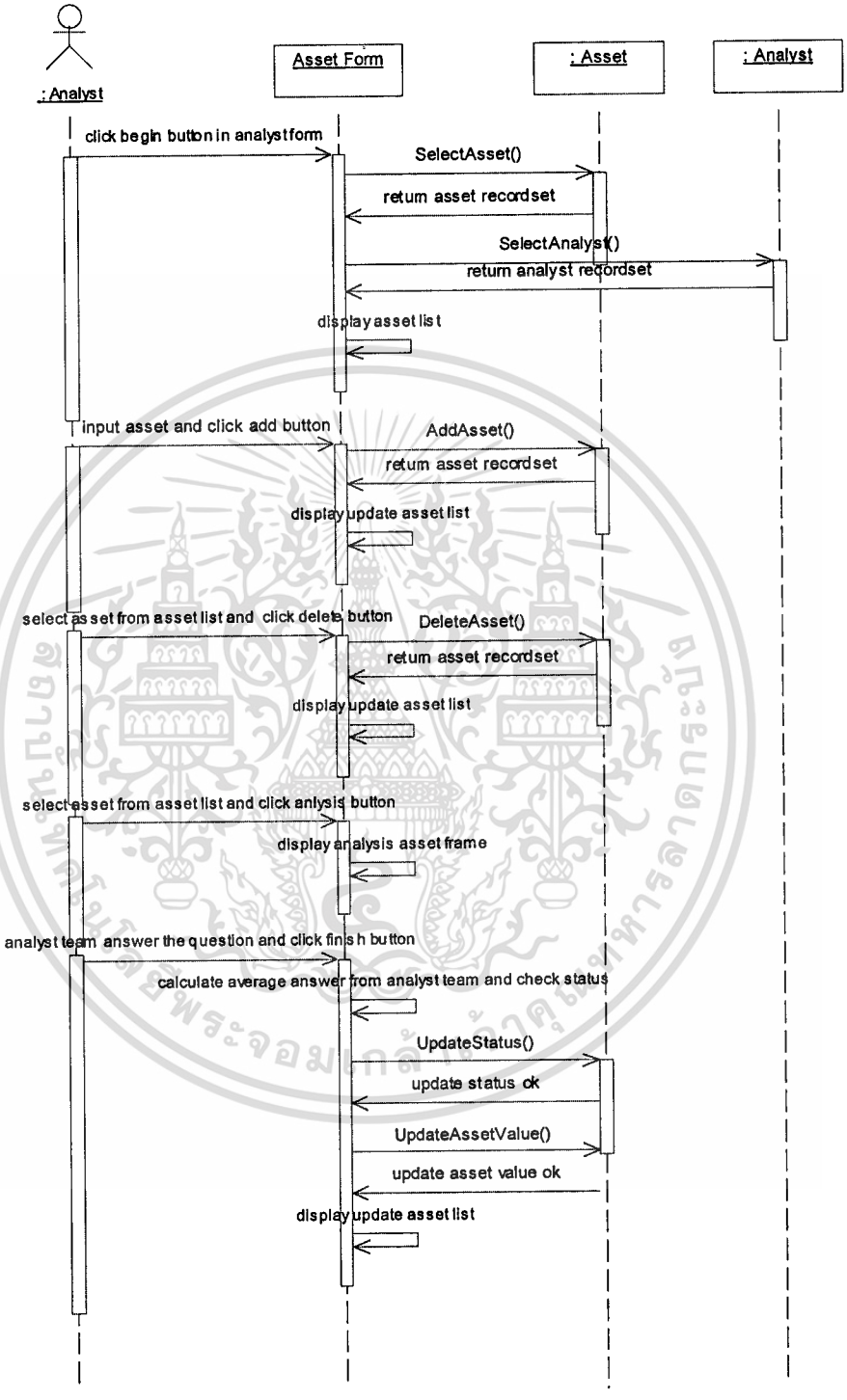
2. ระบบแสดงหน้าจอการจัดการทีมนักวิเคราะห์และแสดงรายชื่อนักวิเคราะห์ความเสี่ยง

3. กรอกข้อมูลเกี่ยวกับนักวิเคราะห์แล้วคลิกปุ่ม “เพิ่ม” โดยทำในกรณีที่ต้องการเพิ่มรายชื่อนักวิเคราะห์เข้าไปในทีม

4. ระบบจะทำการเพิ่มข้อมูลนักวิเคราะห์และแสดงรายชื่อนักวิเคราะห์ที่อัพเดทแล้ว

5. ในกรณีที่ต้องการลบรายชื่อนักวิเคราะห์ออกจากทีมให้เลือกรายชื่อนักวิเคราะห์และคลิกปุ่ม “ลบ”

6. ระบบทำการลบข้อมูลนักวิเคราะห์ที่ถูกเลือกและแสดงรายชื่อนักวิเคราะห์ที่อัพเดทแล้ว

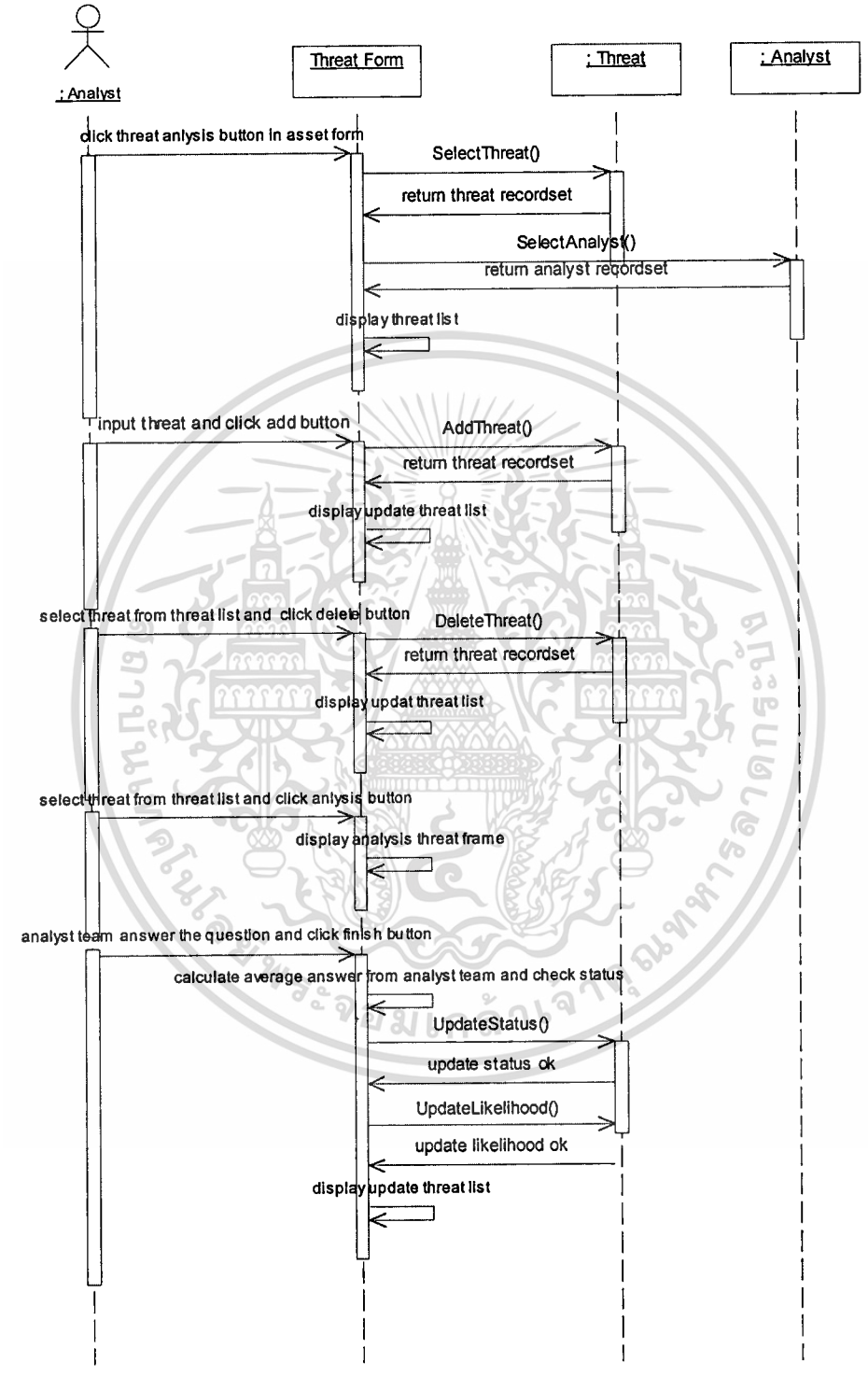


รูปที่ 3.13 Sequence Diagram : Analyze Asset

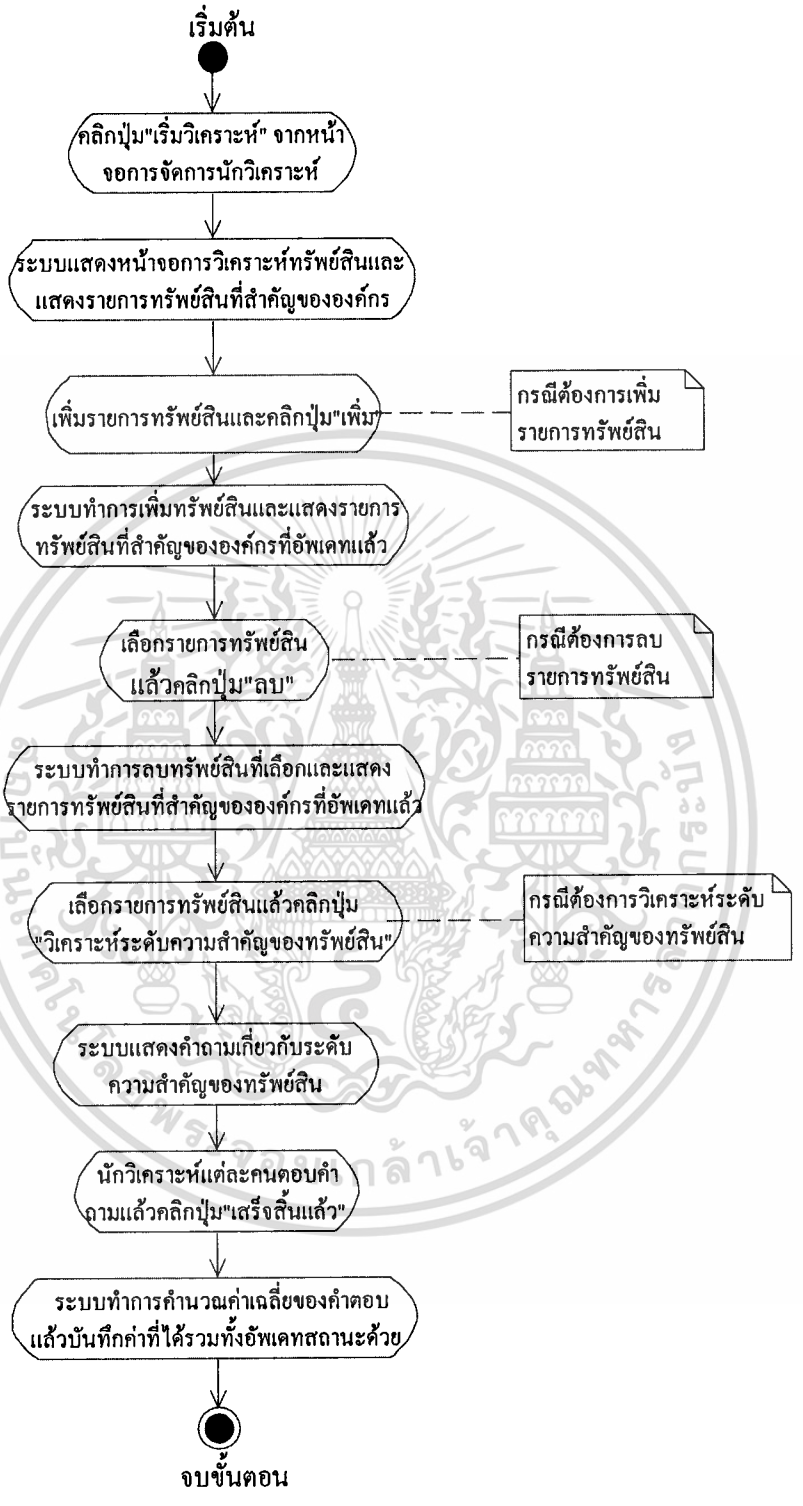
รูปที่ 3.14 Activity Diagram : Analyze Asset

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

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



รูปที่ 3.15 Sequence Diagram : Analyze Threat



รูปที่ 3.16 Activity Diagram : Analyze Threat

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

1. คลิกปุ่ม “เริ่มวิเคราะห์” จากหน้าจอการจัดการนักวิเคราะห์

2. ระบบแสดงหน้าจอการวิเคราะห์ทรัพย์สินและแสดงรายการทรัพย์สินที่สำคัญขององค์กร

3. ในกรณีที่ต้องการเพิ่มรายการทรัพย์สิน ให้คลิกปุ่ม “เพิ่ม”

4. ระบบทำการเพิ่มทรัพย์สินและแสดงรายการทรัพย์สินที่สำคัญขององค์กรที่อัพเดทแล้ว

5. ในกรณีต้องการลบรายการทรัพย์สิน ให้คลิกปุ่ม “ลบ”

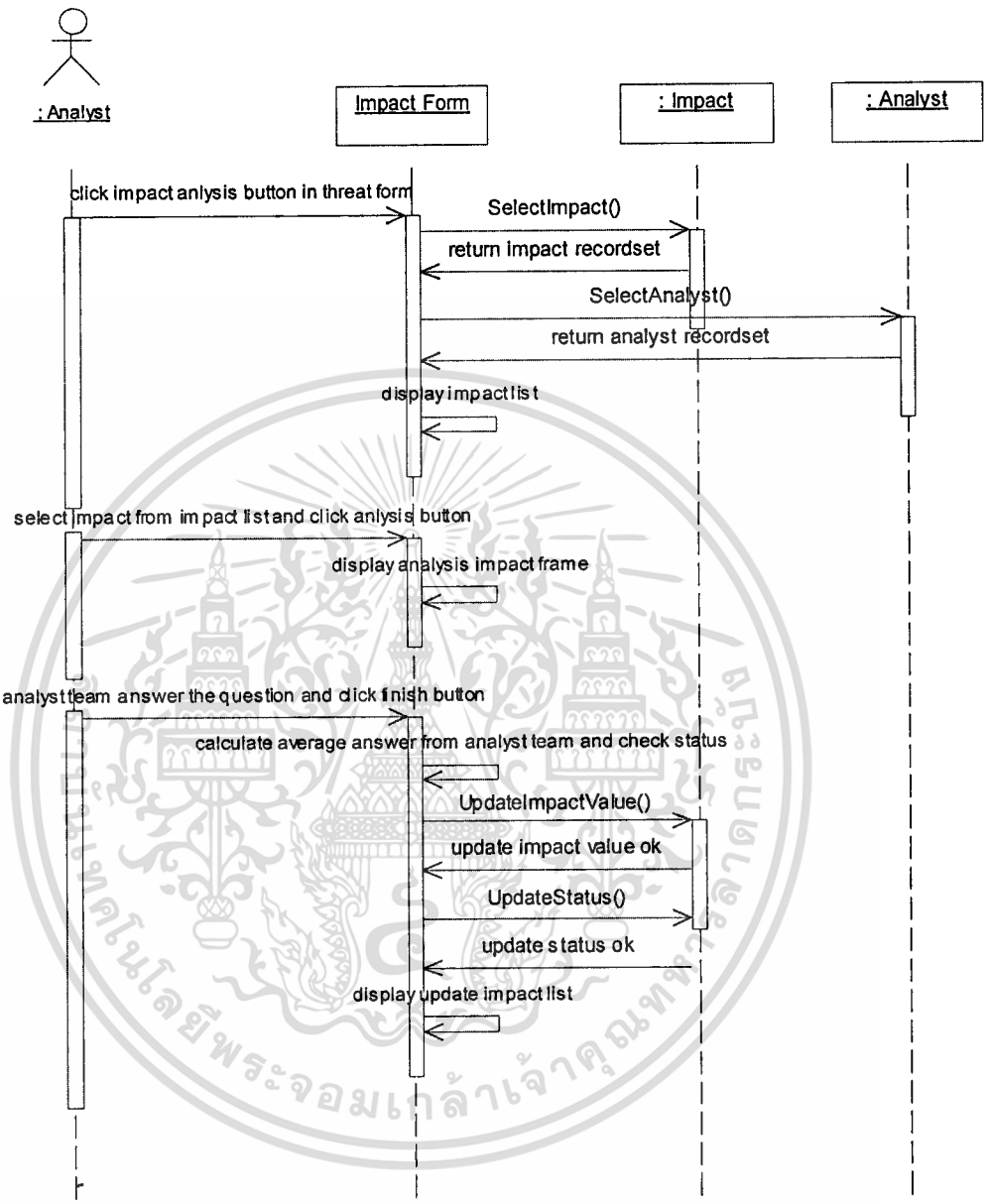
6. ระบบทำการลบทรัพย์สินที่เลือกและแสดงรายการทรัพย์สินที่สำคัญขององค์กรที่อัพเดทแล้ว

7. ในกรณีที่ต้องการวิเคราะห์ระดับความสำคัญของทรัพย์สินให้คลิกปุ่ม “วิเคราะห์ระดับความสำคัญของทรัพย์สิน”

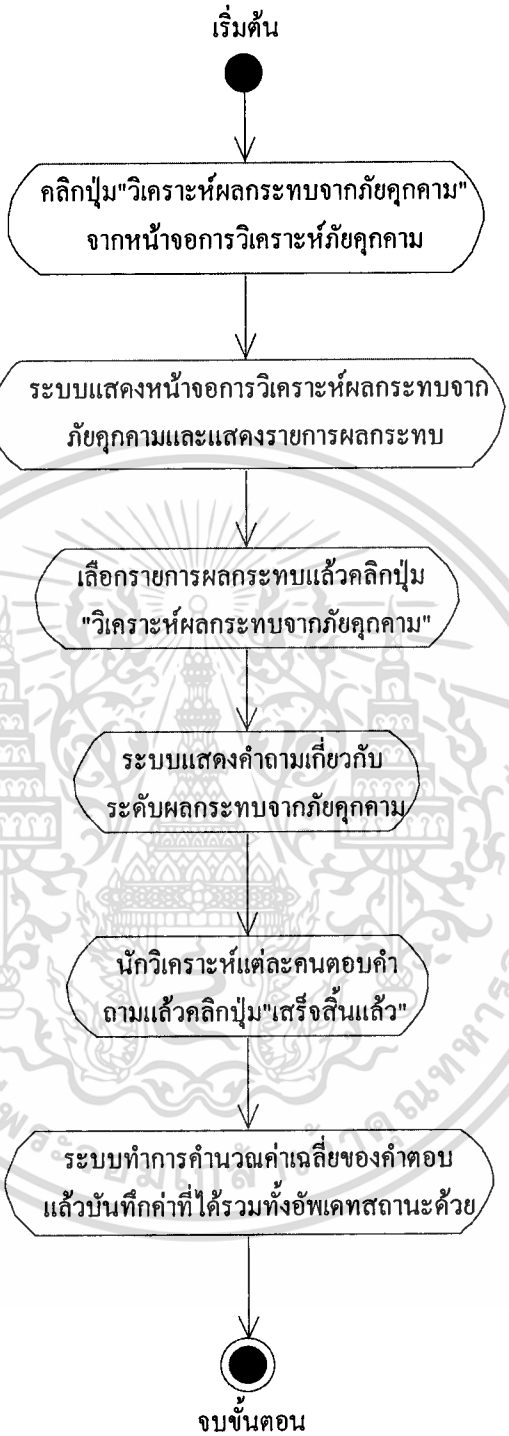
8. ระบบแสดงคำถามเกี่ยวกับระดับความสำคัญของทรัพย์สิน

9. นักวิเคราะห์แต่ละคนตอบคำถามแล้วคลิกปุ่ม “เสร็จสิ้นแล้ว”

10. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัพเดทสถานะด้วย



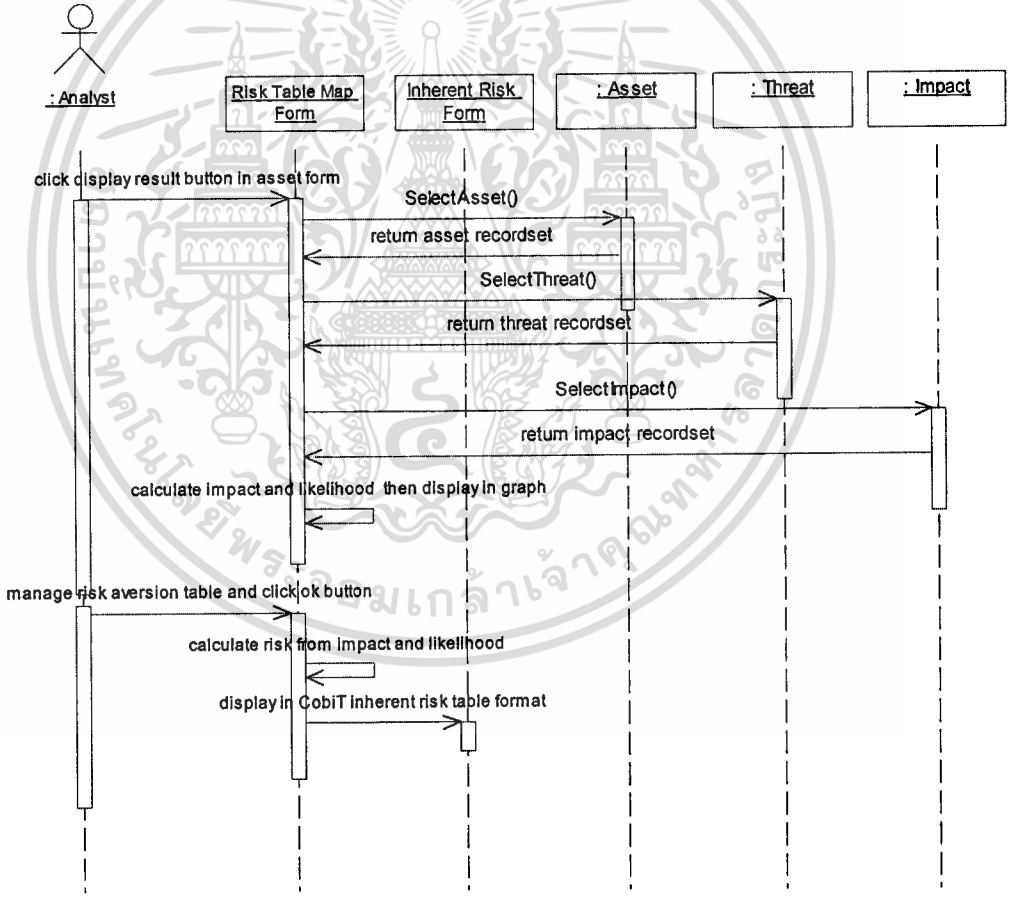
รูปที่ 3.17 Sequence Diagram : Analyze Impact



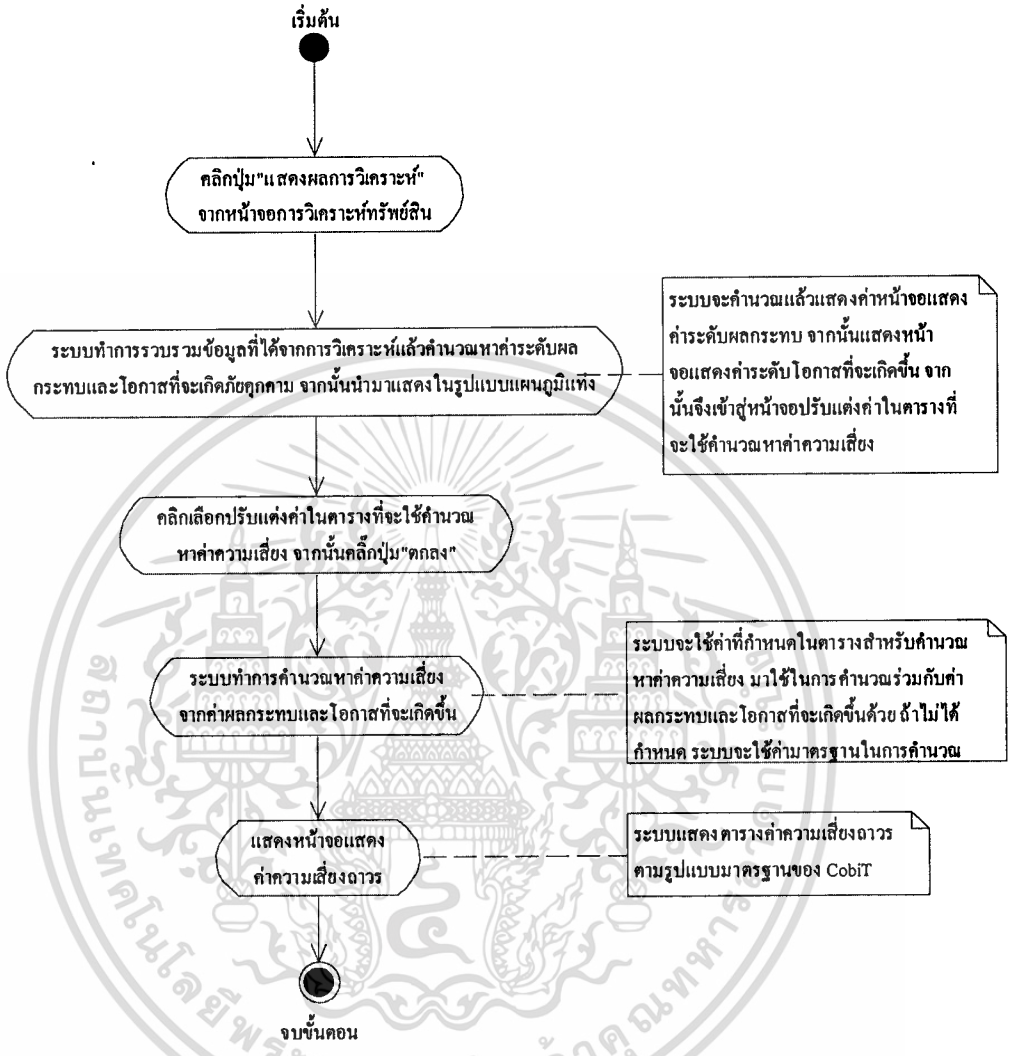
รูปที่ 3.18 Activity Diagram : Analyze Impact

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. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัพเดทสถานะด้วย



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

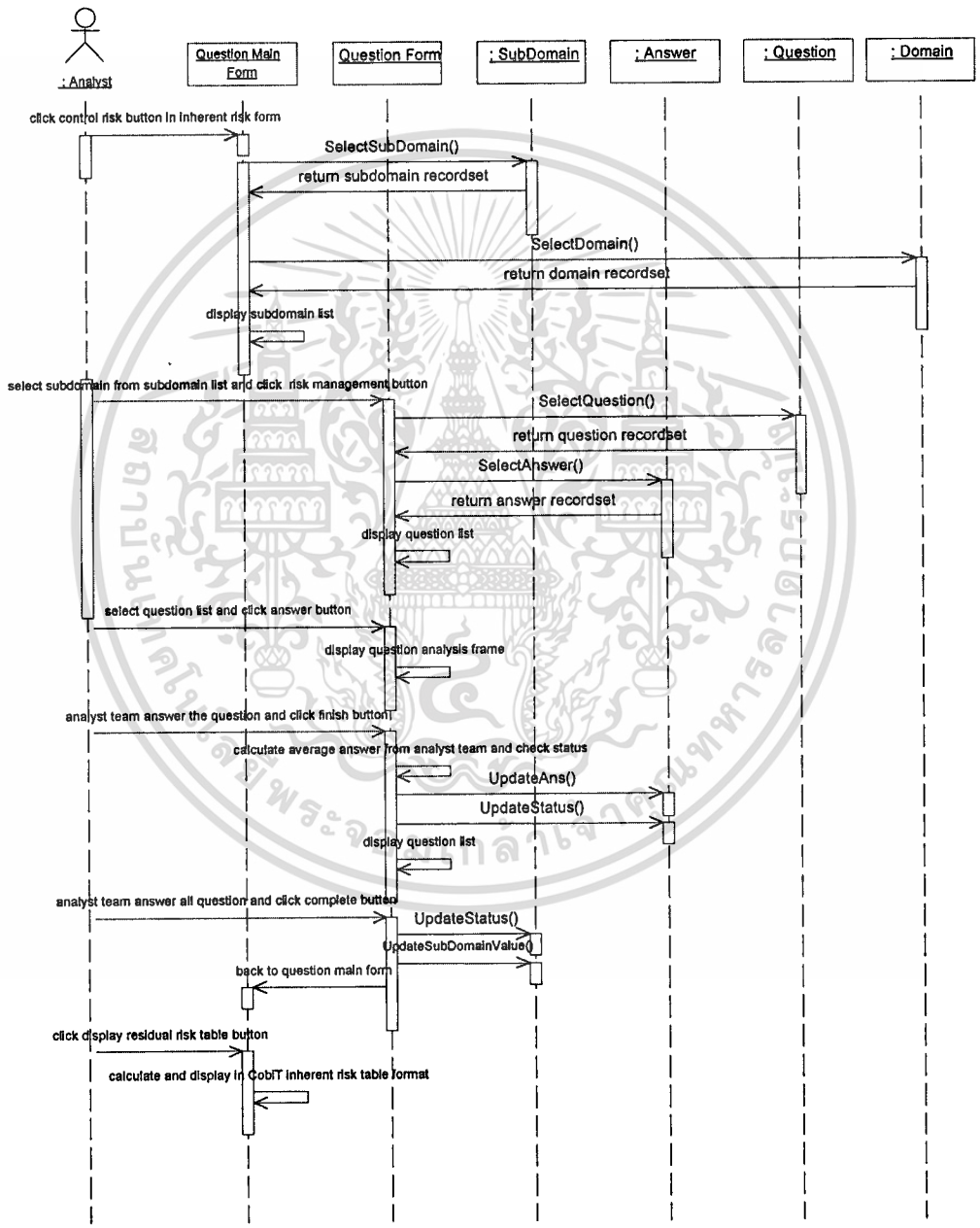
1. คลิกปุ่ม “แสดงผลการวิเคราะห์” จากหน้าจอการวิเคราะห์ทรัพย์สิน

2. ระบบทำการรวบรวมข้อมูลที่ได้จากการวิเคราะห์แล้วคำนวณหาค่าระดับผลกระทบและโอกาสที่จะเกิดภัยคุกคาม จากนั้นนำมาแสดงในรูปแบบแผนภูมิแท่ง

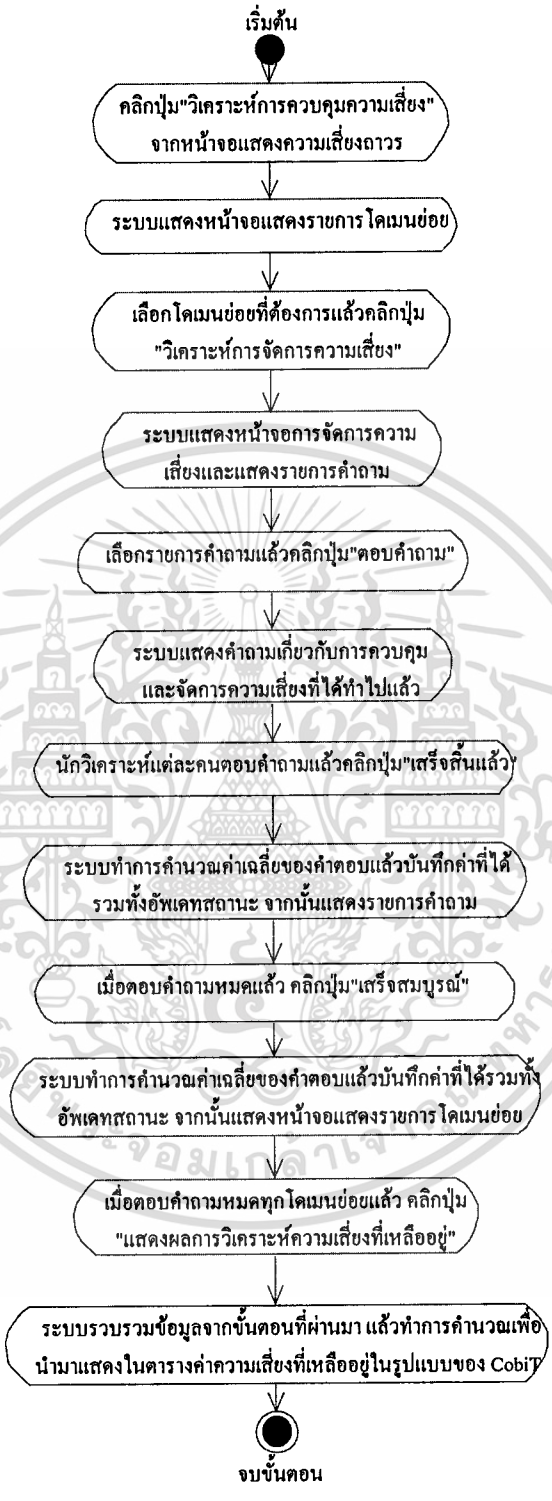
3. คลิกเลือกปรับแต่งค่าในตารางที่จะใช้คำนวณหาค่าความเสี่ยง จากนั้นคลิกปุ่ม “ตกลง”

4. ระบบจะใช้ค่าที่กำหนดในตารางสำหรับคำนวณหาค่าความเสี่ยงมาใช้ในการคำนวณร่วมกับค่าผลกระทบและโอกาสที่จะเกิดขึ้นด้วย ถ้าไม่ได้กำหนดระบบจะใช้ค่ามาตรฐานในการคำนวณ

5. ระบบแสดงตารางค่าความเสี่ยงถาวรตามรูปแบบมาตรฐานของ CobiT



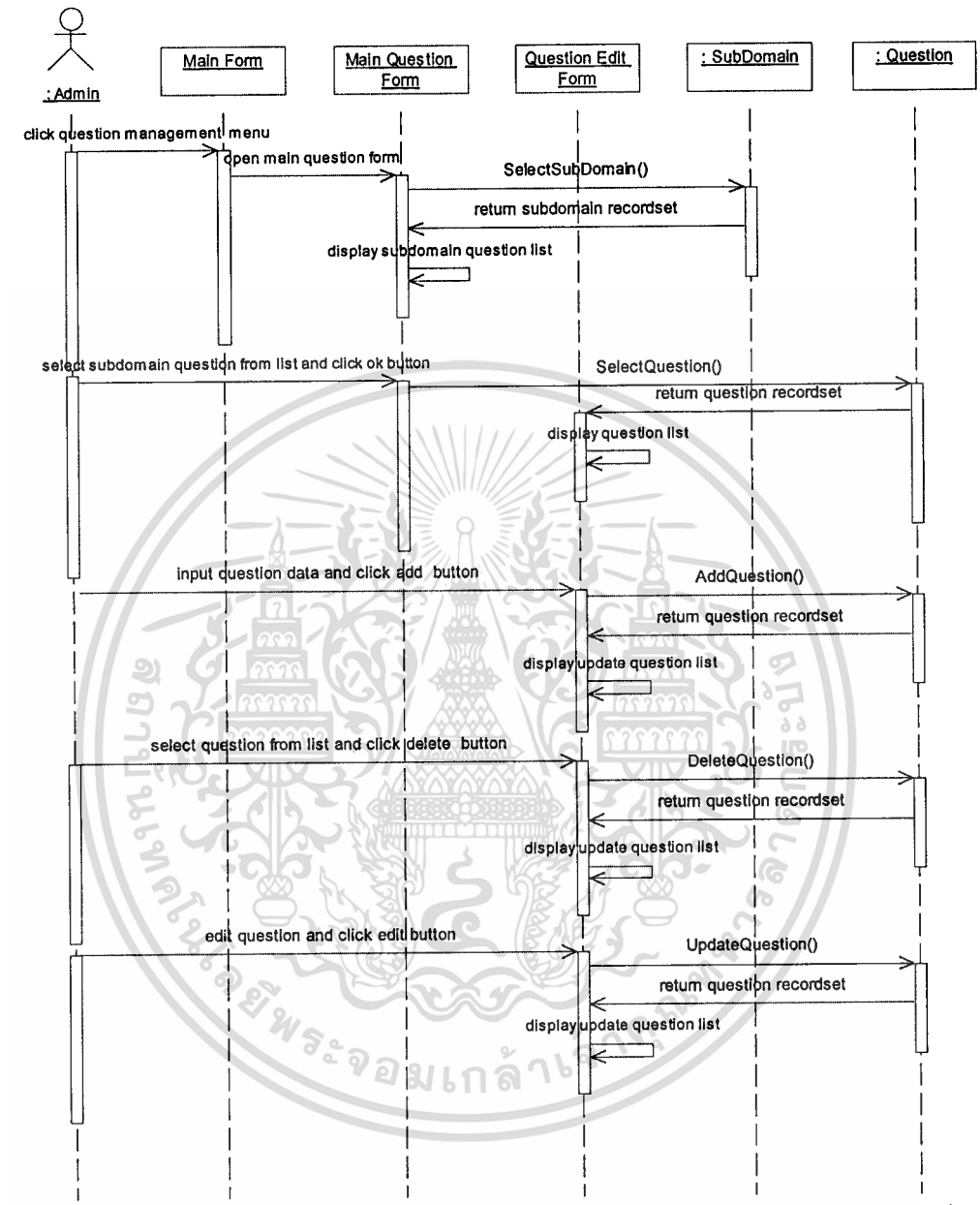
รูปที่ 3.21 Sequence Diagram : : Analyze Residual Risk



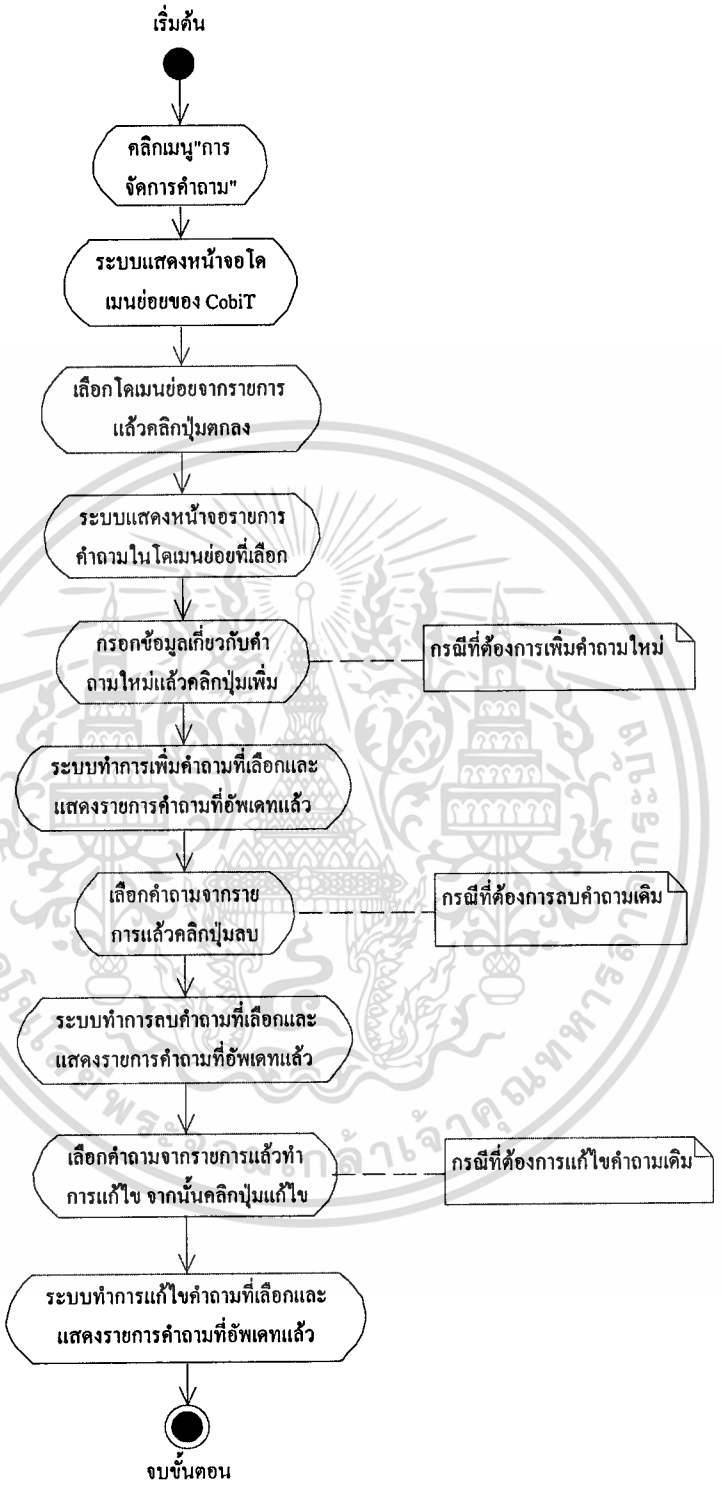
รูปที่ 3.22 Activity Diagram : Analyze Residual Risk

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

1. คลิกปุ่ม "วิเคราะห์การควบคุมความเสี่ยง" จากหน้าจอแสดงความเสี่ยงถาวร
2. ระบบแสดงหน้าจอแสดงรายการโดเมนย่อย
3. เลือกโดเมนย่อยที่ต้องการแล้วคลิกปุ่ม "วิเคราะห์การจัดการความเสี่ยง"
4. ระบบแสดงหน้าจอการจัดการความเสี่ยงและแสดงรายการคำถาม
5. เลือกรายการคำถามแล้วคลิกปุ่ม "ตอบคำถาม"
6. ระบบแสดงคำถามเกี่ยวกับการควบคุมและการจัดการความเสี่ยงที่ได้ทำไปแล้ว
7. นักวิเคราะห์แต่ละคนตอบคำถามแล้วคลิกปุ่ม "เสร็จสิ้นแล้ว"
8. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัพเดทสถานะจากนั้นแสดงรายการคำถาม
9. เมื่อตอบคำถามหมดแล้ว คลิกปุ่ม "เสร็จสมบูรณ์"
10. ระบบทำการคำนวณค่าเฉลี่ยของคำตอบแล้วบันทึกค่าที่ได้รวมทั้งอัพเดทสถานะจากนั้นแสดงหน้าจอแสดงรายการโดเมนย่อย
11. เมื่อตอบคำถามหมดทุกโดเมนย่อยแล้วคลิกปุ่ม "แสดงผลการวิเคราะห์ความเสี่ยงที่เหลืออยู่"
12. ระบบรวบรวมข้อมูลจากขั้นตอนที่ผ่านมา แล้วทำการคำนวณเพื่อนำมาแสดงในตารางค่าความเสี่ยงที่เหลืออยู่ในรูปแบบของ CobiT



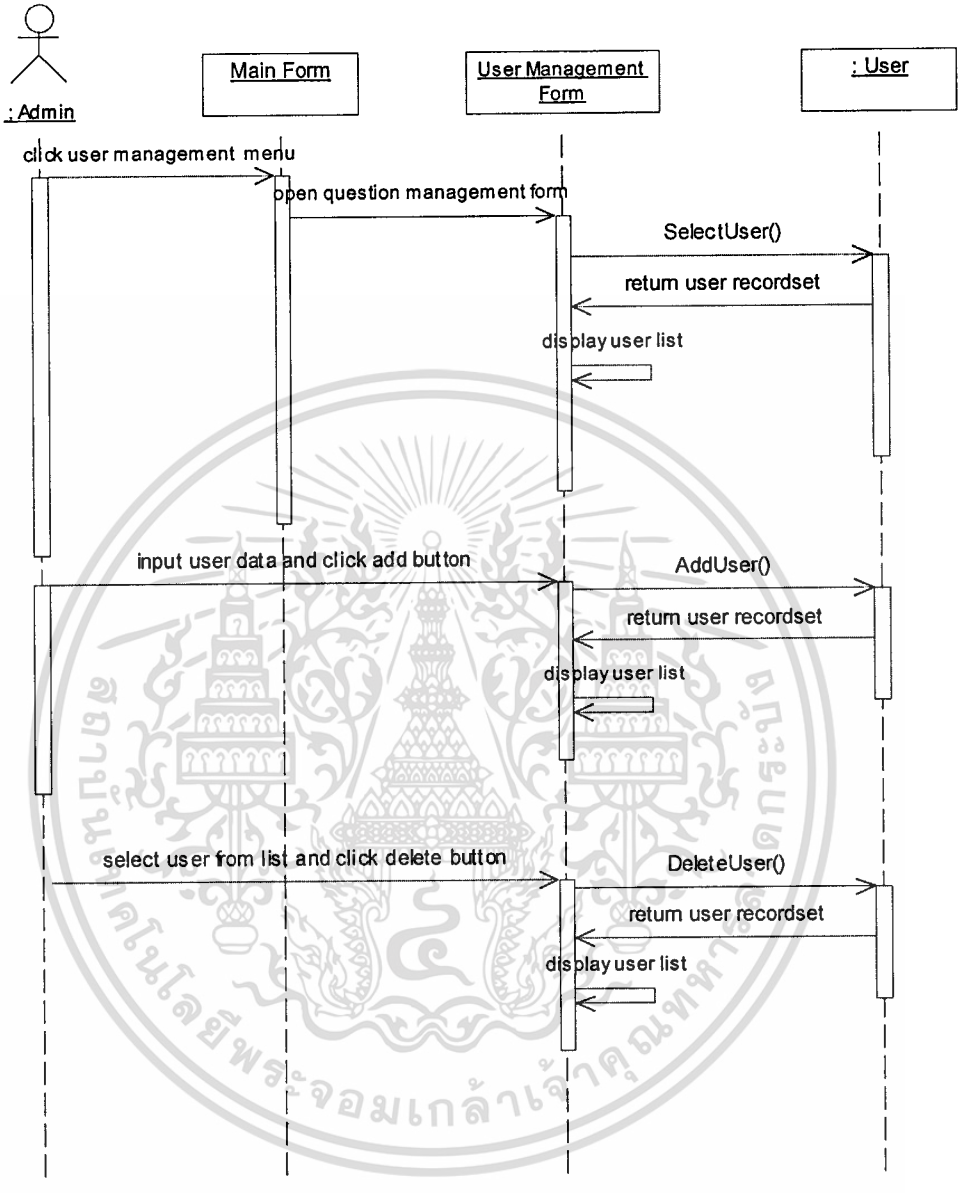
รูปที่ 3.23 Sequence Diagram : Manage Question



รูปที่ 3.24 Activity Diagram : Manage Question

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

1. คลิกเมนู “การจัดการคำถาม”
2. ระบบแสดงหน้าจอโดเมนย่อยของ CobiT
3. เลือกโดเมนย่อยจากรายการแล้วคลิกปุ่มตกลง
4. ระบบแสดงหน้าจอรายการคำถามในโดเมนย่อยที่เลือก
5. กรณีที่ต้องการเพิ่มคำถามใหม่ให้กรอกข้อมูลเกี่ยวกับคำถามใหม่แล้วคลิกปุ่มเพิ่ม
6. ระบบทำการเพิ่มคำถามที่เลือกและแสดงรายการคำถามที่อัพเดทแล้ว
7. กรณีที่ต้องการลบคำถามเดิม ให้เลือกคำถามจากรายการแล้วคลิกปุ่มลบ
8. ระบบทำการลบคำถามที่เลือกและแสดงรายการคำถามที่อัพเดทแล้ว
9. กรณีที่ต้องการแก้ไขคำถามเดิม ให้เลือกคำถามจากรายการแล้วทำการแก้ไขจากนั้นคลิกปุ่มแก้ไข
10. ระบบทำการแก้ไขคำถามที่เลือกและแสดงรายการคำถามที่อัพเดทแล้ว



รูปที่ 3.25 Sequence Diagram : Manage User

รูปที่ 3.26 Activity Diagram : Manage User

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

1. คลิกเลือกเมนู “การจัดการผู้ใช้”
2. ระบบแสดงหน้าจอการจัดการผู้ใช้และแสดงรายชื่อผู้ใช้ระบบ

3. กรณีต้องการเพิ่มผู้ใช้ระบบให้เพิ่มข้อมูลเกี่ยวกับผู้ใช้ระบบแล้วคลิกปุ่ม “เพิ่ม”

4. ระบบทำการเพิ่มผู้ใช้และแสดงรายชื่อผู้ใช้ระบบที่อัพเดทแล้ว

5. กรณีต้องการลบผู้ใช้ระบบให้เลือกรายชื่อผู้ใช้ระบบที่ต้องการจะลบแล้วคลิกปุ่ม “ลบ”

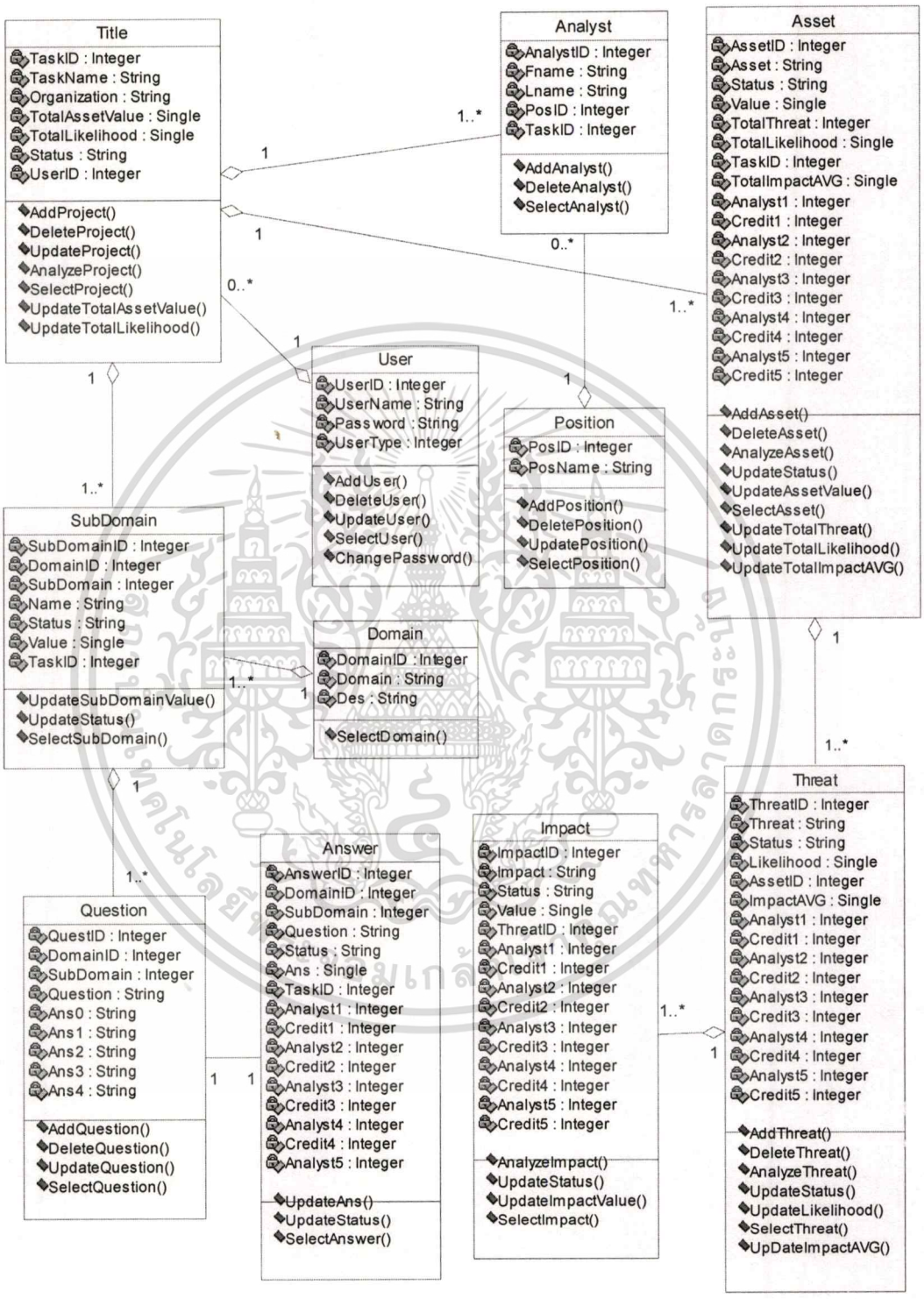
6. ระบบทำการลบผู้ใช้ที่เลือกและแสดงรายชื่อผู้ใช้ระบบที่อัพเดทแล้ว

Class Diagram เป็นแผนภาพที่แสดงความสัมพันธ์ของคลาสทั้งหมดที่ควรมีในระบบ ซึ่งจะทำให้เห็นโครงสร้างของระบบด้วย จากการวิเคราะห์ Use Case Diagram ทำให้ได้คลาสพื้นฐานสำหรับระบบวิเคราะห์ความเสี่ยงของสารสนเทศดังต่อไปนี้

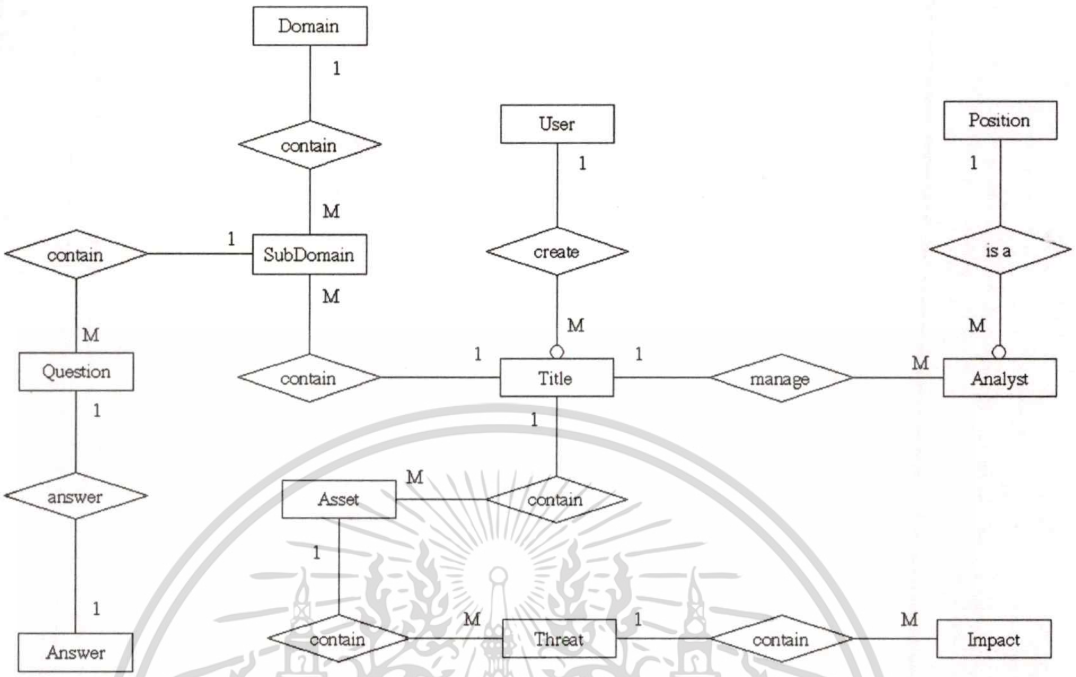
- Analyst	หมายถึง	คลาสนักวิเคราะห์ความเสี่ยง
- Answer	หมายถึง	คลาสคำถามและคำตอบที่ใช้ในการวิเคราะห์
- Asset	หมายถึง	คลาสทรัพย์สินที่สำคัญขององค์กร
- Domain	หมายถึง	คลาสโดเมนหลักของ CobiT
- Impact	หมายถึง	คลาสผลกระทบจากภัยคุกคาม
- Position	หมายถึง	คลาสตำแหน่งงานในองค์กร
- Question	หมายถึง	คลาสคำถามเกี่ยวกับการจัดการความเสี่ยง
- 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 ซึ่งมีการกำหนดแอตทริบิวส์ และเมธอด ของแต่ละคลาส

นอกจาก Class Diagram แล้ว ยังสมารถอธิบายได้โดยใช้ ER Diagram ดังรูปที่ 3.28



รูปที่ 3.27 Class Diagram ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ



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 จัดการวิเคราะห์โครงการได้ทีละ 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 รายการต้องเป็นทรัพย์สินขององค์นั้นองค์กรเดียว
- **Asset กับ Threat** มีความสัมพันธ์กันคือ ทรัพย์สิน 1 รายการ จะมีภัยคุกคามอย่างน้อย 1 ภัยคุกคาม ภัยคุกคามต่อทรัพย์สินนั้น 1 ภัยคุกคาม จะเป็นภัยคุกคามต่อทรัพย์สินนั้นเพียงรายการเดียว

- **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 เป็นโดเมนย่อยของโดเมนนั้นโดเมนเดียว
- **SubDomain กับ Question** มีความสัมพันธ์กันคือ โดเมนย่อย 1 โดเมนย่อย มีคำถามเกี่ยวกับการควบคุมความเสี่ยงอย่างน้อย 1 คำถาม คำถามของโดเมนย่อยนั้น 1 คำถาม เป็นคำถามของโดเมนย่อยนั้นโดเมนย่อยเดียว
- **Question กับ Answer** มีความสัมพันธ์กันคือ คำถาม 1 คำถาม มีคำตอบได้คำตอบเดียว คำตอบของคำถามนั้น 1 คำตอบ เป็นตอบของคำถามนั้นคำถามเดียว

บทที่ 4
การใช้งานระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

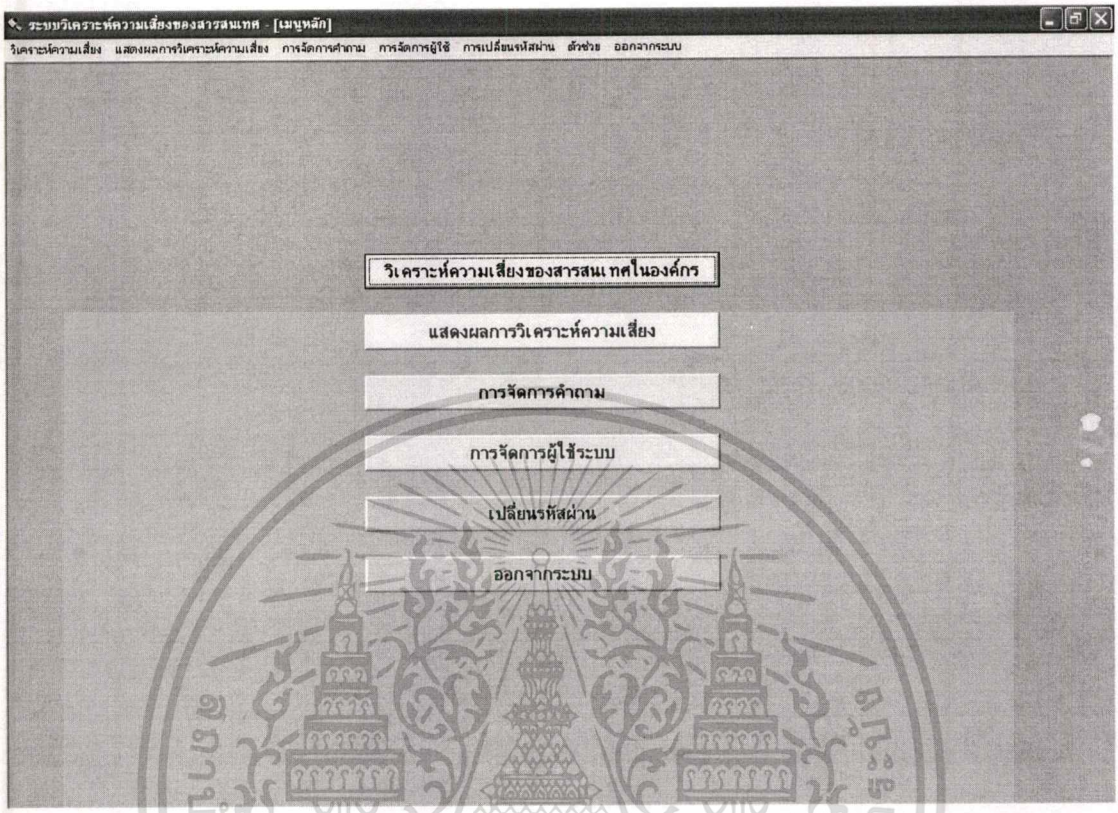
4.1 การเข้าสู่ระบบ

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

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

รูปที่ 4.1 หน้าจอเข้าสู่ระบบ

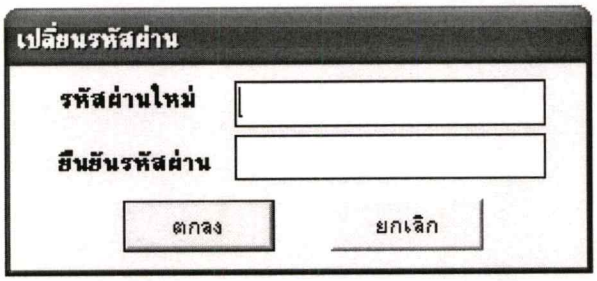
รูปที่ 4.2 เข้าสู่ระบบผิดพลาด



รูปที่ 4.3 หน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

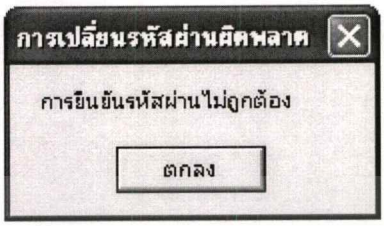
4.2 การเปลี่ยนรหัสผ่าน

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มเปลี่ยนรหัสผ่าน หลังจากนั้นระบบจะแสดงหน้าจอเปลี่ยนรหัสผ่านดังรูปที่ 4.4



รูปที่ 4.4 หน้าจอเปลี่ยนรหัสผ่าน

รูปที่ 4.5 เป็นข้อความที่แสดงเมื่อผู้ใช้ใส่รหัสผ่านใหม่และยืนยันรหัสผ่านไม่ตรงกัน ส่วนรูปที่ 4.6 เป็นข้อความที่แสดงเมื่อระบบได้ทำการเปลี่ยนรหัสผ่านให้เรียบร้อยแล้ว



รูปที่ 4.5 ข้อความยืนยันรหัสผ่านไม่ถูกต้อง

รูปที่ 4.6 ข้อความเปลี่ยนรหัสผ่านเรียบร้อยแล้ว

4.3 การวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กร

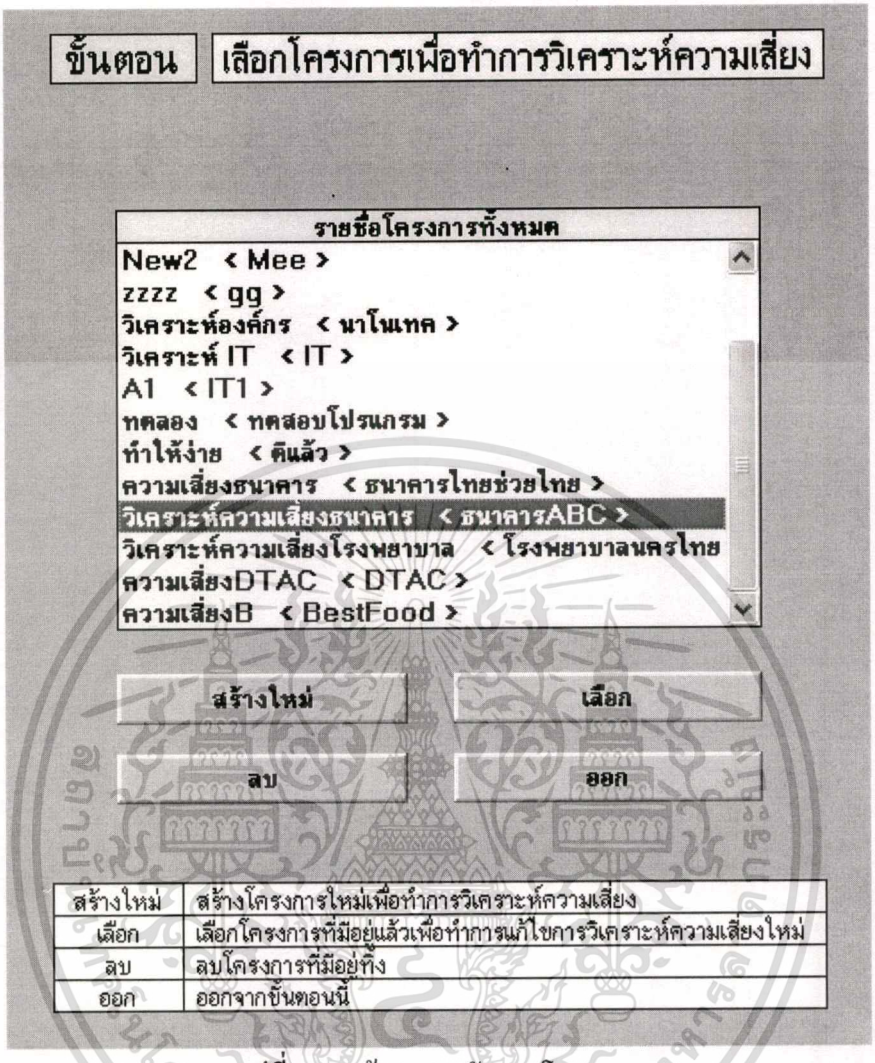
จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กรหรือคลิกการวิเคราะห์ความเสี่ยงที่เมนูข้างบน หลังจากนั้นระบบจะแสดงหน้าจอการจัดการโครงการดังรูปที่ 4.7 ซึ่งจะเป็นการแสดงรายการของโครงการวิเคราะห์ความเสี่ยงทั้งหมดทั้งที่ได้ทำการวิเคราะห์เสร็จสิ้นไปแล้วและยังไม่เสร็จ

4.3.1 การจัดการโครงการ

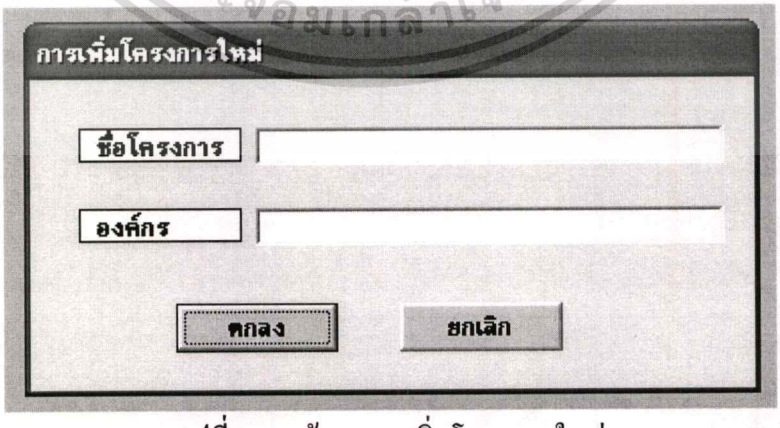
กรณีต้องการสร้างโครงการใหม่ ผู้ใช้สามารถคลิกปุ่มสร้างใหม่ ซึ่งจะแสดงหน้าจอการเพิ่มโครงการใหม่ ดังรูป 4.8 จากนั้นกรอกชื่อโครงการและชื่อองค์กรและคลิกปุ่มตกลง ระบบจะทำการเพิ่มโครงการใหม่แล้วกลับไปที่หน้าจอการจัดการโครงการ

กรณีต้องการลบโครงการ ผู้ใช้สามารถเลือกโครงการที่ต้องการลบแล้วคลิกปุ่มลบ ระบบจะแสดงข้อความยืนยันการลบโครงการดังรูป 4.9 เมื่อผู้ใช้ยืนยันระบบจะทำการลบโครงการที่เลือกและกลับไปที่หน้าจอการจัดการโครงการ

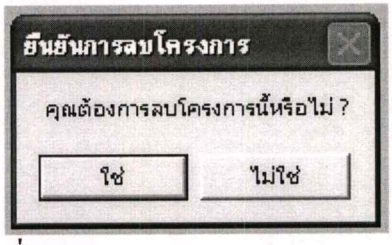
กรณีต้องการเริ่มทำการวิเคราะห์ความเสี่ยง ผู้ใช้สามารถเลือกโครงการและคลิกปุ่มเลือกได้



รูปที่ 4.7 หน้าจอการจัดการโครงการ



รูปที่ 4.8 หน้าจอการเพิ่มโครงการใหม่

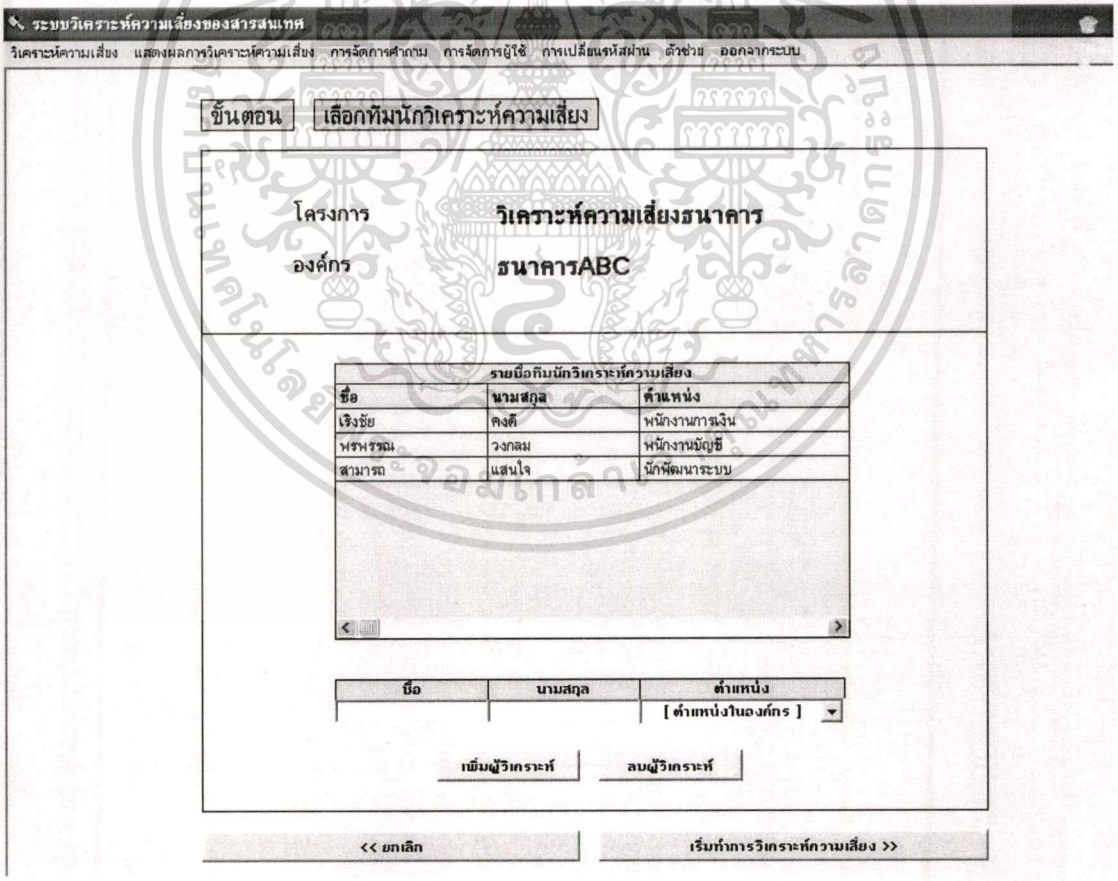


รูปที่ 4.9 ข้อความยืนยันการลบโครงการ

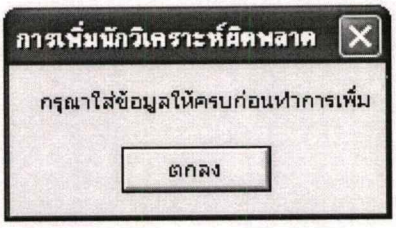
4.2.2 การจัดการทีมนักวิเคราะห์

เมื่อผู้ใช้คลิกเลือกโครงการที่จะทำการวิเคราะห์แล้ว ระบบจะแสดงหน้าจอการจัดการทีมนักวิเคราะห์ดังรูปที่ 4.10

กรณีต้องการเพิ่มรายชื่อนักวิเคราะห์เข้าทีม ผู้ใช้สามารถใส่ ชื่อ นามสกุล ตำแหน่งงาน แล้วคลิกปุ่มเพิ่มผู้วิเคราะห์ ถ้าใส่ข้อมูลไม่ครบระบบจะแสดงข้อความเตือนดังรูปที่ 4.11



รูปที่ 4.10 หน้าจอการจัดการทีมนักวิเคราะห์



รูปที่ 4.11 ข้อความเตือนให้ใส่ข้อมูลให้ครบก่อนคลิกปุ่มเพิ่มผู้วิเคราะห์

กรณีต้องการลบรายชื่อนักวิเคราะห์ออกจากทีม ผู้ใช้สามารถเลือกรายชื่อนักวิเคราะห์ที่ต้องการลบแล้วคลิกปุ่มลบ ระบบจะแสดงข้อความยืนยันการลบ เมื่อผู้ใช้ยืนยันระบบจะทำการลบรายชื่อนักวิเคราะห์ที่เลือกออกจากทีม

กรณีต้องการกลับไปหน้าการจัดการโครงการ ผู้ใช้สามารถคลิกปุ่มยกเลิกเพื่อกลับไปยังหน้าการจัดการโครงการได้

กรณีเลือกทีมนักวิเคราะห์เสร็จแล้ว ต้องการเริ่มวิเคราะห์ความเสี่ยง คลิกปุ่มเริ่มทำการวิเคราะห์ความเสี่ยง ระบบจะแสดงหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร ดังรูป 4.12

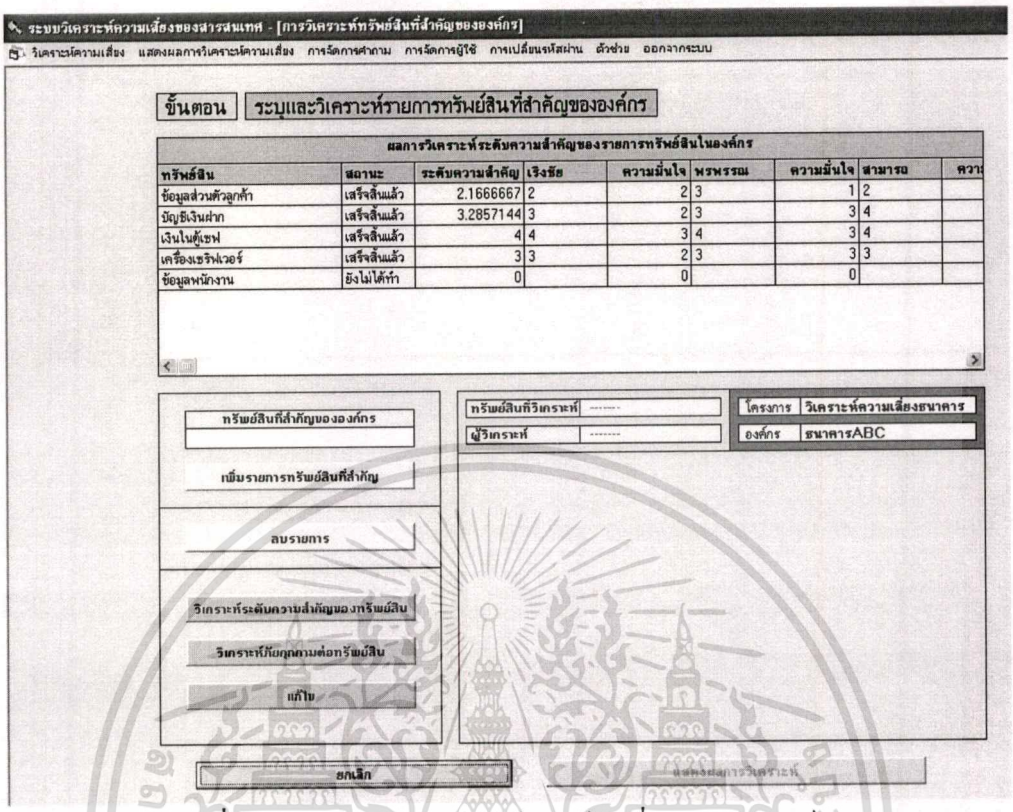
4.3.3 การวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร

ระบบแสดงหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร ดังรูป 4.12 ซึ่งหน้าจอนี้จะเป็นการเพิ่ม ลบและวิเคราะห์ระดับความสำคัญของทรัพย์สิน

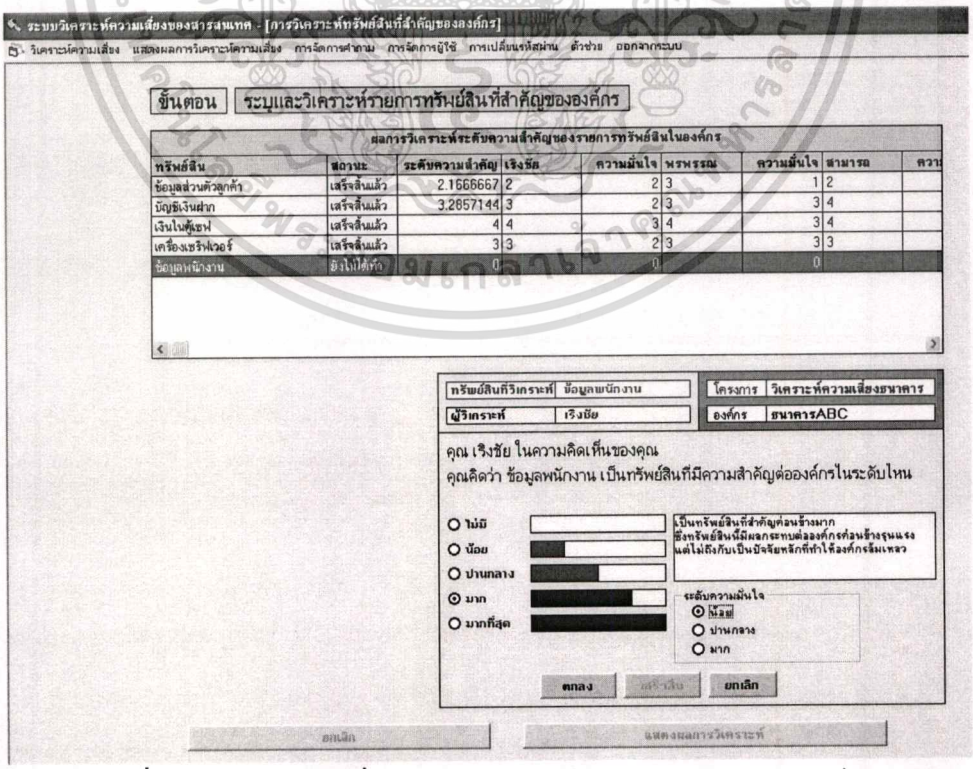
กรณีต้องการเพิ่มรายการทรัพย์สิน ผู้ใช้สามารถใส่รายการทรัพย์สิน แล้วคลิกปุ่มเพิ่มรายการทรัพย์สิน ถ้าใส่ข้อมูลไม่ครบระบบจะแสดงข้อความเตือนลักษณะเดียวกันกับรูป 4.11

กรณีต้องการลบรายการทรัพย์สิน ผู้ใช้สามารถเลือกรายการทรัพย์สินที่ต้องการลบแล้วคลิกปุ่มลบ ระบบจะแสดงข้อความยืนยันการลบ เมื่อผู้ใช้ยืนยัน ระบบจะทำการลบรายการทรัพย์สินที่เลือกออกไป

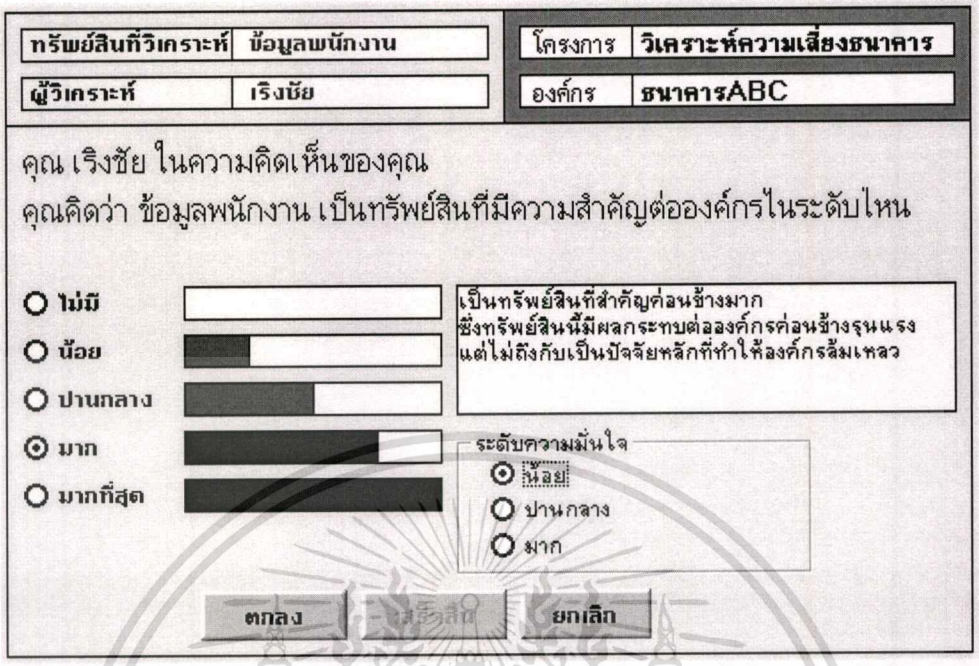
กรณีต้องการวิเคราะห์ระดับความสำคัญของทรัพย์สิน สามารถเลือกรายการทรัพย์สินที่ต้องการแล้วคลิกปุ่มวิเคราะห์ระดับความสำคัญของทรัพย์สิน ระบบจะแสดงหน้าจอดังรูป 4.13 ซึ่งให้นักวิเคราะห์แต่ละคนตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญทรัพย์สิน โดยจะให้มีการกำหนดระดับความมั่นใจในการตอบด้วย แสดงในรูป 4.14 เมื่อนักวิเคราะห์ตอบหมดทุกคนแล้วจะสามารถคลิกปุ่มเสร็จสิ้นได้ ระบบจะทำการหาค่าเฉลี่ยโดยมีการนำระดับความมั่นใจในการตอบมาคิดด้วย จากนั้นระบบจะอัพเดตสถานะและบันทึกข้อมูล



รูปที่ 4.12 หน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร



รูปที่ 4.13 หน้าจอการเมื่อคลิกปุ่มวิเคราะห์ระดับความสำคัญทรัพย์สิน



รูปที่ 4.14 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญทรัพย์สิน

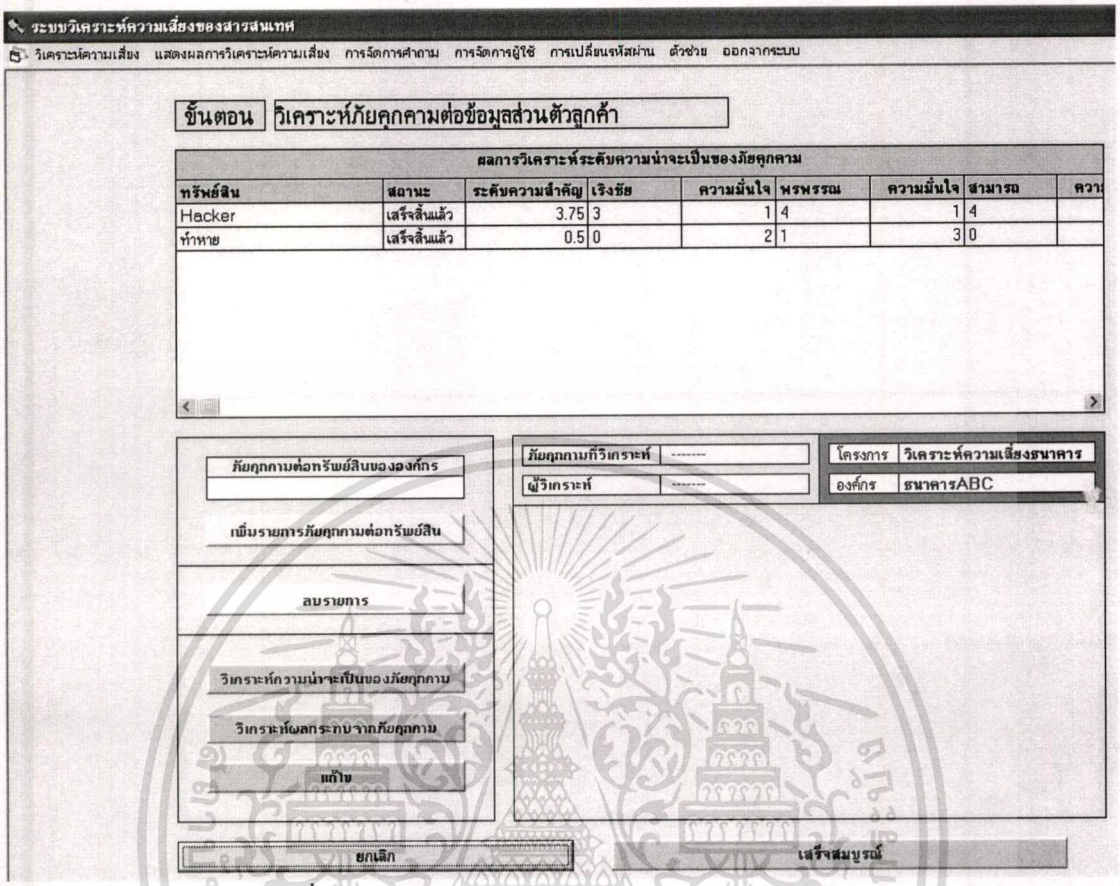
กรณีที่ทำการวิเคราะห์ระดับความสำคัญทรัพย์สินเสร็จแล้ว ต้องการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน สามารถเลือกรายการทรัพย์สินที่ต้องการแล้วคลิกปุ่มวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ระบบจะแสดงหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ดังรูป 4.15

4.3.4 การวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

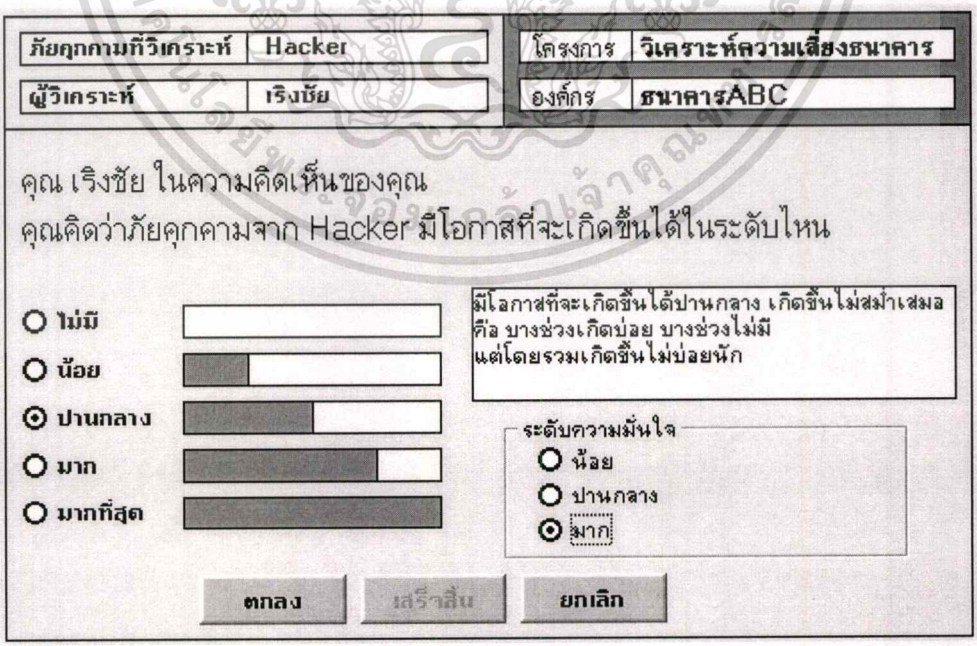
ระบบแสดงหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ดังรูป 4.15 ซึ่งหน้าจอนี้จะเป็นการเพิ่ม ลบและวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

กรณีต้องการวิเคราะห์ระดับโอกาสที่จะเกิดภัยคุกคาม สามารถเลือกรายการภัยคุกคามที่ต้องการแล้วคลิกปุ่มวิเคราะห์ความน่าจะเป็นของภัยคุกคาม ระบบจะแสดงหน้าจอดังรูป 4.16 ซึ่งให้นักวิเคราะห์แต่ละคนตอบคำถามเพื่อวิเคราะห์ระดับโอกาสที่จะเกิดภัยคุกคาม โดยจะให้มีการกำหนดระดับความมั่นใจในการตอบด้วย เมื่อนักวิเคราะห์ตอบหมดทุกคนแล้วจะสามารถคลิกปุ่มเสร็จสิ้นได้ ระบบจะทำการหาค่าเฉลี่ยโดยมีการนำระดับความมั่นใจในการตอบมาคิดด้วย จากนั้นระบบจะอัพเดตสถานะและบันทึกข้อมูล

กรณีต้องการเพิ่มหรือลบรายการภัยคุกคามต่อ ผู้ใช้สามารถกรอกรายการภัยคุกคามแล้วคลิกปุ่มเพิ่มเพื่อเพิ่มรายการ หรือเลือกภัยคุกคามที่ต้องการลบ แล้วคลิกปุ่มลบเพื่อลบรายการนั้น



รูปที่ 4.15 หน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน

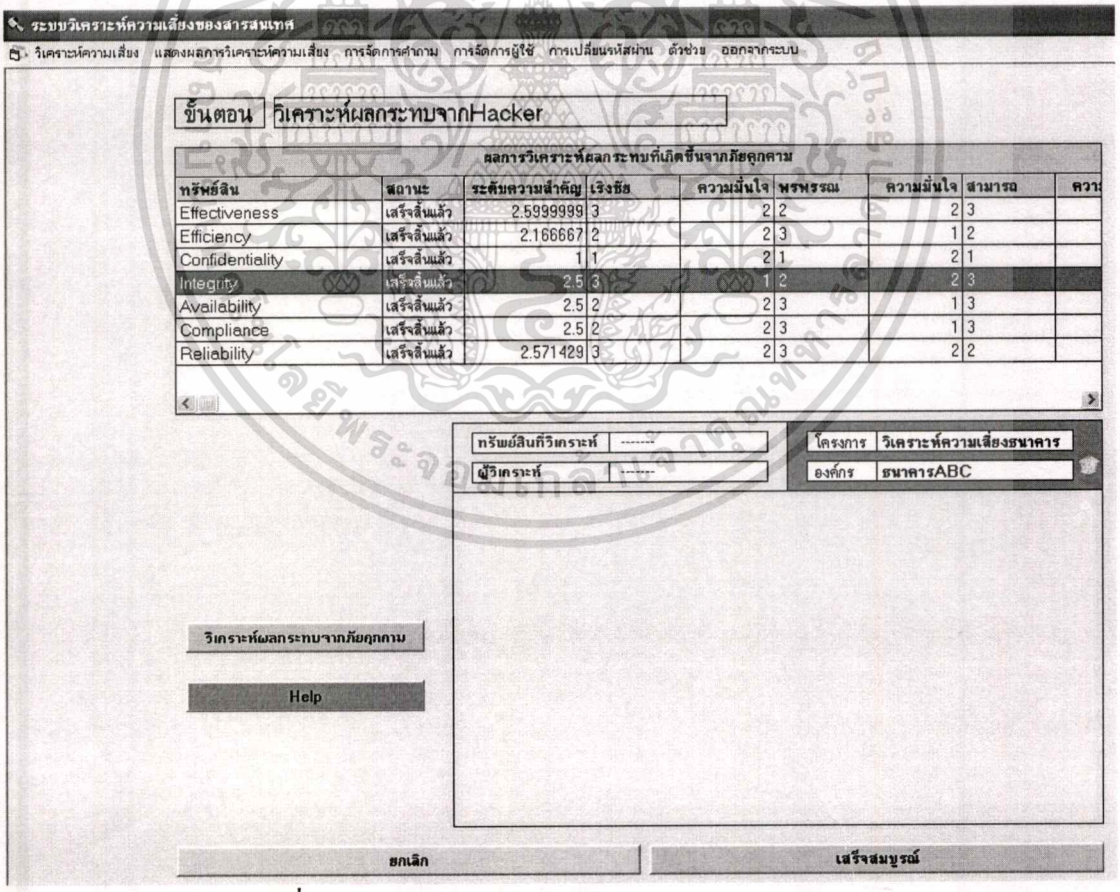


รูปที่ 4.16 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์โอกาสที่จะเกิดภัยคุกคาม

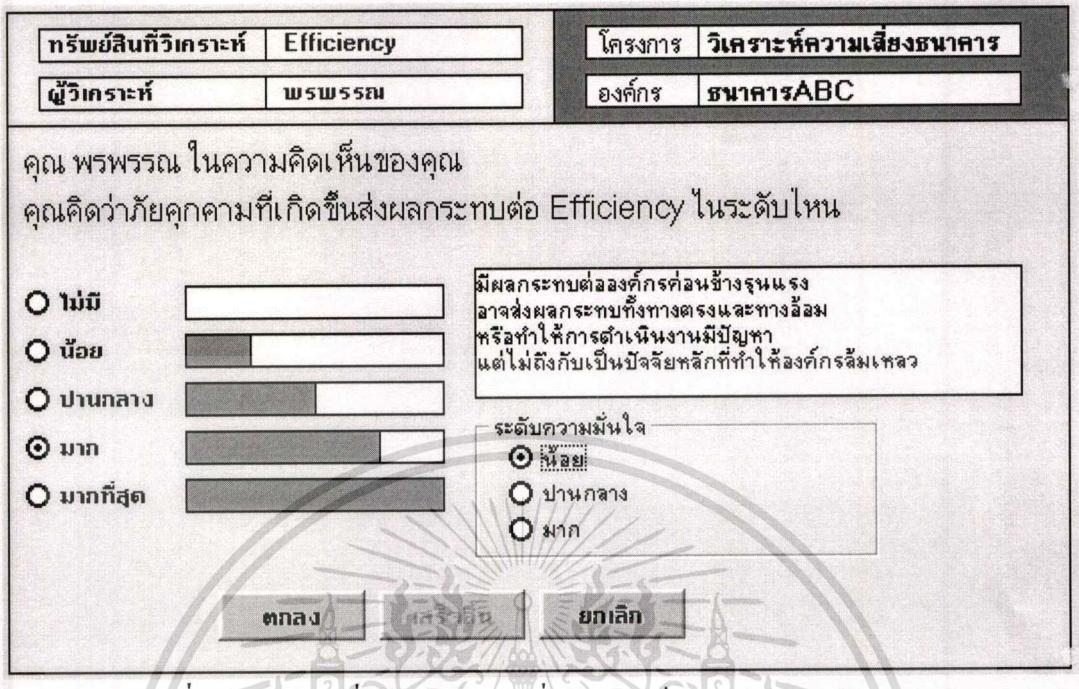
กรณีที่ทำการวิเคราะห์โอกาสที่จะเกิดภัยคุกคามเสร็จแล้ว ต้องการวิเคราะห์ผลกระทบจากภัยคุกคาม สามารถเลือกรายการภัยคุกคามที่ต้องการแล้วคลิกปุ่มวิเคราะห์ผลกระทบจากภัยคุกคาม ระบบจะแสดงหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม ดังรูป 4.17

4.3.5 การวิเคราะห์ผลกระทบจากภัยคุกคาม

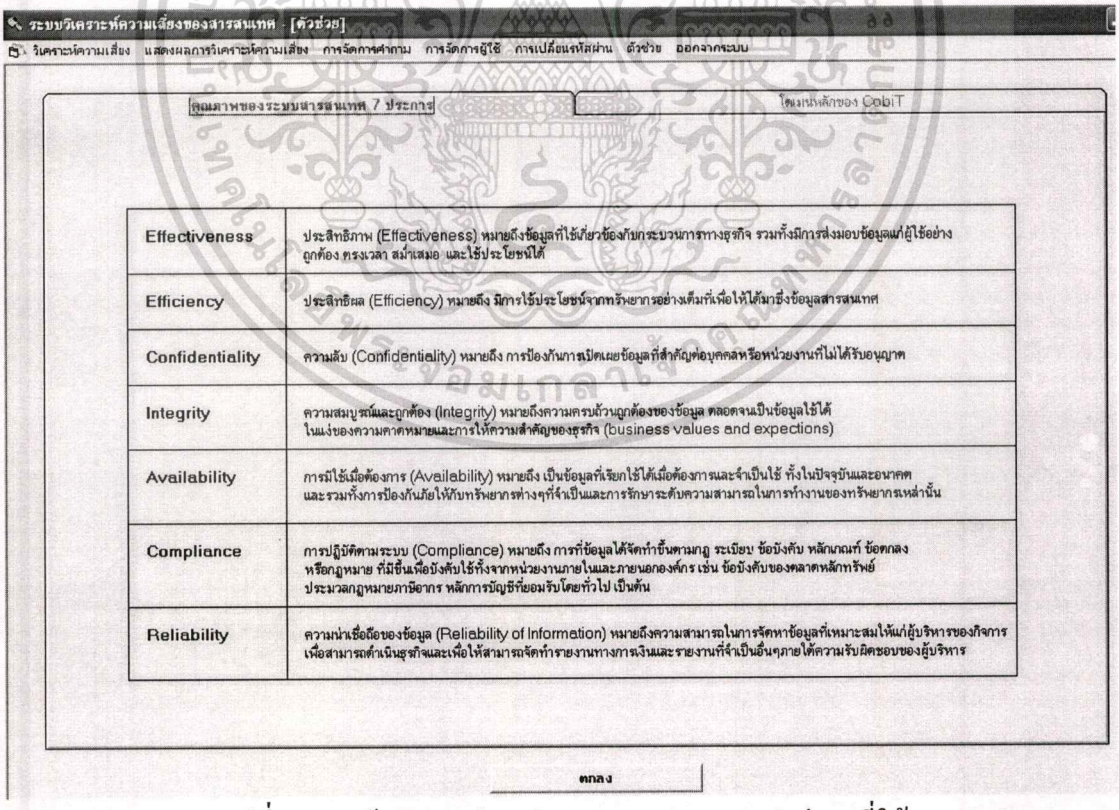
ระบบแสดงหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม ดังรูป 4.17 ซึ่งหน้าจอนี้จะเป็นการวิเคราะห์ผลกระทบจากภัยคุกคาม โดยเลือกรายการผลกระทบที่ต้องการแล้วคลิกปุ่มวิเคราะห์ผลกระทบจากภัยคุกคาม ระบบจะแสดงหน้าจอดังรูป 4.18 ซึ่งให้นักวิเคราะห์แต่ละคนตอบคำถามเพื่อวิเคราะห์ระดับความสำคัญทรัพย์สิน โดยจะให้มีการกำหนดระดับความมั่นใจในการตอบด้วย เมื่อนักวิเคราะห์ตอบหมดทุกคนแล้วจะสามารถคลิกปุ่มเสร็จสิ้นได้ ระบบจะทำการหาค่าเฉลี่ยโดยมีการนำระดับความมั่นใจในการตอบมาคิดด้วย จากนั้นระบบจะอัพเดตสถานะและบันทึกข้อมูล



รูปที่ 4.17 หน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม



รูปที่ 4.18 หน้าจอที่ใช้ตอบคำถามเพื่อวิเคราะห์ผลกระทบจากภัยคุกคาม



รูปที่ 4.19 หน้าจอการช่วยอธิบายความหมายของคำต่างๆที่ใช้

ในกรณีที่ผู้ใช้ต้องการคำแนะนำ สามารถคลิกที่เมนูตัวช่วยได้ตลอดเวลา ตัวอย่างคำอธิบายความหมายของคำที่ใช้แสดงดังรูปที่ 4.19

เมื่อนักวิเคราะห์ทำการตอบคำถามเกี่ยวกับผลกระทบจากภัยคุกคามเสร็จแต่ละรายการ สถานะจะถูกเปลี่ยนจาก "ยังไม่ได้ทำ" เป็น "เสร็จสิ้นแล้ว" ถ้าจนนักวิเคราะห์ทำเสร็จหมดทุกรายการแล้ว จะสามารถคลิกปุ่ม "เสร็จสิ้นสมบูรณ์" ได้ (ถ้ายังทำไม้เสร็จจะไม่สามารถคลิกได้)

เมื่อคลิก "ปุ่มเสร็จสิ้นสมบูรณ์" จากหน้าจอการวิเคราะห์ผลกระทบจากภัยคุกคาม ระบบจะทำการบันทึกค่าต่างๆ และกลับไปหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน จากนั้นระบบจะอัพเดทสถานะของรายการภัยคุกคามที่ถูกวิเคราะห์ผลกระทบแล้ว เปลี่ยนจาก "ยังไม่ได้ทำ" เป็น "เสร็จสิ้นแล้ว"

เมื่อวิเคราะห์ผลกระทบจากภัยคุกคามของแต่ละภัยคุกคามเสร็จแล้ว และวิเคราะห์โอกาสที่จะเกิดภัยคุกคามเสร็จแล้วทุกรายการ จะสามารถคลิกปุ่ม "เสร็จสิ้นสมบูรณ์" บนหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สินได้

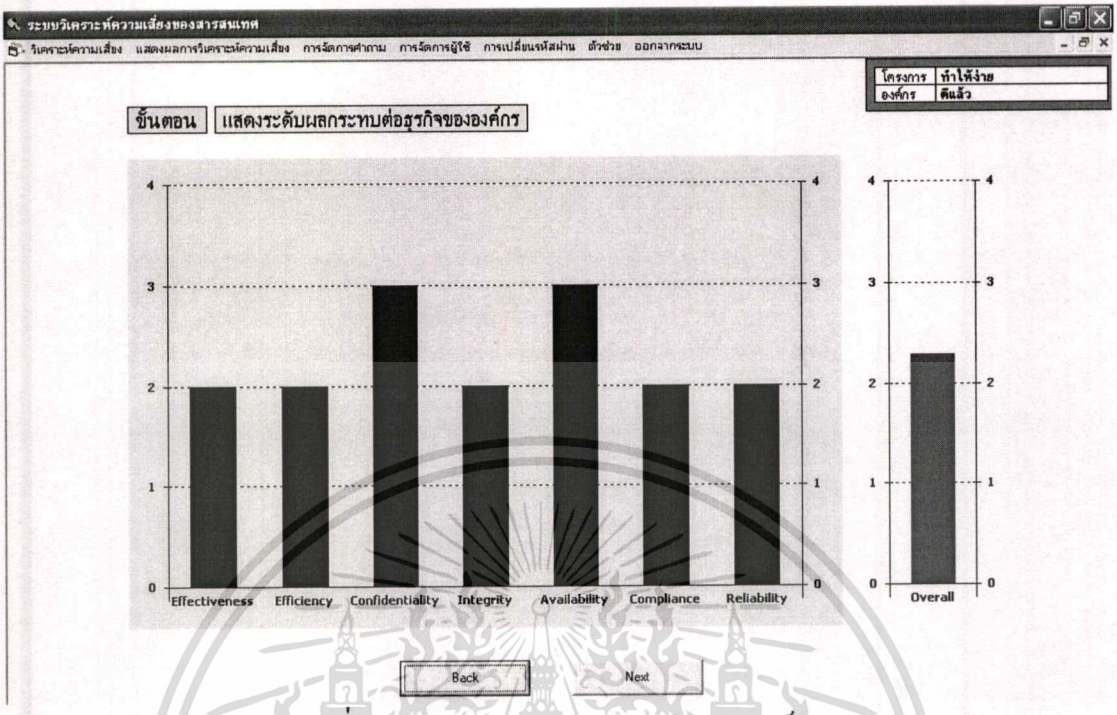
เมื่อคลิก "ปุ่มเสร็จสิ้นสมบูรณ์" จากหน้าจอการวิเคราะห์ภัยคุกคามต่อทรัพย์สิน ระบบจะทำการบันทึกค่าต่างๆ และกลับไปหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญ จากนั้นระบบจะอัพเดทสถานะของรายการทรัพย์สินที่ถูกวิเคราะห์ผลกระทบและภัยคุกคามแล้ว เปลี่ยนจาก "ยังไม่ได้ทำ" เป็น "เสร็จสิ้นแล้ว"

เมื่อวิเคราะห์ภัยคุกคามต่อทรัพย์สินเสร็จแล้ว และวิเคราะห์ระดับความสำคัญของทรัพย์สินเสร็จแล้วทุกรายการ จะสามารถคลิกปุ่ม "แสดงผลการวิเคราะห์" จากหน้าจอการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กรได้

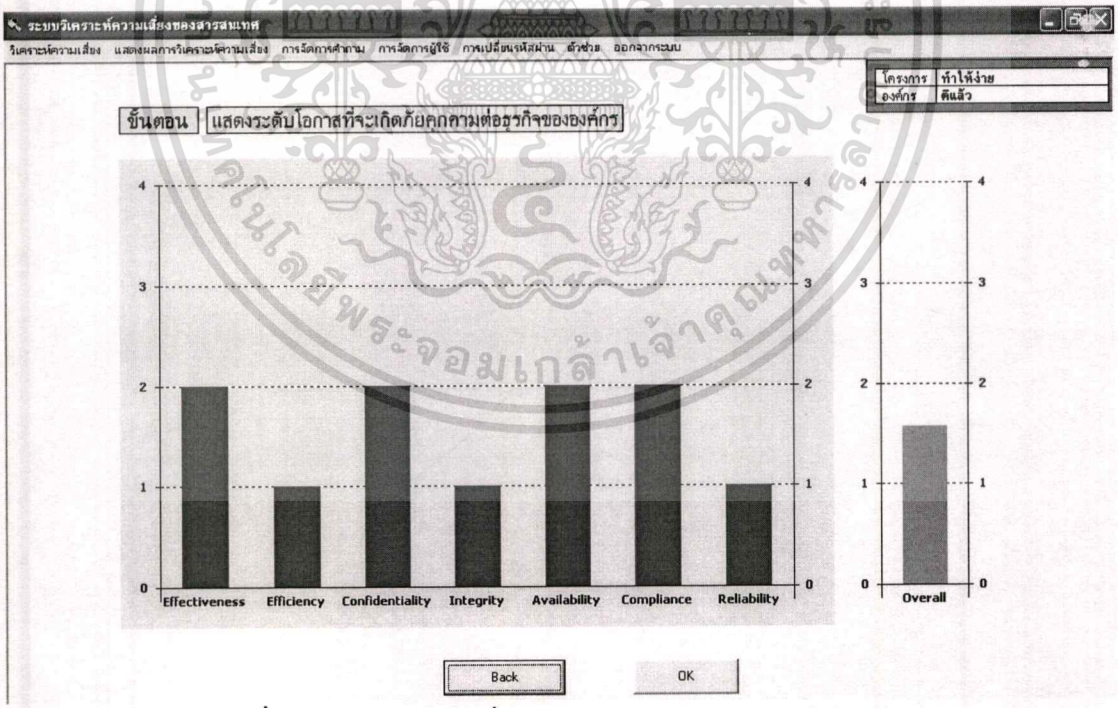
4.3.6 การวิเคราะห์ความเสี่ยงถาวร (Inherent Risk)

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

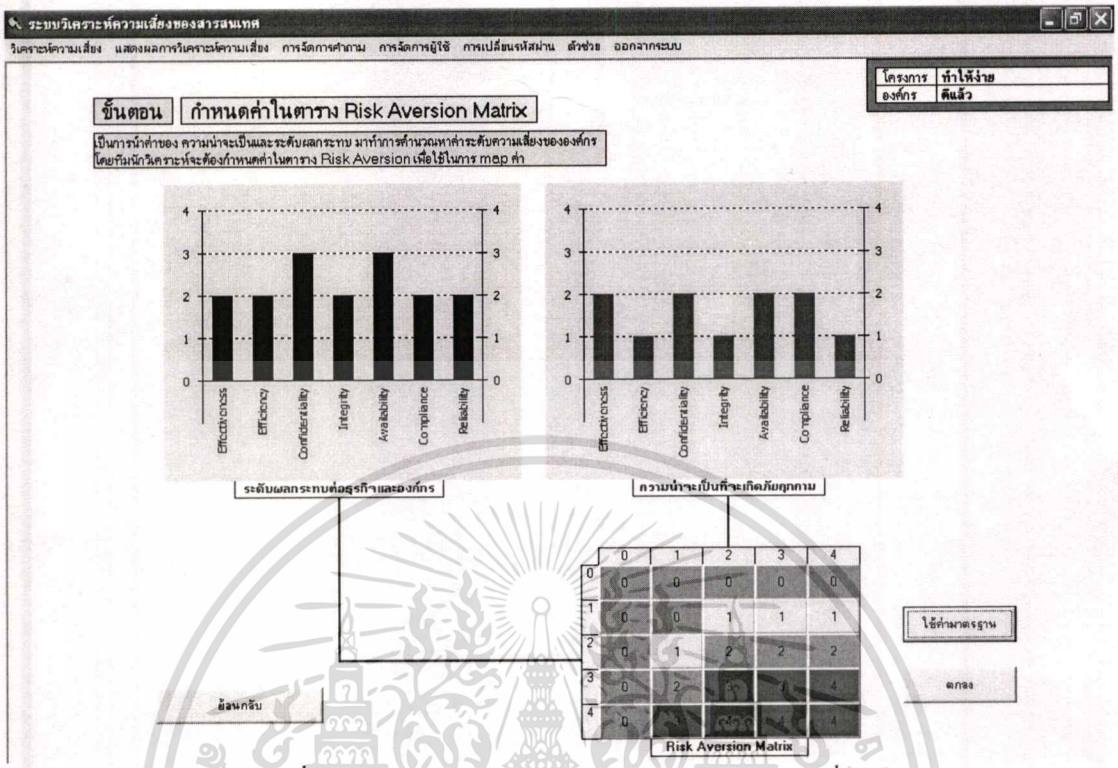
หลังจากนั้นระบบจะแสดงหน้าจอสำหรับกำหนดค่าในตารางที่ใช้คำนวณค่าความเสี่ยง (Risk Aversion Table) แสดงดังรูปที่ 4.22 เพื่อให้นักวิเคราะห์ทำการกำหนดค่าในตารางตามความเหมาะสม ถ้าไม่กำหนด ระบบจะใช้ค่ามาตรฐานในการคำนวณ จะได้ค่าความเสี่ยงดังรูปที่ 4.23



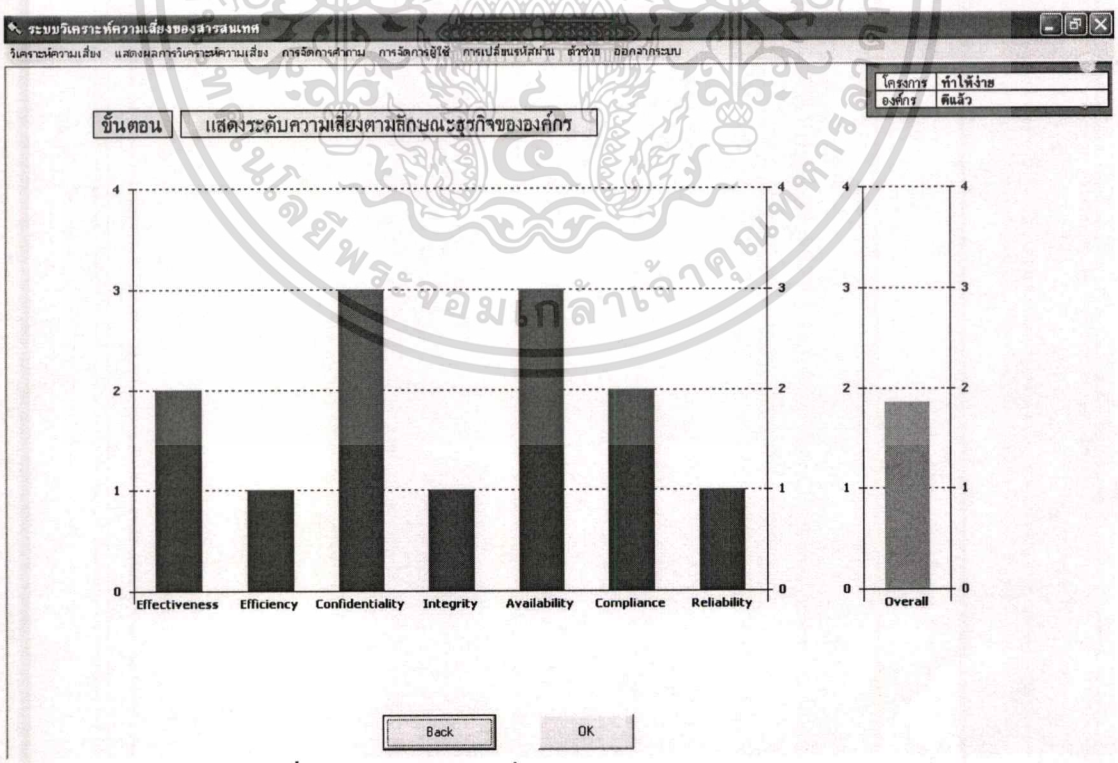
รูปที่ 4.20 ระดับผลกระทบต่อธุรกิจขององค์กร



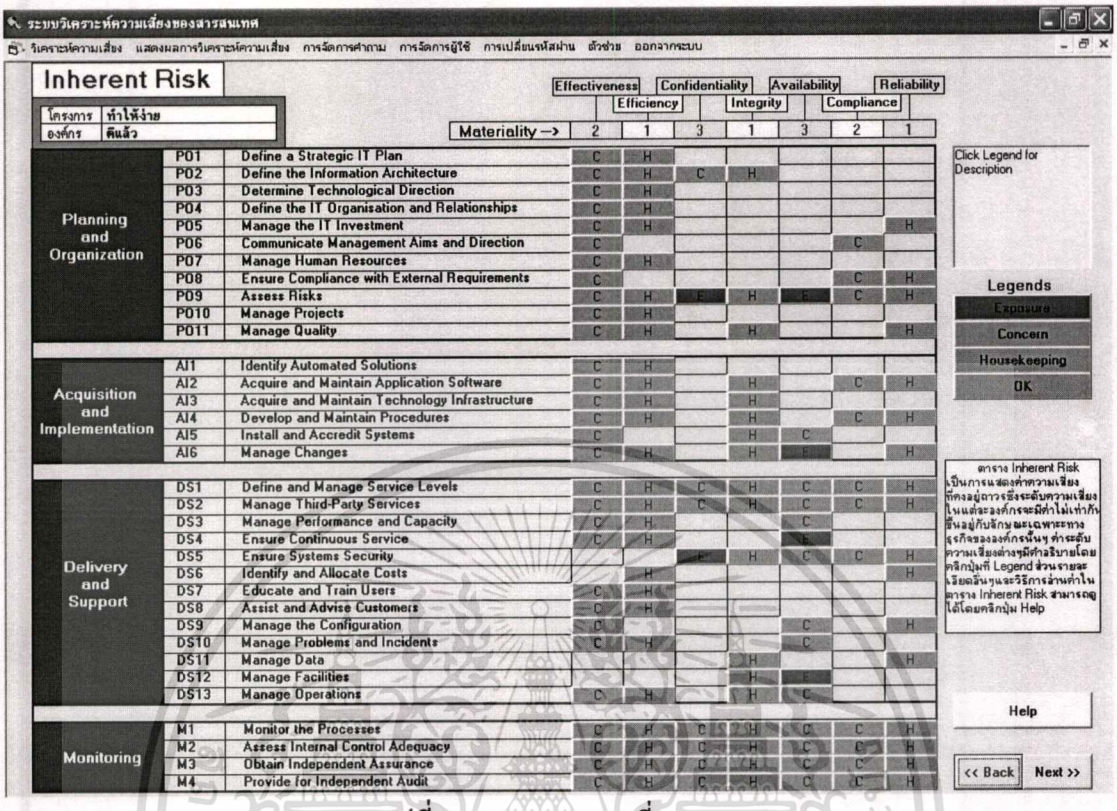
รูปที่ 4.21 ระดับโอกาสที่จะเกิดภัยคุกคามต่อธุรกิจขององค์กร



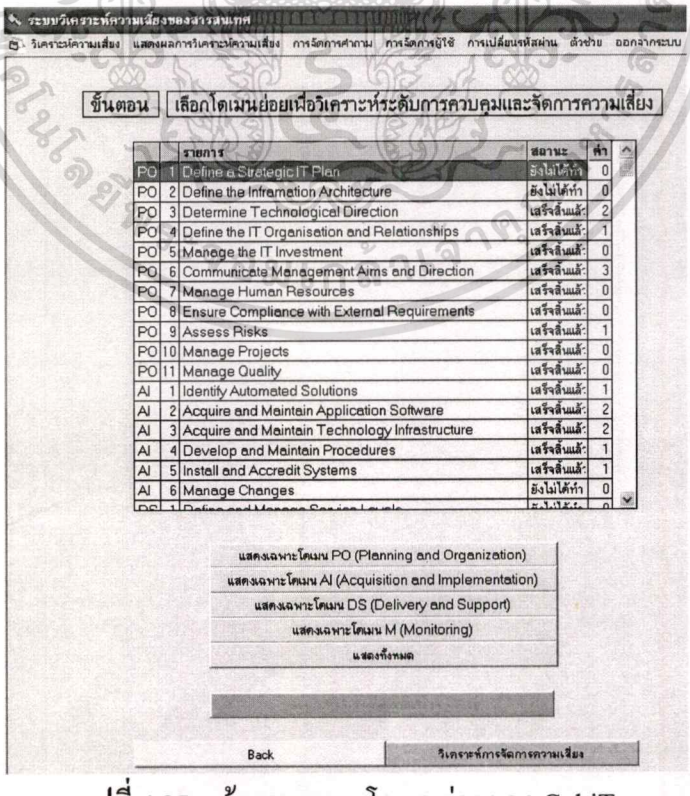
รูปที่ 4.22 ตารางกำหนดค่าในการคำนวณหาความเสี่ยง



รูปที่ 4.23 ระดับความเสี่ยงตามลักษณะธุรกิจขององค์กร



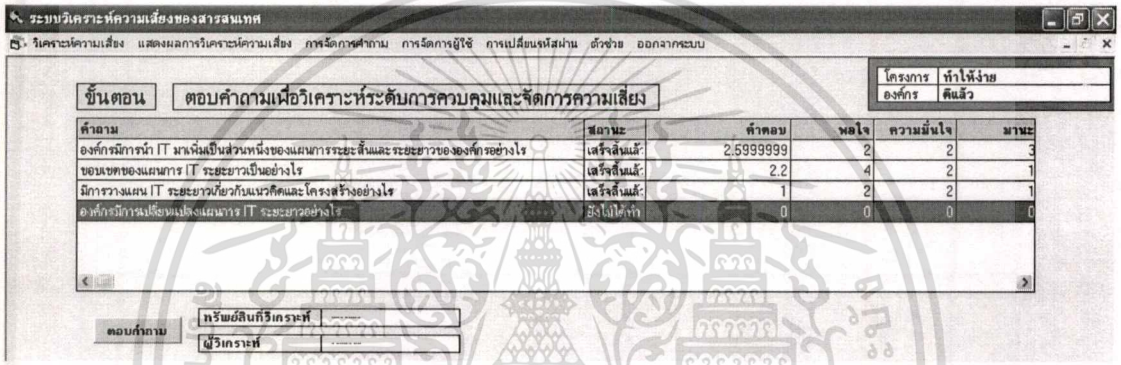
รูปที่ 4.24 ตารางความเสี่ยงถาวร



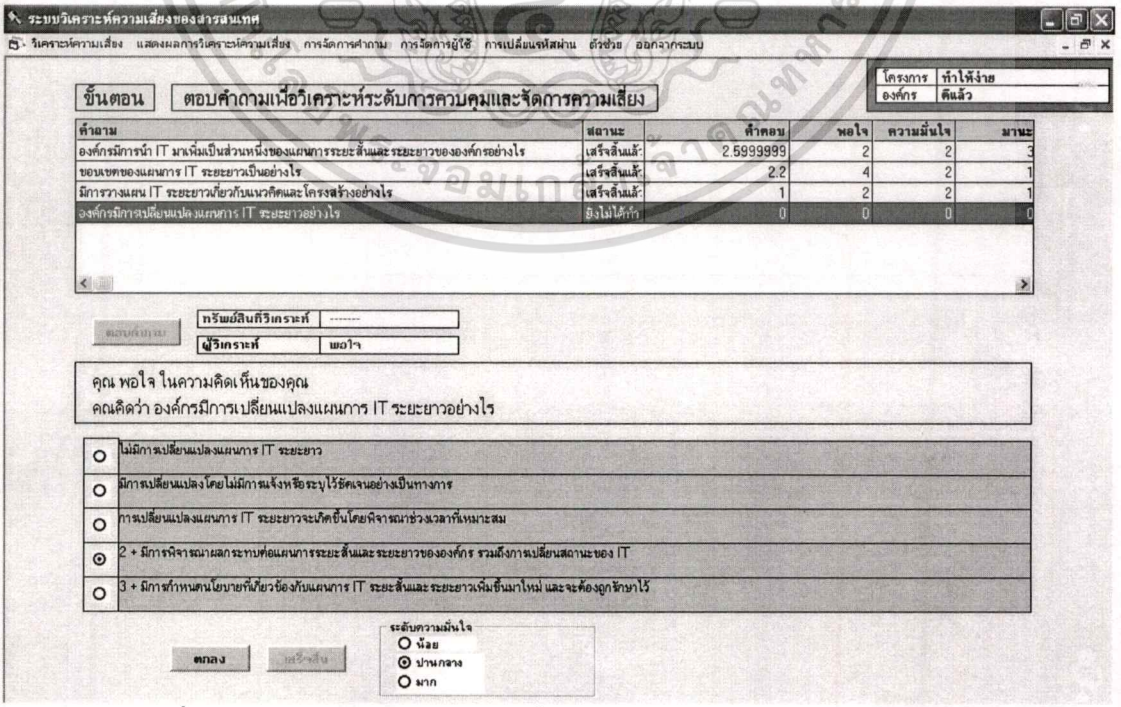
รูปที่ 4.25 หน้าจอรายการโดเมนย่อยของ CobiT

ระบบทำการนำค่าระดับความเสี่ยงที่คำนวณได้มาแสดงในตารางความเสี่ยงถาวรในรูปที่ 4.24 โดยเป็นความเสี่ยงที่เกิดขึ้นตามลักษณะธุรกิจขององค์กรนั้น ยังไม่มีการควบคุมจัดการใดๆ ถ้าต้องการวิเคราะห์ต่อ คลิกปุ่ม Next ระบบจะแสดงหน้าจอโดเมนย่อยของ CobiT ดังรูปที่ 4.25 จากนั้นผู้วิเคราะห์สามารถเลือกโดเมนย่อยแล้วคลิกปุ่มการจัดการความเสี่ยงเพื่อทำการวิเคราะห์ได้

จากนั้นระบบจะแสดงหน้าจอการวิเคราะห์การจัดการความเสี่ยงดังรูปที่ 4.26 นักวิเคราะห์สามารถเลือกตอบคำถามจากรายการได้โดยคลิกปุ่มตอบคำถาม ระบบจะแสดงหน้าจอดังรูปที่ 4.27

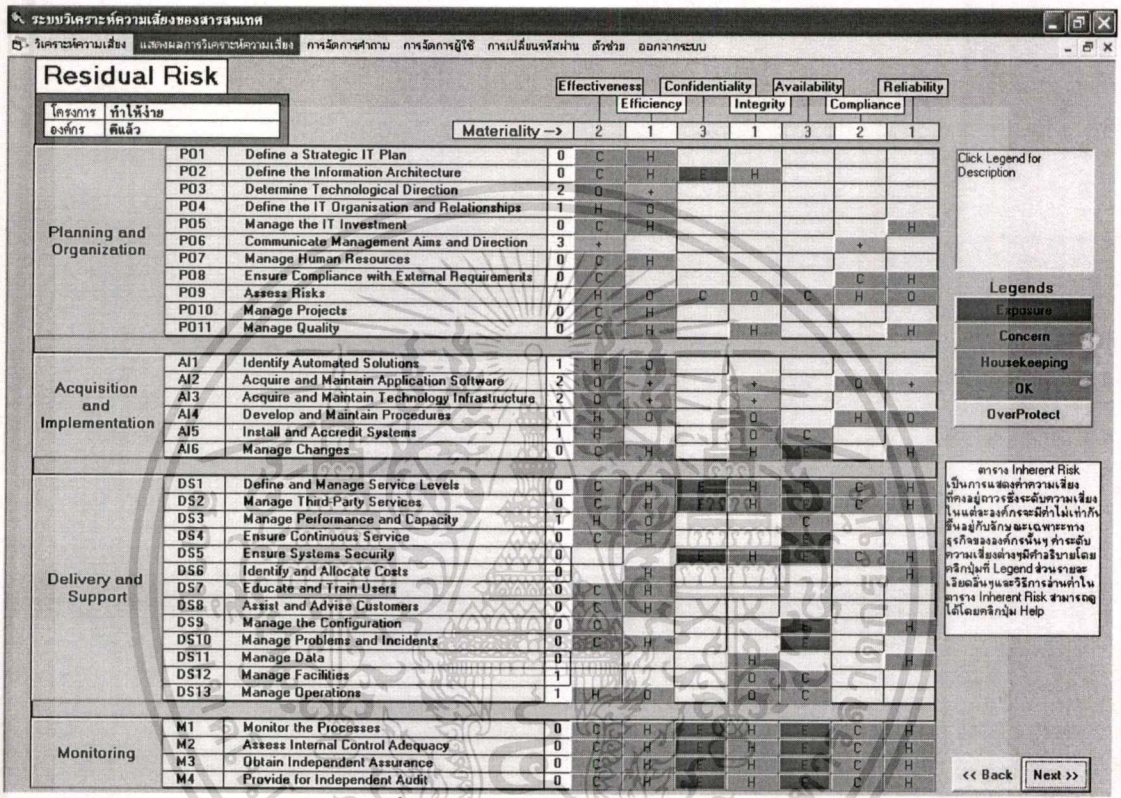


รูปที่ 4.26 หน้าจอการวิเคราะห์การจัดการความเสี่ยง

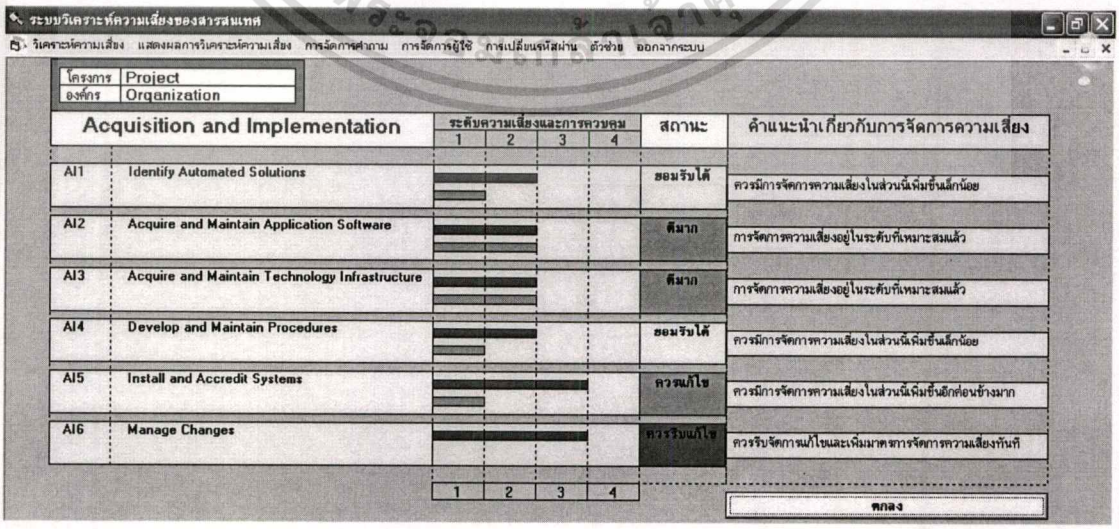


รูปที่ 4.27 นักวิเคราะห์ตอบคำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง

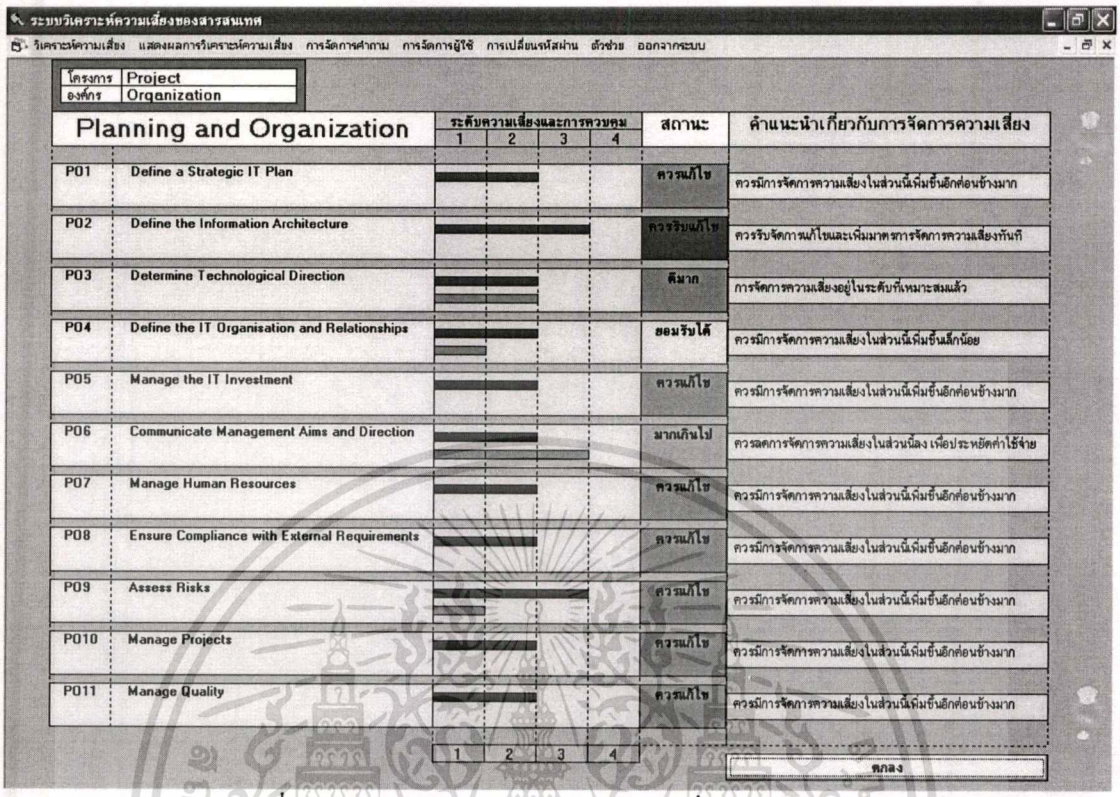
เมื่อนักวิเคราะห์ตอบคำถามหมดแล้ว ระบบจะทำการอัพเดทสถานะจากจาก “ยังไม่ได้ทำ” เป็น “เสร็จสิ้นแล้ว” และจะสามารถคลิกปุ่มแสดงความเสี่ยงที่เหลืออยู่ได้ หลังจากคลิกปุ่มแสดงความเสี่ยงที่เหลือ ระบบจะแสดงหน้าจอตารางความเสี่ยงที่เหลืออยู่ดังรูปที่ 4.28



รูปที่ 4.28 ตารางความเสี่ยงที่เหลืออยู่



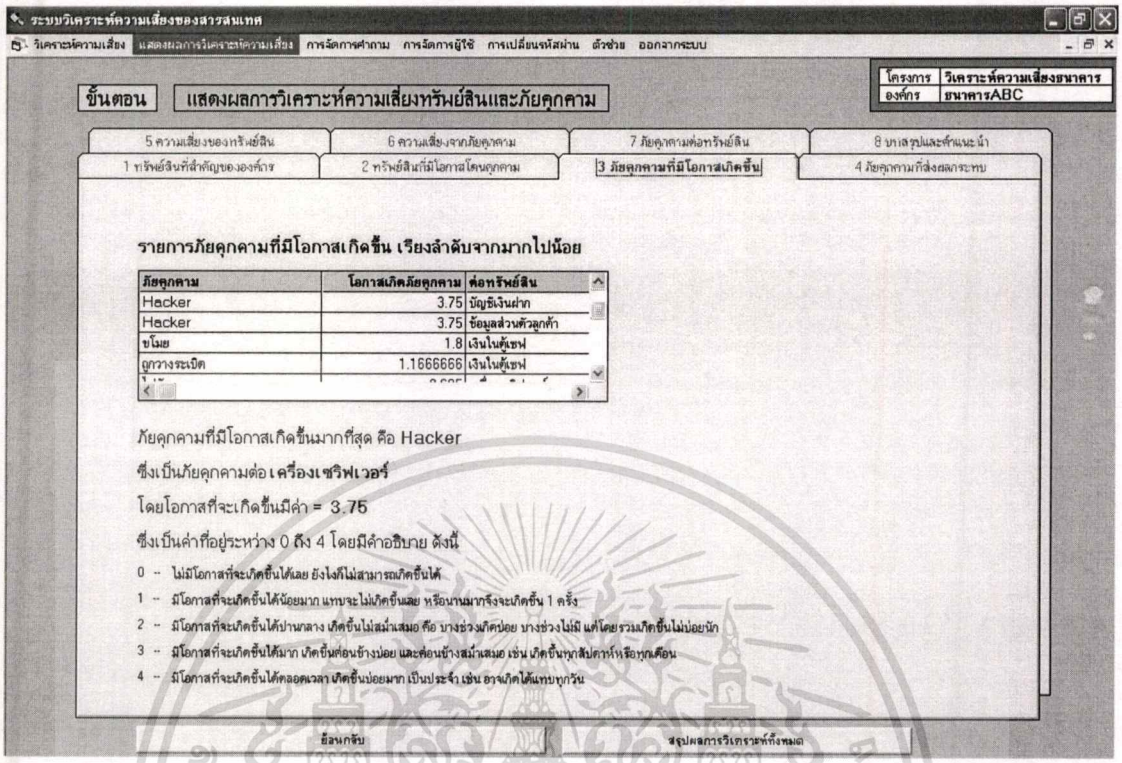
รูปที่ 4.29 คำแนะนำในการจัดการความเสี่ยงในโดเมน AI



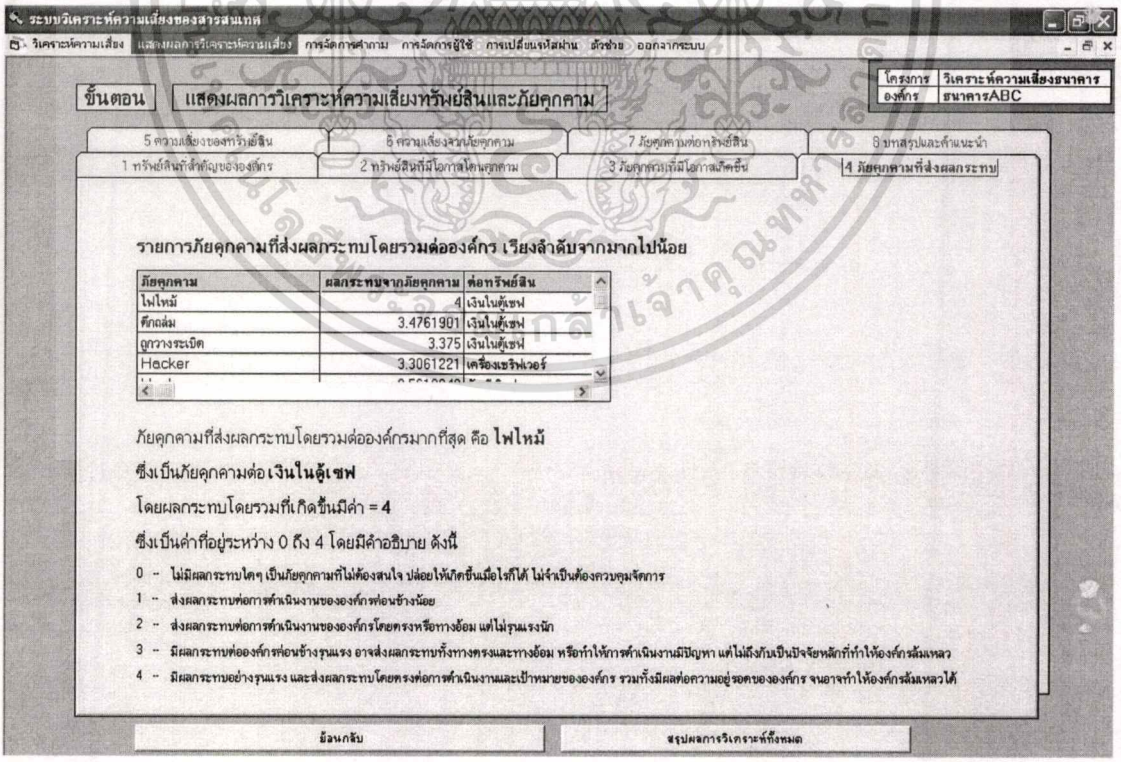
รูปที่ 4.30 คำแนะนำในการจัดการความเสี่ยงในโดเมน PO

จากหน้าจอตารางความเสี่ยงที่เหลืออยู่ดังรูปที่ 4.28 จะสังเกตได้ว่าค่าระดับความเสี่ยงที่อยู่ในตารางความเสี่ยงที่คงอยู่ (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

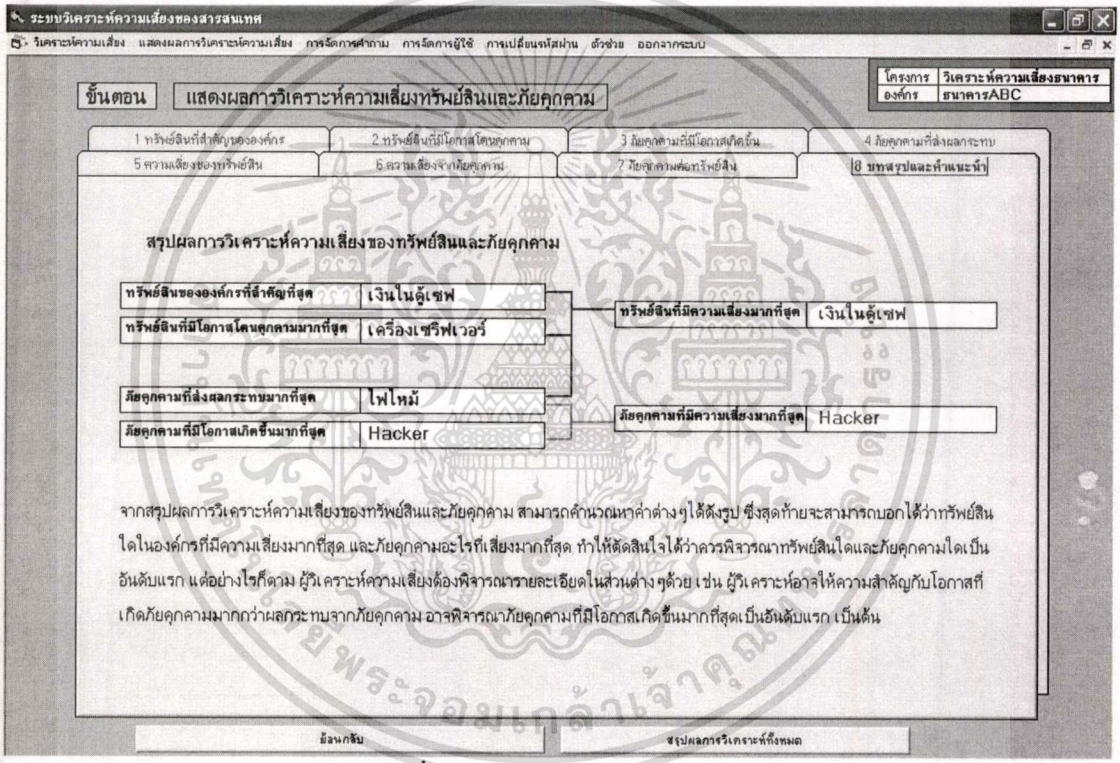


รูปที่ 4.31 ภัยคุกคามที่มีโอกาสเกิดขึ้นมากที่สุด



รูปที่ 4.32 ภัยคุกคามที่ส่งผลกระทบมากที่สุด

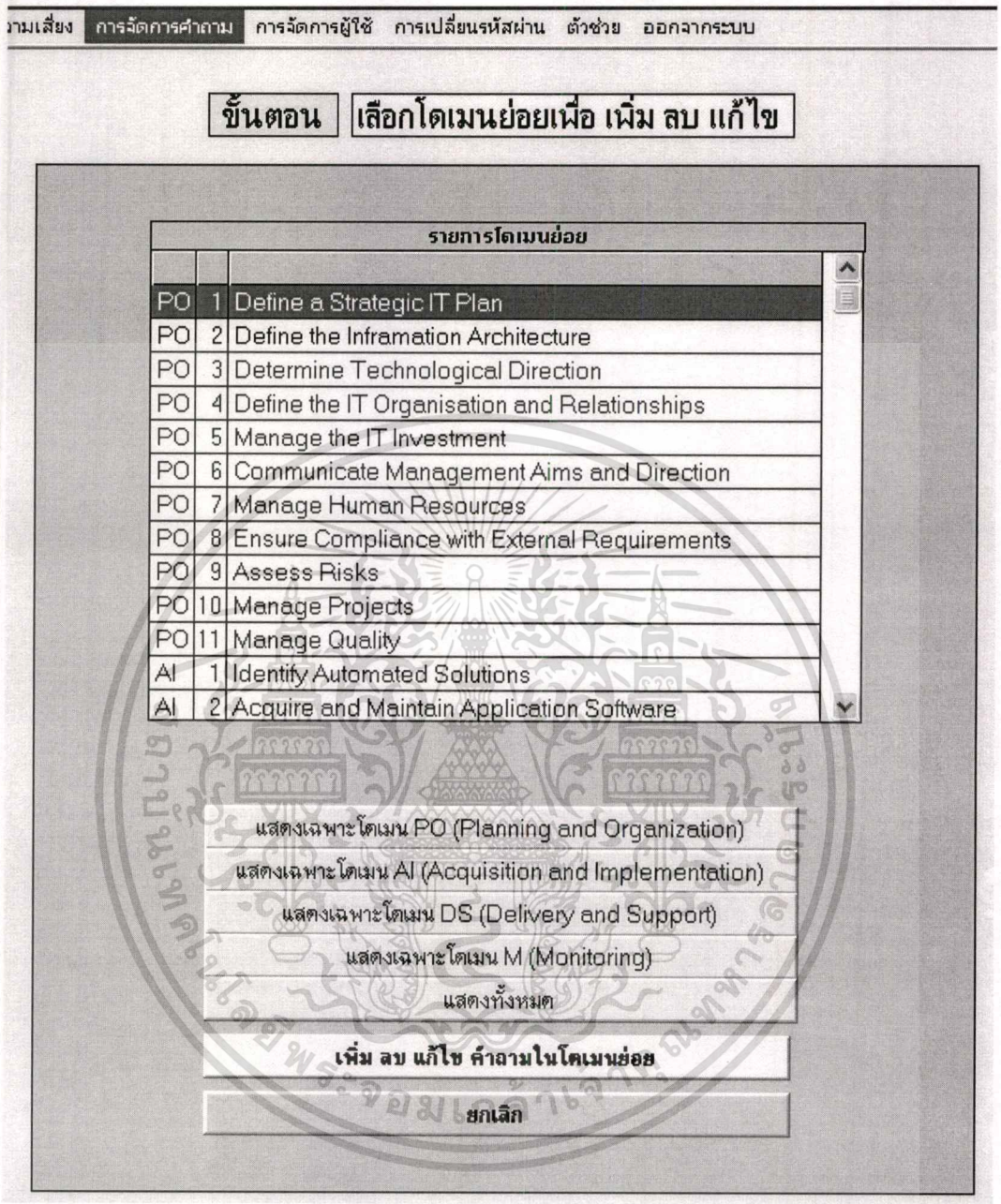
ส่วนสุดท้ายเป็นหน้าจอแสดงผลการวิเคราะห์ทรัพย์สินที่สำคัญขององค์กรและภัยคุกคามต่อทรัพย์สิน โดยวิเคราะห์เป็น 6 ส่วน คือ ความสำคัญของทรัพย์สิน ทรัพย์สินที่มีโอกาสโดนคุกคาม ภัยคุกคามที่มีโอกาสเกิดขึ้น ภัยคุกคามที่ส่งผลกระทบ ความเสี่ยงของทรัพย์สิน ความเสี่ยงจากภัยคุกคาม โดยรูปที่ 4.31 แสดงภัยคุกคามที่มีโอกาสเกิดขึ้นเรียงจากมากไปน้อย ส่วนรูปที่ 4.32 แสดงภัยคุกคามที่ส่งผลกระทบเรียงจากมากไปน้อย ส่วนรูปที่ 4.33 เป็นบทสรุปและคำแนะนำซึ่งจะช่วยให้นักวิเคราะห์ความเสี่ยงเห็นภาพรวมมากขึ้น ส่วนรายละเอียดในส่วนต่างๆ สามารถคลิกแท็บต่างๆ ดูได้



รูปที่ 4.33 บทสรุปและคำแนะนำ

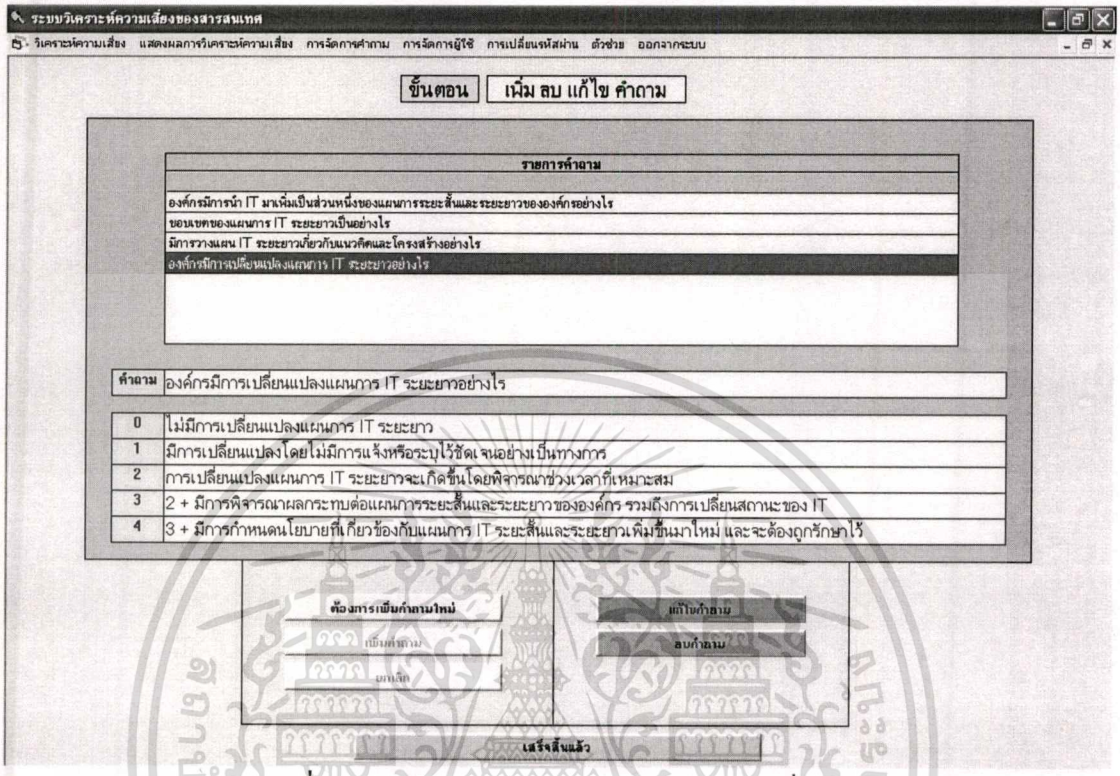
4.4 การจัดการคำถามเกี่ยวกับการควบคุมและจัดการความเสี่ยง

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มการจัดการคำถามหรือคลิกการจัดการคำถามที่เมนูข้างบน หลังจากนั้นระบบจะแสดงหน้าจอการจัดการคำถามดังรูปที่ 4.34 ซึ่งจะเป็นการแสดงรายการโดเมนย่อยของ CobiT ทั้งหมด ซึ่งสามารถเลือกให้แสดงรายการในแต่ละโดเมนได้ เช่น คลิกปุ่มแสดงเฉพาะโดเมน PO จะแสดงแสดงเฉพาะโดเมน PO เป็นต้น



รูปที่ 4.34 หน้าจอการจัดการคำถาม

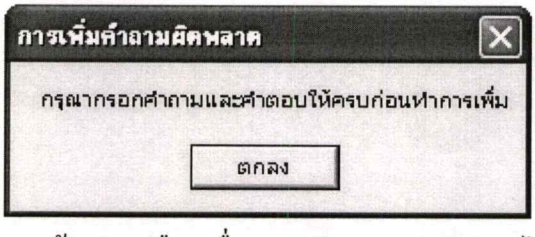
จากหน้าจอการจัดการคำถาม กรณีที่ผู้ดูแลระบบต้องการ เพิ่ม ลบ แก้ไข คำถามในโดเมนย่อย สามารถเลือกรายการโดเมนย่อย แล้วคลิกปุ่มต้องการ เพิ่ม ลบ แก้ไข คำถามในโดเมนย่อย ระบบจะแสดงหน้าจอรายการคำถามในโดเมนย่อยที่เลือก ดังรูปที่ 4.35 และสามารถเลือกคำถามที่ต้องการแก้ไข และคลิกปุ่มแก้ไข เพื่อแก้ไขได้ดังรูปที่ 4.36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



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 คำถามและคำตอบต้องการจะแก้ไข



รูปที่ 4.37 ข้อความเตือนเมื่อกรอกคำถามและคำตอบไม่ครบ

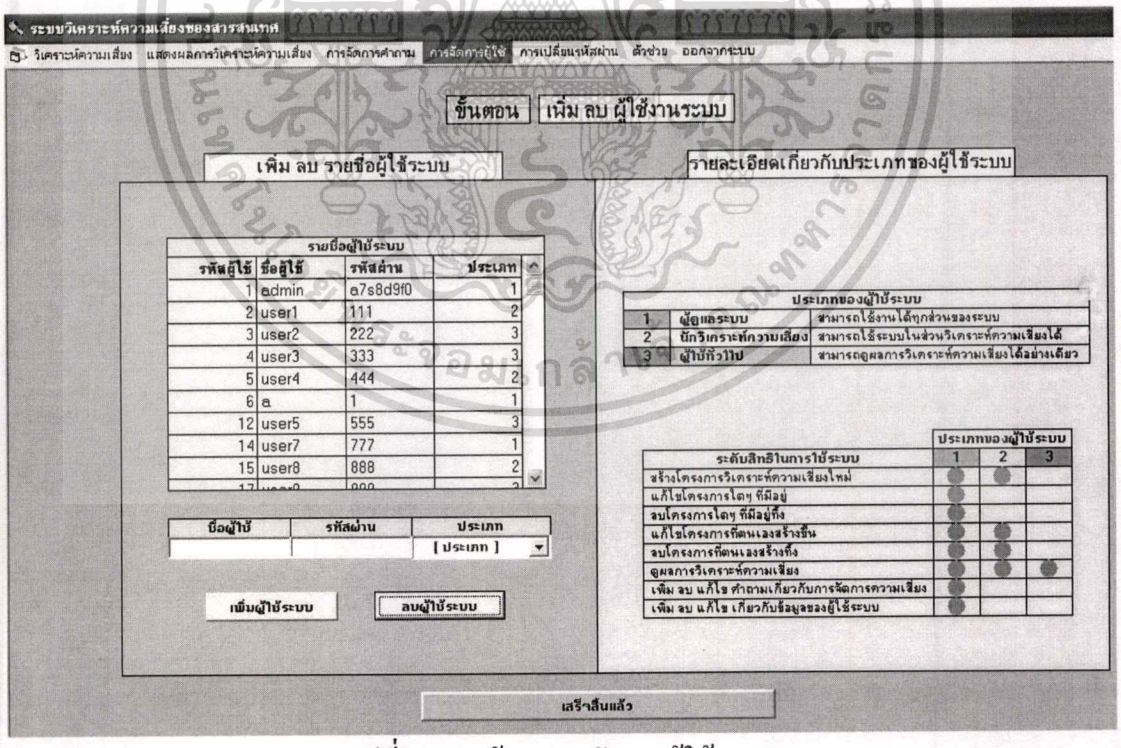
4.5 การจัดการผู้ใช้ระบบ

จากหน้าจอหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ คลิกปุ่มการจัดการผู้ใช้ระบบหรือคลิกการจัดการผู้ใช้ที่เมนูข้างบน โดยผู้ดูแลระบบเท่านั้นที่มีสิทธิในการเข้าใช้ส่วนนี้ หลังจากนั้นระบบจะแสดงหน้าจอการจัดการผู้ใช้ระบบดังรูปที่ 4.38 ซึ่งจะเป็นการแสดงรายการผู้ใช้ระบบทั้งหมด

กรณีต้องการเพิ่มรายการผู้ใช้ระบบ ผู้ดูแลระบบสามารถกรอกข้อมูลผู้ใช้ระบบ แล้วคลิกปุ่มเพิ่มผู้ใช้ระบบ ถ้าใส่ข้อมูลไม่ครบระบบจะแสดงข้อความเตือนลักษณะเดียวกันกับรูป 4.37

กรณีต้องการลบรายการผู้ใช้ระบบ ผู้ดูแลระบบสามารถเลือกรายการผู้ใช้ระบบที่ต้องการลบแล้วคลิกปุ่มลบผู้ใช้ระบบ ระบบจะแสดงข้อความยืนยันการลบ เมื่อผู้ใช้ยืนยัน ระบบจะทำการลบรายการผู้ใช้ระบบ ที่เลือกออกไป

ประเภทของผู้ใช้ระบบแบ่งออกเป็น 3 ประเภท คือ ผู้ดูแลระบบ นักวิเคราะห์ระบบ และผู้ใช้ทั่วไป โดยผู้ใช้แต่ละประเภทมีสิทธิในการใช้ระบบไม่เท่ากัน โดยรายละเอียดเกี่ยวกับผู้ใช้ระบบแสดงไว้ด้านซ้ายของหน้าจอการจัดการผู้ใช้ระบบ ดังรูปที่ 4.39

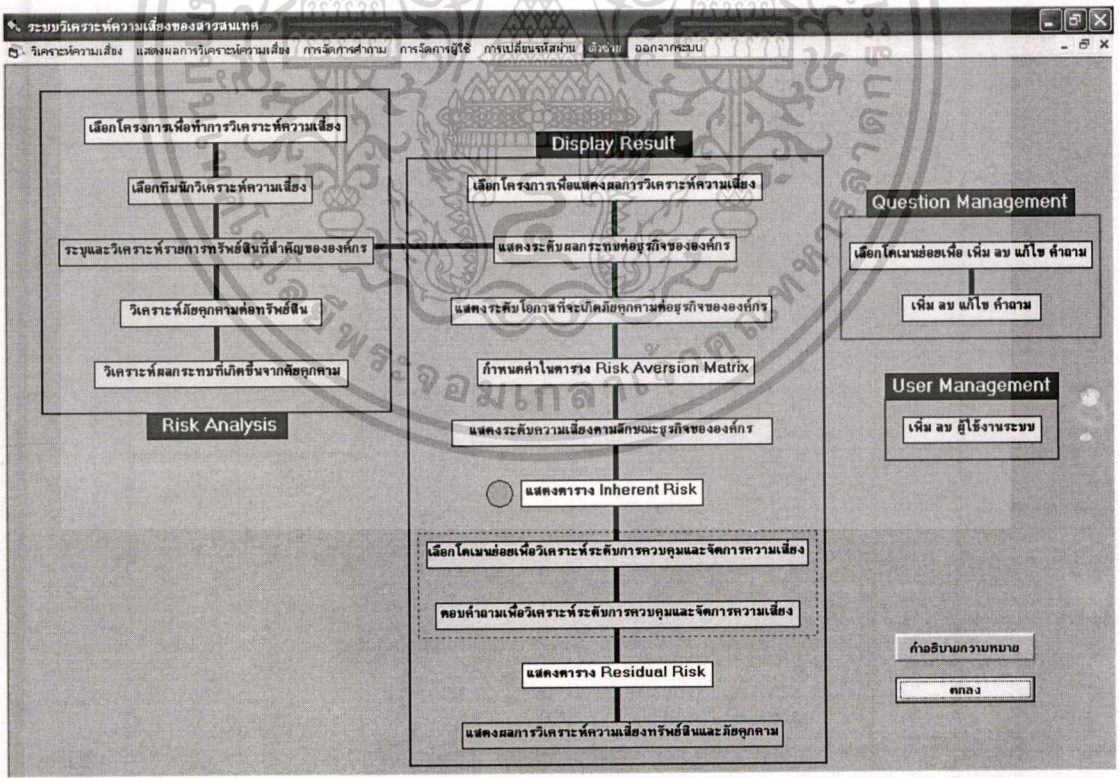


รูปที่ 4.38 หน้าจอการจัดการผู้ใช้ระบบ

ประเภทของผู้ใช้ระบบ		
1	ผู้ดูแลระบบ	สามารถใช้งานได้ทุกส่วนของระบบ
2	นักวิเคราะห์ความเสี่ยง	สามารถใช้ระบบในส่วนวิเคราะห์ความเสี่ยงได้
3	ผู้ใช้ทั่วไป	สามารถดูผลการวิเคราะห์ความเสี่ยงได้อย่างเดียว

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

รูปที่ 4.39 รายละเอียดเกี่ยวกับผู้ใช้ระบบ



รูปที่ 4.40 หน้าจอแสดงสถานะการใช้งานระบบ

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

บทที่ 5
การพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

5.1 รูปแบบการพัฒนาระบบและวิธีการคำนวณที่ใช้ในการวิเคราะห์ความเสี่ยง

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศ ได้ทำการพัฒนาเป็น Window GUI แอพพลิเคชัน (วินโดว์สฟอร์ม) หรือโปรแกรมที่ทำงานบนไมโครซอฟต์วินโดว์ส โดยมี RiskAnalysis.exe เป็นโปรแกรมหลักของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ

การพัฒนาระบบวิเคราะห์ความเสี่ยงของสารสนเทศใช้โปรแกรม Visual Bisic ในการพัฒนาและใช้ Microsoft Access เป็นระบบจัดการฐานข้อมูล โดยมีการนำแนวคิดการวิเคราะห์ความเสี่ยงต่างๆ มาประยุกต์ใช้เพื่อเป็นแนวทางในการพัฒนา

กระบวนการทำงานของระบบในการวิเคราะห์ความเสี่ยงจะประกอบด้วยการวิเคราะห์ที่สำคัญดังนี้

5.1.1 การวิเคราะห์ทรัพย์สินที่สำคัญขององค์กร

เป็นการวิเคราะห์ว่าในองค์กรมีทรัพย์สินอะไรบ้าง และทรัพย์สินแต่ละรายการมีระดับความสำคัญแค่ไหนและมีภัยคุกคามอะไรบ้าง โดยมีกระบวนการทำงานดังนี้

1. ทีมนักวิเคราะห์กำหนดทรัพย์สินที่สำคัญขององค์กร
2. วิเคราะห์ระดับความสำคัญของทรัพย์สิน ดังนี้

$$AssetValue = [(Analyst1 \times Credit1) + (Analyst2 \times Credit2) + \ldots + (AnalystN \times CreditN)] / [Credit1 + Credit2 + \ldots + CreditN]$$

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

Likelihood = [(Analyst1 x Credit1) + (Analyst2 x Credit2) +...+ (AnalystN x CreditN)] / [Credit1 + Credit2 +...+ 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

เป็นการวิเคราะห์ว่าภัยคุกคามส่งผลกระทบต่อการดำเนินงานขององค์กรในระดับไหน โดยมีกระบวนการทำงานดังนี้

วิเคราะห์ระดับผลกระทบจากภัยคุกคาม ดังนี้

ImpactValue = [(Analyst1 x Credit1) + (Analyst2 x Credit2) +...+ (AnalystN x CreditN)] / [Credit1 + Credit2 +...+ 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

AssetImpact = (ImpactValue1 + ImpactValue2 +...+ ImpactValueN) / (TotalThreat)

BusinessImpact = [(AssetImpact1 x AssetValue1) +...+ (AssetImpactN x AssetValueN)] / [AssetValue1 + AssetValue2 +...+ 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

BusinessLikelihood = [(Likelihood1 x ImpactValue1) +...+(LikelihoodN x ImpactValueN)] / [Likelihood1 + Likelihood2 +...+ 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

Answer = [(Analyst1 x Credit1) + (Analyst2 x Credit2) +...+ (AnalystN x CreditN)] / [Credit1 + Credit2 +...+ CreditN]

SubDomain = [Answer1 + Answer2 +...+ AnswerN] / [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

AssetRisk = AssetValue x (Likelihood1 + Likelihood2 +...+ LikelihoodN) x (ImpactValue1 + ImpactValue +...+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

ThreatRisk = Likelihood x (ImpactValue1 + ImpactValue +...+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

จากนี้ไปจะเป็นแสดงให้เห็นถึงโครงสร้างของตารางในฐานข้อมูลทั้งหมดของระบบวิเคราะห์ความเสี่ยงของสารสนเทศ 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	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

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

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

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	รหัสโดเมนย่อยของ CobiT
DomainID	FK	Integer	รหัสโดเมนของ CobiT
SubDomain		Integer	โดเมนย่อยของ CobiT
Name		String	ชื่อโดเมนย่อย
Status		String	สถานะการวิเคราะห์การควบคุมและจัดการความเสี่ยง
Value		Single	ค่าผลการวิเคราะห์การควบคุมและจัดการความเสี่ยง
TaskID	FK	Integer	รหัสโครงการ

ตารางที่ 5.9 โครงสร้างของตาราง Threat

ชื่อแอตทริบิวต์		ชนิดข้อมูล	ความหมาย
ThreatID	PK	Integer	รหัสภัยคุกคาม
Threat		String	ภัยคุกคาม
Status		String	สถานะการวิเคราะห์โอกาสที่จะเกิดภัยคุกคาม
Likelihood		Single	โอกาสที่จะเกิดภัยคุกคาม
ImpactAVG		Single	ค่าเฉลี่ยของผลกระทบจากภัยคุกคาม
AssetID	FK	Integer	รหัสทรัพย์สิน
Analyst1		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 1
Credit1		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่1
Analyst2		Integer	ค่าคำตอบของนักวิเคราะห์คนที่ 2
Credit2		Integer	ค่าความมั่นใจในการตอบคำถามของนักวิเคราะห์คนที่2
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	รหัสโครงการ
TaskName		String	ชื่อโครงการ
Organization		String	ชื่อองค์กร
TotalAssetValue		Single	ผลรวมของระดับความสำคัญของทรัพย์สิน
TotalLikelihood		Single	ผลรวมของโอกาสภัยคุกคามที่จะเกิดขึ้น
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

บทที่ 6
สรุป

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศเป็นระบบที่นำเอาระบบคอมพิวเตอร์เข้ามาช่วยในการวิเคราะห์ความเสี่ยงของสารสนเทศในองค์กร เพื่ออำนวยความสะดวกให้นักวิเคราะห์ความเสี่ยงสามารถวิเคราะห์ความเสี่ยงได้อย่างรวดเร็วและเป็นระบบ เพื่อช่วยวิเคราะห์และประเมินความเสี่ยง ซึ่งผลการวิเคราะห์ความเสี่ยงสามารถนำมาใช้เป็นแนวทางในการแก้ไขความเสี่ยงได้

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

ระบบวิเคราะห์ความเสี่ยงของสารสนเทศใช้ UML ช่วยในการออกแบบ ซึ่งมีการใช้โมเดลต่างๆมาช่วยอธิบายระบบงานนั้นๆ ทำให้สามารถแสดงภาพรวมของระบบทั้งหมดได้อย่างชัดเจน และช่วยทำให้นักวิเคราะห์ระบบ นักพัฒนาและผู้ใช้ มีมุมมองที่เข้าใจตรงกัน ทำให้การพัฒนาระบบเป็นไปอย่างรวดเร็ว

ผลการวิเคราะห์ความเสี่ยงที่ได้จากการวิเคราะห์จะสามารถบอกได้ว่าทรัพย์สินใดในองค์กรมีความเสี่ยงในระดับใดบ้าง องค์กรมีความเสี่ยงจากภัยคุกคามอะไรบ้าง ในระดับไหน ทำให้ช่วยตัดสินใจได้ว่าควรพิจารณาทรัพย์สินใดและภัยคุกคามใดเป็นอันดับแรก นอกจากนั้นยังให้คำแนะนำว่าควรมีการเพิ่มหรือลดการควบคุมและจัดการความเสี่ยงในแต่ละโดเมนย่อยของ CobiT แต่อย่างไรก็ตาม ระบบวิเคราะห์ความเสี่ยงของสารสนเทศไม่สามารถช่วยแก้ไขความเสี่ยงที่เกิดขึ้นได้ เพียงแต่เป็นระบบที่ช่วยในการวิเคราะห์ความเสี่ยงและช่วยแนะนำว่าควรทำอย่างไร จึงเป็นหน้าที่ของผู้ดูแลระบบและผู้ที่เกี่ยวข้อง ในการวางแผนแก้ไขและจัดการความเสี่ยงเหล่านั้นต่อไป

บรรณานุกรม

ชาลี วรกุลพิพัฒน์ และเทพฤทธิ์ บัณฑิตพัฒนาวงศ์. 2544. **UML ภาษามาตรฐานเพื่อผู้พัฒนาซอร์ฟแวร์.** กรุงเทพฯ: ซีเอ็ดยูเคชั่น.

วุฒิพงศ์ พงศ์สุวรรณ. 2543. **How to learn Visual Basic.** กรุงเทพฯ: ซอร์ฟแวร์ ปาร์ค.

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