ระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัย ในการใช้เทคโนโลยีสารสนเทศ

IT SECURITY RISK MANAGEMENT SUPPORT SYSTEM

โดย

ศศิวิมล เนตรสูงเนิน

SASIWIMOL NEDSOONGNEAN

อาจารย์ที่ปรึกษา

ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานฉบับนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2550

IT SECURITY RISK MANAGEMENT SUPPORT SYSTEM

SASIWIMOL NEDSOONGNEAN

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2 / 2007

หัวข้อ	ระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ
นักศึกษา	นางสาวศศิวิมล เนตรสูงเนิน
รหัสนักศึกษา	47066606
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2550
อาจารย์ที่ปรึกษา	ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

เอกสารฉบับนี้จะกล่าวถึงการพัฒนาระบบช่วยบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ โดยส่วนแรกจะเป็นการอธิบายถึงการบริหารจัดการความเสี่ยง ปัจจัยต่างๆ และขั้นตอนกระบวนการในการบริหารจัดการความเสี่ยงตามมาตราฐาน ISO/IEC 73:2002 และในส่วนที่สองจะกล่าวถึงการวิเคราะห์และออกแบบระบบโดยใช้แผนภาพการไหลของข้อมูล แผนภาพโครงสร้างของระบบ และการออกแบบฐานข้อมูลโดยใช้โมเดลความสัมพันธ์ระหว่างเอนติที (Entity-Relationship Diagram: E-R Diagram).

Title	IT Security Risk Management Support System.
Student	Miss Sasiwimol Nedsoongnean
Student ID	47066606
Degree	Master of Science
Program	Information Science
Academic Year	2007
Advisor	Assoc. Prof. Dr. Chanboon Sathitwiriyawong

ABSTRACT

The objective and primary focus of this paper is to provide a simple overview of the framework for IT risk management which is guide by ISO/IEC 73:2002 Standard. The paper is divides into two sections. The first section describes in details the risk management system which includes the definition of the risk management system, the risk management process and drivers of key risks within corporate it system. The second section describes in details the structure of the IT risk management support system and provides detailed analysis of the structure which is supported by Data Flow Diagram (DFD), Structure Chart and Entity-Relationship Diagram (E-R Diagram).

กิตติกรรมประกาศ

ในความสำเร็จของโครงการนี้ ผู้เขียนใคร่ขอแสดงความระลึกถึงบุคคลสำคัญผู้อยู่เบื้องหลังดังต่อไปนี้

อาจารย์ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษาโครงการ ผู้ให้คำปรึกษา และคำแนะนำต่างๆ ที่เป็นประโยชน์ยิ่งจนทำให้โครงการนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณบัณฑิตศึกษาและบัณฑิตวิทยาลัย คณะเทคโนโลยีสารสนเทศที่ให้ความช่วยเหลือในเรื่องต่างๆ

สุดท้ายนี้ข้าพเจ้าขอกราบขอบคุณ บิดา มารดา และครอบครัวของข้าพเจ้าที่เป็นกำลังใจและให้การสนับสนุนในทุกเรื่องๆ ทำให้ข้าพเจ้าสามารถทำโครงงานฉบับนี้สำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงมาจากโครงงานฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

ศศิวิมล เนตรสูงเนิน

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมา

ปัจจุบันระบบสารสนเทศได้เข้ามามีบทบาท และเป็นส่วนที่สำคัญสำหรับองค์กรทำให้เกิดข้อได้เปรียบในด้านการแข่งในเชิงธุรกิจ และถือเป็นส่วนประกอบหลักขององค์กรที่ขาดไม่ได้ ดังนั้นความปลอดภัยของระบบสารสนเทศจึงเป็นสิ่งจำเป็นที่ต้องพิจารณาความสำคัญของการมุ่งเน้นให้มีการระวังภัย เตรียมการป้องกัน หรือ รับมือต่อความเป็นไปได้ในอันที่จะเกิดความสูญเสีย ความเสียหาย ปัญหา อุปสรรค ภัยคุกคาม และสถานการณ์ที่ไม่แน่นอนต่างๆ ที่จะส่งผลทำให้เกิดความล้มเหลว และความผิดพลาดต่อความปลอดภัยของระบบสารสนเทศ ดังนั้นเพื่อที่จะสามารถป้องกันระบบสารสนเทศขององค์กรให้ปลอดภัยทั้งจากภายในและภายนอกองค์กร จึงต้องมีการจัดนโยบายทางด้านความปลอดภัยขององค์กรให้เหมาะสมกับกระบวนการทางธุรกิจ (Business Process) ของแต่ละองค์กร เพื่อป้องกันความเสียหาย หรือความสูญเสียที่อาจจะเกิดขึ้นกับระบบสารสนเทศ โดยในแต่ละส่วนของระบบสารสนเทศจะมีความเสี่ยงต่อการสูญเสียและทำให้เกิดความเสียหายต่อองค์กรมากน้อยแตกต่างกัน การจะกำหนดนโยบายทางด้านความปลอดภัยให้กับองค์กรแต่ละองค์กรได้นั้นจะต้องมีการบริหารจัดการความเสี่ยง (Risk Management) ของแต่ละองค์กรว่ามีความเสี่ยงในเรื่องใดบ้างและมีความเสี่ยงมากน้อยเพียงใด เพื่อที่จะนำมากำหนดนโยบายทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพ และเหมาะสมกับองค์กรนั้นๆ

การวิเคราะห์และออกแบบระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศนี้ เพื่อช่วยสนับสนุนการบริหารจัดการความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กร โดยจะเป็นการช่วยวิเคราะห์ความเสี่ยงทางด้านระบบสารสนเทศขององค์กรตามระบบการบริหารจัดการความปลอดภัยของระบบสารสนเทศ (Information Security Management System) ตามมาตราฐาน ISO 17799: 2005 ระบบบริหารจัดการความเสี่ยงจะทำให้เราทราบปัญหาล่วงหน้าและสามารถเตรียมวิธีการป้องกันแก้ไขได้ ช่วยลดโอกาสสูญเสียและเพิ่มโอกาสความสำเร็จ ส่งผลให้องค์กรดำรงอยู่อย่างยั่งยืน และเติบโตอย่างต่อเนื่อง

1.2 วัตถุประสงค์ของการพัฒนาระบบงาน

ระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ มีความมุ่งหมายและวัตถุประสงค์ในการพัฒนาระบบงานมีดังนี้

1. เพื่อศึกษาและวิเคราะห์การบริหารจัดการความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ และนำมาใช้เป็นส่วนประกอบในการพัฒนาระบบให้เหมาะสมและมีประสิทธิภาพ
2. เพื่อพัฒนาระบบที่เข้ามาช่วยในการวิเคราะห์ความเสี่ยงทางด้านความปลอดภัยของระบบสารสนเทศของแต่ละองค์กร ทำให้สามารถศึกษาถึงความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศว่ามีความเสี่ยงในด้านใดบ้าง และมีแนวทาง วิธีการในการลดความเสี่ยงอย่างไร
3. เพื่อให้เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศสามารถกำหนดนโยบายทางด้านความปลอดภัยของระบบสารสนเทศให้กับองค์กรได้
4. เพื่อให้บุคคลผู้ที่ไม่มีความรู้ทางด้านความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศสามารถศึกษาหาความรู้ได้จากระบบที่พัฒนาขึ้น

1.3 เป้าหมายโครงการ

เป้าหมายของการพัฒนาระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ คือ การพัฒนาระบบเพื่อให้ผู้ใช้งานระบบสารสนเทศสามารถทำการวิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ และสามารถกำหนดรูปแบบการควบคุมความเสี่ยงให้กับระบบสารสนเทศ โดยมุ่งเน้นที่ความสะดวก ความเข้าใจในการใช้งานระบบสารสนเทศอย่างปลอดภัย และความรวดเร็วในการวิเคราะห์ความเสี่ยงรวมถึงการควบคุมความเสี่ยงที่จะเกิดขึ้น รวมถึงสามารถทำการปรับปรุงข้อมูลทางด้านความมั่นคงปลอดภัยให้ทันสมัย

1.4 ขอบเขตการพัฒนาระบบงาน

ระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศนี้ จะเป็นการนำเสนอข้อมูลที่ได้จากการศึกษามาทำการวิเคราะห์และออกแบบระบบโดยใช้หลักการของ SDLC (System Development Lift Cycle) ซึ่งเป็นภาษาสัญลักษณ์ในการอธิบาย จำลองการสร้างและจัดทำคู่มือในกระบวนการพัฒนาซอฟต์แวร์ ในการวิเคราะห์และออกแบบระบบนี้ประกอบด้วย แผนภาพการไหลของข้อมูล (Data Flow Diagram: DFD) แผนภาพโครงสร้าง (Structure Chart) และใช้แบบจำลองความสัมพันธ์ระหว่างเอนทิตี (Entity-Relationship Diagram: E-R Diagram) ในการออกแบบฐานข้อมูล โดยขอบเขตของระบบมีรายละเอียดดังนี้

1. สามารถบันทึก ปรับปรุง และลบข้อมูลทรัพย์สิน ข้อมูลช่องโหว่ ข้อมูลภัยคุกคาม ที่จะนำมาใช้ในการกำหนดการวิเคราะห์ความเสี่ยง

2. สามารถบันทึก ปรับปรุง และลบการกำหนดช่องโหว่ ภัยคุกคามให้ การควบคุมให้แต่ละทรัพย์สิน
3. สามารถบันทึก ปรับปรุง และลบข้อมูลรายละเอียดขององค์กรที่เข้าทำการวิเคราะห์ความเสี่ยง รวมถึงรายละเอียดของทรัพย์สินขององค์กร ช่องโหว่ ภัยคุกคามที่มีโอกาสที่จะเกิด และผลกระทบที่จะเกิดขึ้นกับองค์กร
4. มีรายงานแสดงความเสี่ยงที่จะเกิดขึ้นกับทรัพย์สินในแต่ละประเภท ในแต่ละคลาสของทรัพย์สิน รวมถึงการควบคุมความเสี่ยงเหล่านั้นด้วย

1.5 ขั้นตอนและการดำเนินโครงการ

ขั้นตอนการพัฒนาระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศจะแบ่งออกเป็น 6 ขั้นตอนหลักๆ ดังนี้

1. ขั้นตอนการศึกษากระบวนการในการจัดทำการบริหารจัดการความเสี่ยงตามมาตราฐาน ISO/IEC 73:2002 โดยพิจารณาการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศภายในองค์กรตามมาตราฐาน ISO 17799:2005
2. ทำการเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศภายในและภายนอกองค์กร ข้อมูลการวิเคราะห์ความปลอดภัย ข้อมูลการวิเคราะห์โอกาสและผลกระทบที่อาจจะเกิดความเสี่ยงกับระบบสารสนเทศ ข้อมูลการควบคุมความเสี่ยงเพื่อไม่ให้เกิดความเสี่ยง หรือลดความเสี่ยงลงให้น้อยที่สุด
3. นำข้อมูลที่ได้จากการศึกษาและเก็บรวบรวมทั้งหมด มาทำการวิเคราะห์และออกแบบระบบ
4. ศึกษาเทคโนโลยีต่างๆ ที่เกี่ยวข้องในการพัฒนาระบบเพื่อเลือกใช้เทคโนโลยีที่เหมาะสมในการพัฒนาระบบช่วยบริหารจัดการความเสี่ยงทางด้านความปลอดภัยในการใช้ระบบสารสนเทศ
5. พัฒนาโปรแกรมตามการวิเคราะห์และออกแบบระบบที่ได้มีการจัดทำไว้
6. ทำการทดสอบระบบทั้งหมดตามการออกแบบระบบ และทำการแก้ไขปรับปรุงข้อผิดพลาดของระบบ เพื่อทำให้ระบบทำงานได้อย่างถูกต้องและมีประสิทธิภาพ
7. สรุปผลการดำเนินการและข้อเสนอแนะ

1.6 รายละเอียดในบทต่างๆ

- **บทที่ 2** จะกล่าวถึงทฤษฎี และหลักการที่เกี่ยวข้องในการพัฒนาระบบงาน มาตรฐานที่ได้นำมาใช้ในการศึกษา รวมไปถึงนำมาใช้ในการกำหนดรูปแบบการ

บริหารจัดการความเสี่ยง การกำหนดนโยบายในด้านความมั่นคงปลอดภัยให้กับระบบสารสนเทศ

- **บทที่ 3** จะกล่าวถึงการวิเคราะห์การบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ โดยกำหนดเป็นขั้นตอนตั้งแต่การจัดประเภททรัพย์สิน กำหนดนิยามทรัพย์สิน วิเคราะห์ภัยคุกคามและช่องโหว่ที่สามารถเกิดขึ้นกับการใช้งานระบบสารสนเทศ การกำหนดลักษณะของโอกาสที่จะเกิดเหตุการณ์ที่เป็นภัยคุกคาม รวมถึงการกำหนดผลกระทบที่คาดว่าจะเกิด และรูปแบบในการพิจารณาความเสี่ยง
- **บทที่ 4** จะกล่าวถึงการออกแบบระบบสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศ โดยทำการศึกษาถึงการวิเคราะห์และออกแบบโดยแผนภาพกระแสการไหลของข้อมูล และแผนผังโครงสร้างของระบบ
- **บทที่ 5** กล่าวถึงการออกแบบฐานข้อมูล
- **บทที่ 6** จะกล่าวถึงการออกแบบสถาปัตยกรรมของระบบ การออกแบบเว็บเพจหน้าจอในการรับส่งข้อมูล และหน้าจอแสดงข้อมูลต่างๆ
- **บทที่ 7** จะกล่าวถึงผลสรุปของการดำเนินงานประโยชน์ของระบบที่พัฒนาขึ้นใหม่

บทที่ 2
ทฤษฎีที่เกี่ยวข้องกับระบบการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

ในบทนี้จะกล่าวถึงทฤษฎี และหลักการต่างๆที่เกี่ยวข้องกับระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ ซึ่งจะประกอบด้วยการบริหารจัดการความเสี่ยง (Risk Management) การประเมินความเสี่ยง (Risk Assessment) และมาตรฐานการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ

2.1 การบริหารจัดการความเสี่ยง

ระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ โดยขั้นตอนการพัฒนาระบบจะเป็นไปตามมาตรฐานการจัดตั้งการบริหารจัดการความเสี่ยงของ ISO/IEC Guide 73:2002 (AIRMIC, ALARM, and IRM. 2002 : 2-11)

ความเสี่ยง (Risk) คือ ภาวะคุกคามปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อองค์กร ทั้งในทางกลยุทธ์ การปฏิบัติงาน การเงิน และการดำเนินธุรกิจอย่างต่อเนื่องและสม่ำเสมอ

การบริหารความเสี่ยง (Risk Management) คือ การกำหนดแนวทางและกระบวนการในการระบุ ประเมิน จัดการและติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือการดำเนินงานขององค์กร รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ จากรูปที่ 1 ความเสี่ยงจะแบ่งออกเป็น 4 ประเภทใหญ่ๆ ดังนี้

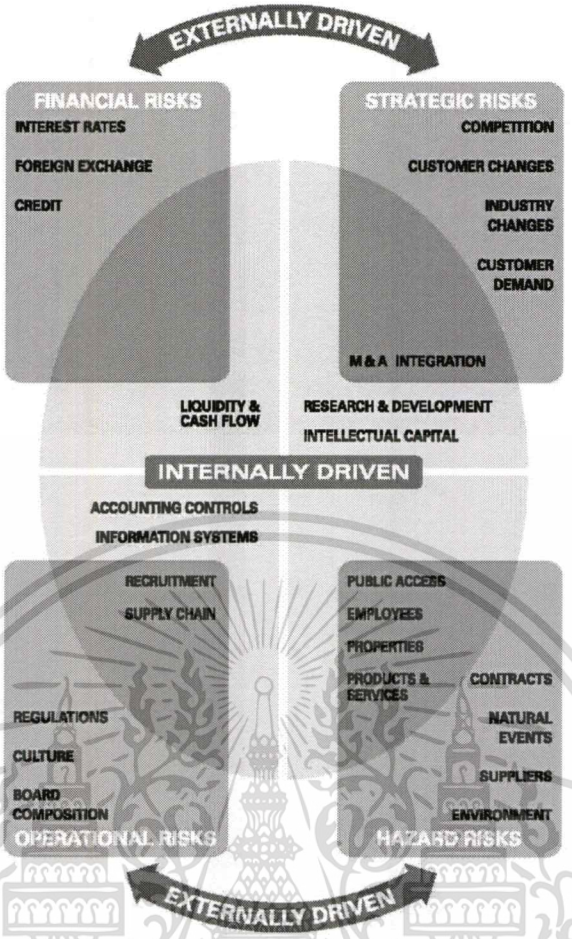
ความเสี่ยงทางด้านการเงิน (Financial Risk)

ความเสี่ยงทางด้านกลยุทธ์ (Strategic Risk)

ความเสี่ยงทางด้านขั้นตอน อุปกรณ์การปฏิบัติงาน(Operational Risk)

ความเสี่ยงของบุคคลและสิ่งแวดล้อม(Hazard Risk)

โดยความเสี่ยงทั้ง 4 ประเภทจะมีการแบ่งความเสี่ยงออกเป็นปัจจัยภายใน และปัจจัยภายนอก ดังรูปที่ 2.1



รูปที่ 2.1 แสดงส่วนประกอบและปัจจัยของการบริหารจัดการความเสี่ยง

กระบวนการบริหารจัดการความเสี่ยงของระบบสารสนเทศตามมาตราฐาน ISO / IEC Guide 73:2002 มีกระบวนการของการบริหารจัดการความเสี่ยง ดังรูปที่ 2.2 ซึ่งจะมีขั้นตอนหลักๆ ดังนี้

ขั้นตอนที่ 1 การกำหนดวัตถุประสงค์ทางด้านกลยุทธ์ขององค์กร (The Organization's Strategic Objectives) เป็นการกำหนดกรอบ (Framework) ความเป็นไปได้ของการปฏิบัติและการวิธีการในการควบคุมสำหรับองค์กร เป็นการกำหนดการตัดสินใจ การวางแผน และการกำหนดลำดับความสำคัญตามโครงสร้างของกระบวนการทางธุรกิจ (business activity) ของแต่ละองค์กร

ขั้นตอนที่ 2 การประเมินความเสี่ยง (Risk Assessment) องค์กรจะใช้การประเมินความเสี่ยงสำหรับกำหนดขอบเขตความเป็นไปได้ของความเสี่ยง และความสัมพันธ์ระหว่างความเสี่ยงกับระบบสารสนเทศ การพิจารณาจะพิจารณาทั้งโอกาศ (likelihood) ที่

ความเสี่ยงจะเกิดในอนาคต และการวิเคราะห์ถึงผลกระทบที่อาจจะเกิดขึ้น ซึ่งระบบช่วยวิเคราะห์ความเสี่ยงทางด้านความปลอดภัยของระบบสารสนเทศ

รูปที่ 2.2 แสดงขั้นตอนกระบวนการของการบริหารจัดการความเสี่ยง

ขั้นตอนที่ 3 การรายงานความเสี่ยง (Risk Reporting) เป็นการรายงานถึงความน่าจะเป็นที่จะเกิดภัยคุกคาม และความน่าจะเป็นของผลกระทบจากภัยคุกคามนั้น

ขั้นตอนที่ 4 การตัดสินใจในการจัดการความเสี่ยง ว่าความเสี่ยงที่เกิดขึ้นนั้นเป็นความเสี่ยงที่สามารถยอมรับได้ หรือจัดการกับความเสี่ยง โดยการลดความเสี่ยง หรือ ส่งผ่านความเสี่ยง เปรียบเทียบระดับความเสี่ยงที่เกิดกับระดับความเสี่ยงที่ยอมรับได้ และความคุ้มค่าในการที่จะบริหารความเสี่ยงที่เหลืออยู่ (Residual Risk) นั้น และทำการพิจารณาเลือกวิธีการที่ควรกระทำตามผลการประเมินความเสี่ยง

ขั้นตอนที่ 5 การจัดการกับความเสี่ยง

ขั้นตอนที่ 6 การรายงานความเสี่ยงยังเหลืออยู่ (Residual Risk Reporting) หลังจากการดำเนินในการจัดการความเสี่ยงแล้วนั้น ต้องทำรายงานความเสี่ยงที่ยังเหลืออยู่ ว่ามีความเสี่ยงใดบ้างที่เหลืออยู่ เพื่อจะทำการกำหนดขั้นตอนในการดำเนินการต่อไป

ขั้นตอนที่ 7 <u>การมอนิเตอร์ (Monitoring)</u> การติดตามประเมินผลและรายงานผลการบริหารความเสี่ยงจะต้องมีการกำหนดขั้นตอนและระยะเวลาดำเนินการประสานงานติดตามผล สรุปและทบทวนปัจจัยความเสี่ยงและจัดทำร่างรายงานการจัดการความเสี่ยง ระบบบริหารความเสี่ยงที่สมบูรณ์นั้นควรจะประกอบไปด้วย การติดตามและสอบทานผลอย่างเป็นระบบ มีการ รายงานผลและตรวจสอบอย่างสม่ำเสมอถึงระดับความเสี่ยงในแต่ละประเด็น เพื่อที่เราจะได้ทราบว่าความเสี่ยงต่าง ๆ อยู่ ในระดับใด รุนแรงหรือไม่ แผนจัดการความเสี่ยงแผนใดประสบความสำเร็จ หรือแผนใดไม่มีประสิทธิภาพ เป็นต้น

2.2 การประเมินความเสี่ยง (Risk Assessment)

จากการบริหารจัดการความเสี่ยงในหัวข้อ 2.1 นั้น ในส่วนของการประเมินความเสี่ยงถือว่าเป็นส่วนที่มีความสำคัญที่สุด จากรูปที่ 2.3 จะแสดงถึงกระบวนการในการประเมินความเสี่ยงที่ได้นำมาใช้ในการพัฒนาระบบ โดยมีรายละเอียดดังนี้ (National Institute of Standards and Technology. 2002 : 8-41)

2.2.1 System Characterization

ขั้นตอนแรกสำหรับการทำการประเมินความเสี่ยง คือขอบเขตการให้นิยามระบบสารสนเทศ เป็นการอธิบายลักษณะของระบบสารสนเทศขององค์กร เนื่องจากการนิยามความเสี่ยงสำหรับระบบสารสนเทศต้องทำความเข้าใจถึงกระบวนการของระบบ รวมไปถึงสภาพแวดล้อมของระบบ ดังนั้นจึงต้องทำการเก็บรวบรวมความสัมพันธ์ของระบบสารสนเทศ โดยจะทำการแยกประเภทดังนี้

- Hardware
- Software
- System Interface (เช่น Internal and External Connectivity)
- Data and Information
- Persons (ที่ดูแล หรือใช้งานระบบสารสนเทศ)
- System mission
- System and Data criticality
- System and Data sensitivity

2.2.2 Threat Identification

การระบุและจำแนกภัยคุกคามที่อาจจะเกิดขึ้น และจะเป็นสาเหตุที่ก่อให้เกิดความเสี่ยง ยกตัวอย่างเช่น

- ภัยคุกคามทางธรรมชาติ (Natural Threats) เช่น น้ำท่วม แผ่นดินไหว ทอร์นอโด เป็นต้น

- ภัยคุกคามจากมนุษย์ (Human Threats) เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- ภัยคุกคามทางด้านสิ่งแวดล้อม (Environmental Threats) เช่น ระบบไฟฟ้าขัดข้อง มลภาวะต่างๆ เป็นต้น

2.2.3 Vulnerability Identification

การระบุและจำแนกข้อบกพร่อง หรือความอ่อนแอของกระบวนการ การออกแบบ การจัดตั้ง หรือการควบคุมความปลอดภัยของระบบ โดยการวิเคราะห์ภัยคุกคาม(Threats) ของระบบสารสนเทศจะประกอบด้วยการวิเคราะห์ข้อบกพร่อง หรือความอ่อนแอ (Vulnerability) ที่มีความสัมพันธ์กับสิ่งแวดล้อมของระบบ

2.2.4 Control Analysis

เป้าหมายของขั้นตอนนี้คือ การวางแผนสำหรับการจัดตั้งความปลอดภัย โดยเป็นการลดหรือการประเมินโอกาสที่น่าจะเกิดความเสี่ยงที่ได้จากการวิเคราะห์ภัยคุกคาม และข้อบกพร่องของระบบ

2.2.5 Likelihood Determination

การพิจารณาความน่าจะเกิด หรือโอกาสที่จะเกิดความเสี่ยง โดยจะทำการพิจารณาเป็นระดับของโอกาสที่จะเกิดความเสี่ยง เช่น ระดับสูง (High Level) ระดับกลาง (Medium Level) ระดับต่ำ (Low Level)

2.2.6 Impact Analysis

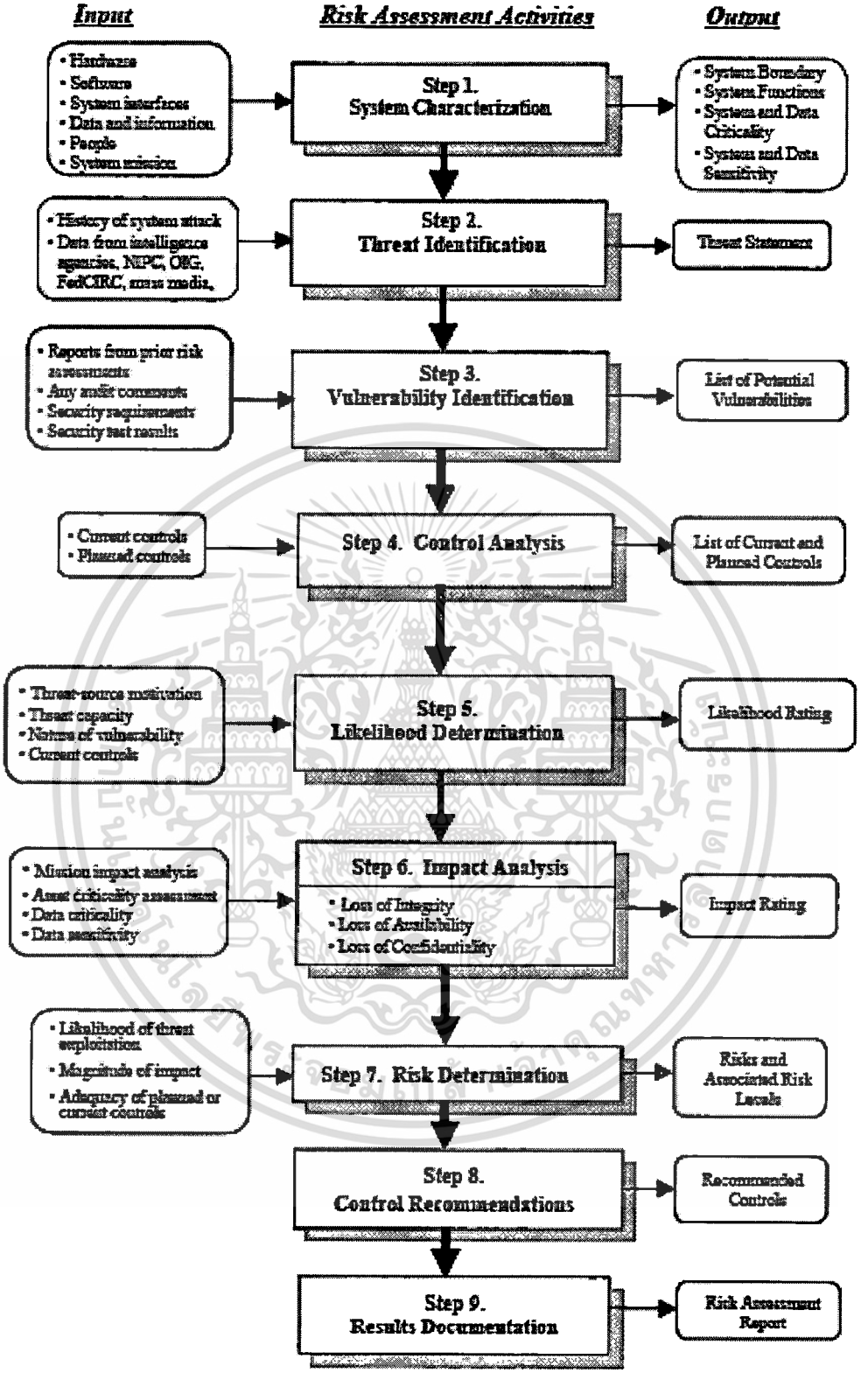
ขั้นตอนการวิเคราะห์ผลกระทบถือเป็นขั้นตอนหลักในการพิจารณาความเสี่ยง เนื่องจากผลกระทบที่เกิดขึ้นจากภัยคุกคาม และจากข้อบกพร่องของระบบสารสนเทศขององค์กรจะก่อให้เกิดความสูญเสียไม่ว่าจะเป็น การสูญเสียความถูกต้องของข้อมูล (Loss Of Integrity) การสูญเสียความเสถียรภาพ (Loss Of Availability) การสูญเสียทางด้านความมั่นคง (Loss of Confidentiality)

2.2.7 Risk Determination

การพิจารณาความเสี่ยงเป็นการจัดระดับความเสี่ยงของระบบสารสนเทศ โดยจะพิจารณาความเสี่ยงจากความเป็นไปได้จากการที่จะเกิดภัยคุกคาม และการเกิดข้อบกพร่องหรือความอ่อนแอของระบบสารสนเทศ โดยการจัดทำแผนผังเมทริกซ์แสดงระดับความเสี่ยง(Risk-Level Matrix)

2.2.8 Control Recommendations

กระบวนการควบคุมจะเป็นการบรรเทาหรือกำจัดความเสี่ยงที่จะเกิดขึ้น โดยเป้าหมายของการควบคุมคือการลดระดับความเสี่ยงของระบบสารสนเทศให้อยู่ในระดับที่สามารถยอมรับได้ จะเป็นการกำหนดกระบวนการ เทคนิคการควบคุม การจัดตั้งความปลอดภัย



รูปที่ 2.3 แสดงขั้นตอนกระบวนการในการจัดทำ Risk Assessment

2.3 มาตรฐานการรักษาความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ (ISO 17799:2005)

มาตรฐานการรักษาความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 17799:2005 ได้กำหนดแนวทางในการจัดตั้ง และการปฏิบัติที่เหมาะสมในการสนับสนุนการการจัดตั้งการรักษาความมั่งคงปลอดภัยในระบบสารสนเทศ ซึ่งมีรายละเอียดดังนี้ (คณะอนุกรรมการด้านความมั่นคง ใน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. 2549)

ตารางที่ 2.1 ตารางแสดงมาตรฐานการรักษาความมั่นคงปลอดภัยในเทคโนโลยีสารสนเทศ

หัวข้อ	การควบคุม	
1.	**นโยบายความมั่นคงปลอดภัย (Security policy)**	
1.1	**นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)** จุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการ ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้อง กับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง	
1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	(ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ
1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	(ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร
2.	**โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)**	
2.1	**โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)** มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร	

ตารางที่ 2.1 (ต่อ)

2.1.1	การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	(ผู้บริหารองค์กร) ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร
2.1.2	การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน
2.1.3	การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	(ผู้บริหารสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน
2.1.4	กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information)	(ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการ processing facilities)
2.1.5	การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)	(หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น)รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

ตารางที่ 2.1 (ต่อ)

2.1.6	การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)	(ผู้บริหารสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ, บมจ. ทศท คอร์เปอเรชั่น, บมจ. กสท โทรคมนาคม ผู้ให้บริการอินเตอร์ เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์
2.1.7	การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest	(ผู้บริหารองค์กรและหัวหน้างานสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่ความสนใจด้านความมั่นคงปลอดภัยสารสนเทศหรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม
2.1.8	การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับ (security) สารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร
2.2	**โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)** มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก	
2.2.1	การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to External parties)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิด จากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

ตารางที่ 2.1 (ต่อ)

2.2.2	การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)	(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได
2.2.3	การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)	(หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
3.	**การบริหารจัดการทรัพย์สินขององค์กร (Asset management)**	
3.1	**หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)** มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้	
3.1.1	การจัดทำบัญชีทรัพย์สิน (Inventory of assets)	(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ
3.1.2	การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)	(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) จะต้องจัดทำกฎระเบียบหรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม
3.2	**การจัดหมวดหมู่สารสนเทศ (Information classification)** มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม	
3.2.1	การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)	(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า

ตารางที่ 2.1 (ต่อ)

		ข้อกำหนดทาง กฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม
3.2.2	การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)	(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว
4.	**ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)**	
4.1	**การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)** มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภาย นอก เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์	
4.1.1	การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)	(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงานผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
4.1.2	การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)	(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงาน ภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบจริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการ

ตารางที่ 2.1 (ต่อ)

		เข้าถึงประกอบการคัดเลือกด้วย
4.1.3	การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)	(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
4.2	**การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)** มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยหน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่	
4.2.1	หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)	(ผู้บริหารองค์กร) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบาย
4.2.2	การสร้างความตระหนัก การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)	(หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง) ต้องกำหนดให้ชพนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอก ได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ และขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย
4.2.3	กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)	(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

ตารางที่ 2.1 (ต่อ)

4.3	**การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)** มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตนเมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน	
4.3.1	การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)	(หัวหน้างานบุคคล) ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว
4.3.2	การคืนทรัพย์สินขององค์กร (Return of assets)	(หัวหน้างานบุคคลและหัวหน้างานพัสดุ) ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน
4.3.3	การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	(หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน
5.	**การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)**	
5.1	**บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)** มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร	
5.1.1	การจัดทำบริเวณล้อมรอบ (Physical security perimeter)	(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทาง เข้า-ออกที่มีการควบคุม ตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศ
5.1.2	การควบคุมการเข้า-ออก (Physical entry controls)	(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า-ออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัยและ

ตารางที่ 2.1 (ต่อ)

		อนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น
5.1.3	การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)	(หัวหน้างานอาคาร) ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ
5.1.4	การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)	หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ
5.1.5	การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย
5.1.6	การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑโดยบุคคลภายนอก (Public access, delivery, and loading areas)	(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก
5.2	**ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)** มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมยหรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สิน ขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก	
5.2.1	การจัดวางและการป้องกันอุปกรณ์ (Equipment setting and protection)	(พนักงาน) ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต
5.2.2	ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบ

ตารางที่ 2.1 (ต่อ)

		น้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรองระบบสายสื่อสารสำรองเป็นต้น
5.2.3	การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)	(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิ้ลอื่นๆ ได้รับการป้องกัน จากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย
5.2.4	การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆอย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน
5.2.5	การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)	การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)
5.2.6	กำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)	(พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง
5.2.7	การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)	(หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น
6.	**การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)**	
6.1	**การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)**	

ตารางที่ 2.1 (ต่อ)

	มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย	
6.1.1	ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงานปรับปรุงตามระยะเวลาอันสมควรและแจกจ่ายให้กับผู้ที่เกี่ยวข้อง
6.1.2	การควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการปลี่ยนแปลงปรับปรุง หรือ แก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ
6.1.3	การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)	(ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต
6.1.4	การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)	(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต
6.2	**การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)** มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก	
6.2.1	การให้บริการโดยหน่วยงานภายนอก (Service delivery)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ
6.2.2	การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงาน

ตารางที่ 2.1 (ต่อ)

	third party services)	ภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก
6.3	**การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)** มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ	
6.3.1	การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)	(หัวหน้างานสารสนเทศ) ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน
6.3.2	การตรวจรับระบบ (System acceptance)	(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติมหรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน
6.4	**การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)** มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี	
6.4.1	การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	(ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย
6.4.2	การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)	(ผู้ดูแลระบบ) ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิด เคลื่อนที่จากหน่วยความจำของ

ตารางที่ 2.1 (ต่อ)

		เครื่องคอมพิวเตอร์ไปทำงานในหน่วยความจำของอีก ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆสามารถ ทำงานหรือใช้งานได้
6.5	**การสำรองข้อมูล (Back-up)** มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ	
6.5.1	การสำรองข้อมูล (Information back-up)	(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร
6.6	**การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)** มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย	
6.6.1	มาตรการทางเครือข่าย (Network controls)	(ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย
6.6.2	ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)	(หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก
6.7	**การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling)**	

ตารางที่ 2.1 (ต่อ)

	มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ	
6.7.1	การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)	(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้
6.7.2	การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้วการทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย
6.7.3	ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)	(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์
6.7.4	การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)	(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต
6.8	**การแลกเปลี่ยนสารสนเทศ (Exchange of information)** มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลเปลี่ยนกับหน่วยงานภายนอก	
6.8.1	นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)	(ผู้บริหารองค์กร) ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด
6.8.2	ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)	(หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่าง องค์กร อย่างเป็นลายลักษณ์อักษร
6.8.3	การส่งสื่อบันทึกข้อมูลออกไปนอก	(หัวหน้างานสารสนเทศและหัวหน้างาน

ตารางที่ 2.1 (ต่อ)

	องค์กร(Physical media in transit)	ธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร
6.8.4	การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)	(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์
6.8.5	ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน(Business information systems)	(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน
6.9	**การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)** มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน	
6.9.1	การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)	(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผยและการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต
6.9.2	การทำธุรกรรมออนไลน์ (On-line transactions)	(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

ตารางที่ 2.1 (ต่อ)

6.9.3	สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ(Publicly available information)	(ผู้ดูแลระบบ) ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ
6.10	**การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)** มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต	
6.10.1	การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย อย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้
6.10.2	การตรวจสอบการใช้งานระบบ (Monitoring system use)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่
6.10.3	การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต
6.10.4	บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ
6.10.5	การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร
6.10.6	การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน	(ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงาน (Clock synchronization) ให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบ

ตารางที่ 2.1 (ต่อ)

		ช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก
7.	**การควบคุมการเข้าถึง (Access control)**	
7.1	**ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)** มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ	
7.1.1	นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ
7.2	**การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)** มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้า ถึงโดยไม่ได้รับอนุญาต	
7.2.1	การลงทะเบียนพนักงาน (User registration)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น
7.2.2	การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน
7.2.3	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	(ผู้ดูแลระบบ) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

ตารางที่ 2.1 (ต่อ)

7.2.4	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	(หัวหน้างานสารสนเทศ) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้
7.3	**หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)** มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ	
7.3.1	การใช้งานรหัสผ่าน (Password use)	(ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน
7.3.2	การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)	(พนักงาน) ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล
7.3.3	นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)	(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น
7.4	**การควบคุมการเข้าถึงเครือข่าย (Network access control)** มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต	
7.4.1	นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้
7.4.2	การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)	(ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่ อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้
7.4.3	การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)	(ผู้ดูแลระบบ) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือ

ตารางที่ 2.1 (ต่อ)

		สถานที่ที่ได้รับอนุญาตแล้ว
7.4.4	การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	(ผู้ดูแลระบบ) ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
7.4.5	การแบ่งแยกเครือข่าย (Segregation in networks)	(ผู้ดูแลระบบ) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ
7.4.6	การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)	(ผู้ดูแลระบบ) ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้
7.4.7	การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	(ผู้ดูแลระบบ) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง
7.5	**การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)** มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต	
7.5.1	ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	(ผู้ดูแลระบบ) ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ
7.5.2	การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)	(ผู้ดูแลระบบ) ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ
7.5.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	(ผู้ดูแลระบบ) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการ

ตารางที่ 2.1 (ต่อ)

		กำหนดรหัสผ่านที่มีคุณภาพ
7.5.4	การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	(ผู้ดูแลระบบ) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว
7.5.5	การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	(ผู้ดูแลระบบ) ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้
7.5.6	การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	(ผู้ดูแลระบบ) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง
7.6	**การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)** มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต	
7.6.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	(ผู้ดูแลระบบ) ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของ แอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน
7.6.2	การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	(หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ
7.7	**การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)** มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร	
7.7.1	การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และ

ตารางที่ 2.1 (ต่อ)

		ต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้
7.7.2	การปฏิบัติงานจากภายนอกสำนักงาน	(ผู้บริหารสนเทศ) ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน
8.	**การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)**	
8.1	**ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)** มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ	
8.1.1	การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)	(ผู้พัฒนา และผู้เป็นเจ้าของระบบ) ต้องวิเคราะห์และระบุข้อกำหนด ทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว
8.2	**การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct processing in applications)** มีจุดประสงค์เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับ อนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์	
8.2.1	การตรวจสอบข้อมูลนำเข้า (Input data validation)	(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอปพลิเคชันว่าข้อ มูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป
8.2.2	การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)	(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวล ผลการกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น
8.2.3	การตรวจสอบความถูกต้องของข้อความ (Message integrity)	(ผู้พัฒนาระบบ) ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอฟพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็น

ตารางที่ 2.1 (ต่อ)

		ข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต
8.2.4	การตรวจสอบข้อมูลนำออก (Output data validation)	(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอพพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม
8.3	**มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)** มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการการเข้ารหัสข้อมูล	
8.3.1	นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร
8.3.2	การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร
8.4	**การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)** มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆ ของระบบที่ให้บริการ	
8.4.1	การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)	(หัวหน้างานสารสนเทศ) ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้
8.4.2	การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)	(ผู้พัฒนาระบบ) ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้อง

ตารางที่ 2.1 (ต่อ)

		กำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ
8.4.3	การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)	(หัวหน้างานสารสนเทศ) ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา
8.5	**การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและ กระบวนการสนับสนุน (Security in development and support processes)** มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ	
8.5.1	ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)	(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้
8.5.2	การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)	(ผู้ดูแลระบบ) ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอปพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่
8.5.3	การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)	(หัวหน้างานสารสนเทศ) ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้นและต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย
8.5.4	การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)	(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของ

ตารางที่ 2.1 (ต่อ)

		สารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป
8.5.5	การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)	(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก
8.6	**การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)** มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ	
8.6.1	มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว
9.	**การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)**	
9.1	**การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)** มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการ ที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม	
9.1.1	การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)	(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้
9.1.2	การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องบันทึกและ

ตารางที่ 2.1 (ต่อ)

		รายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่
9.2	**การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)** มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร	
9.2.1	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)	(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้น ตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี
9.2.2	การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)	(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า
9.2.3	การเก็บรวบรวมหลักฐาน (Collection of evidence)	(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา
10.	**การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)**	
10.1	**หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management)** มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็น ผลมาจากการล้มเหลวหรือหายนะที่มีต่อ	

ตารางที่ 2.1 (ต่อ)

	ระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม	
10.1.1	กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดัง กล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ
10.1.2	การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	(หัวหน้างานสารสนเทศ) ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
10.1.3	การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)	(ผู้บริหารสารสนเทศ) ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงักหรือล้มเหลว
10.1.4	การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework)	(ผู้บริหารสารสนเทศ) ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกันครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ
10.1.5	การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี
11.	**การปฏิบัติตามข้อกำหนด (Compliance)**	

ตารางที่ 2.1 (ต่อ)

11.1	**การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)** มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ	
11.1.1	การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)	(หัวหน้างานนิติการ) ต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว
11.1.2	การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectualproperty rights (IRP))	(หัวหน้างานนิติการ) ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา(ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์ จากผู้ขายด้วย
11.1.3	การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง
11.1.4	การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)	(หัวหน้างานนิติการ และหัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย

ตารางที่ 2.1 (ต่อ)

		ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง
11.1.5	การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)	(หัวหน้างานสารสนเทศ) ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต
11.1.6	การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)	(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตาม หรือต้องสอดคล้องกับข้อตกลง กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง
11.2	**การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards and technical compliance)**	
	มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร	
11.2.1	การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)	(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบ คุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร
11.2.2	การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร
11.3	**การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)**	
	มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อ กระบวนการทางธุรกิจน้อยที่สุด	

ตารางที่ 2.1 (ต่อ)

11.3.1	มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)	(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน
11.3.2	การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)	(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

บทที่ 3
การวิเคราะห์การบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

ระบบการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศได้ทำการพัฒนาระบบตามมาตรฐาน ISO/IEC Guide 73:2002 ตามที่ได้กล่าวไว้ในบทที่ 2 ซึ่งกระบวนการของการบริหารจัดการความเสี่ยงของระบบที่พัฒนาขึ้นโดยเริ่มจากการบริหารจัดการความเสี่ยงของทรัพย์สินเทคโนโลยีสารสนเทศซึ่งถือว่าเป็นทรัพย์สินอย่างหนึ่ง และเป็นทรัพย์สินที่มีมูลค่าสูง และเป็นทรัพย์สินที่ขาดไม่ได้สำหรับในองค์กรปัจจุบัน การที่จะทราบว่าทรัพย์สินหรือเทคโนโลยีสารสนเทศของเรานั้นมีความปลอดภัยหรือไม่นั้น เราจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงของทรัพย์สิน โดยระบบที่พัฒนาขึ้นนี้มีกระบวนการในการบริหารจัดการความเสี่ยงของทรัพย์สินที่เป็นเทคโนโลยีสารสนเทศตามขั้นตอนดังนี้

3.1 การจัดประเภท และการให้นิยามทรัพย์สินของระบบเทคโนโลยีสารสนเทศ

การบริหารจัดการความเสี่ยงของทรัพย์สินนั้น จะต้องทำการกำหนดถึงขอบเขตของการบริหารจัดการความเสี่ยงว่าต้องการจะทำการบริหารจัดการความเสี่ยงของทรัพย์สิน อะไรบ้าง โดยทำการจัดประเภทของทรัพย์สิน ว่าทรัพย์สินที่จะทำการบริหารจัดการความเสี่ยงนั้นสามารถจัดเป็นประเภทได้กี่ประเภทหลักๆ พร้อมกำหนดนิยามของแต่ละประเภทเพื่อให้มีความเข้าใจที่ตรงกันในแต่ละประเภทที่ได้มีการแยกประเภทไว้ ระบบฯแบ่งประเภททรัพย์สินในส่วนที่เป็นเทคโนโลยีสารสนเทศออกเป็น 5 ประเภท โดยให้นิยามในแต่ละประเภทของทรัพย์สินตามตารางที่ 3.1 (Queensland Government. 2005 ; Government Chief Information Office. 2007 : 8)

ตารางที่ 3.1 ตารางแสดงประเภททรัพย์สินและคำนิยามของทรัพย์สิน

ลำดับที่	ประเภททรัพย์สิน (เทคโนโลยีสารสนิทศ)	คำนิยามของทรัพย์สิน
1	Physical equipment, facilities and Hardware	เป็นกลุ่มของอุปกรณ์ที่ใช้ในกระบวนการทางด้านเทคโนโลยีสารสนเทศ หรือใช้ในการจัดเก็บเทคโนโลยีสารสนเทศ ซึ่งจะประกอบด้วยโฮสต์ เครื่องไคเอ็นต์ หรือเครื่องเซิรฟเวอร์ทุกเครื่องภายในระบบ
2	Data and Information	เป็นทรัพย์สินประเภทไฟล์ข้อมูล ไฟล์เอกสารต่างๆ ไฟล์ข้อมูลผลิตภัณฑ์ ไฟล์คู่มือ เป็นต้น

ตารางที่ 3.1 (ต่อ)

ลำดับที่	ประเภททรัพย์สิน (เทคโนโลยีสารสนิทศ)	คำนิยามของทรัพย์สิน
3	Paper Document	เป็นทรัพย์สินประเภทเอกสารสัญญา แบบฟอร์มต่างๆ
4	Software Application	เป็นทรัพย์สินประเภทดาต้าเบส แอพพลิเคชันที่ใช้งานอยู่ในสำนักงาน เป็นต้น
5	Service and Communication	เป็นทรัพย์สินประเภทการให้บริการทางอินเทอร์เน็ต การให้บริการทางด้าน WAN Link เป็นต้น

รายการทรัพย์สินทั้งหมดจะต้องทำการกำหนดมูลค่าความสำคัญ (Asset Value) โดยเป็นการกำหนดค่าความสำคัญของทรัพย์สินดังนี้ (EBIOS Club. 2004 : 21)

Confidentiality คือ ระดับการกำหนดหรือจำกัดสิทธิในการเข้าถึงทรัพย์สินต่างๆ ว่าทรัพย์สินนั้นมีระดับของการเข้าถึงทรัพย์สินอยู่ในระดับใดดังนี้

- Public ระดับที่มีความสำคัญในลักษณะสาธารณะ (ผู้ใดเข้าถึงก็ได้)
- Restricted ระดับต้องมีการจำกัดให้เฉพาะผู้ที่กำหนด
- Confidential (partners) ระดับที่เป็นความ
- Confidential (internal)
- Critical

Availability คือ ค่าความต้องการใช้งานของทรัพย์สิน ว่าทรัพย์สินนั้นต้องการให้มีความพร้อมในการใช้งานมากน้อยแค่ไหนต่อองค์กร

- No availability need ไม่จำเป็นต้องมีความพร้อมใช้งานของทรัพย์สิน
- Long term (specify) ระยะเวลาที่ต้องการให้มีความพร้อมในการใช้งานของทรัพย์สินมีในระยะเวลายาว
- Medium (specify) ระยะเวลาที่ต้องการให้มีความพร้อมในการใช้งานของทรัพย์สินมีในระยะเวลาปานกลาง
- Shot term ระยะเวลาที่ต้องการให้มีความพร้อมในการใช้งานของทรัพย์สินมีในระยะเวลาสั้น
- Very short term (specify) ระยะเวลาที่ต้องการให้มีความพร้อมในการใช้งานของทรัพย์สินมีในระยะเวลาสั้น หรือตลอดเวลา

Integrity คือ เฉพาะผู้ที่มีสิทธิสามารถเข้าถึงข้อมูลที่กำหนดได้เท่านั้น

- No Integrity need
- Medium integrity need
- Total integrity

ระบบที่พัฒนาใช้การพิจารณาประเภทของความปลอดภัยจัดเป็นระดับ โดยจัดเป็น 5 ระดับเริ่มตั้งแต่ระดับ 0 ถึงระดับ 4 ตามตารางที่ 3.2

ตารางที่ 3.2 ตารางแสดงระดับของความปลอดภัยโดยพิจารณาจาก Availability Integrity และ Confidentiality

Security needs	Availability	Integrity	Confidentiality
0	No availability need	No Integrity need	Public
1	Long term(specify)	(value not used)	Restricted
2	Medium(specify)	Medium integrity need	Confidential(partners)
3	Shot term	(value not used)	Confidential(internal)
4	Very shot term(specify)	Total integrity	Critical

ตารางที่ 3.3 มูลค่าและระดับความสำคัญ (EBIOS Club. 2004 : 24)

Asset Value (Availability+ Integrity+ Confidentiality)	ระดับความสำคัญ
0-1	ไม่มีมูลค่า/ความสำคัญ
2-3	มีมูลค่า/ความสำคัญในระดับน้อยมาก
4-5	มีมูลค่า/ความสำคัญในระดับน้อย
6-7	มีมูลค่า/ความสำคัญในระดับปานกลาง
8-10	มีมูลค่า/ความสำคัญในระดับสำคัญ
11-12	มีมูลค่า/ความสำคัญในระดับสำคัญมาก

ซึ่งเมื่อมีการกำหนดค่าความสำคัญแล้วจะสามารถกำหนดประเภทความสำคัญของทรัพย์สินนั้นๆ ได้ ดังตัวอย่าง

มูลค่าของทรัพย์สิน(Asset Value) = Availability + Integrity + Confidentiality

ยกตัวอย่างเช่น

มูลค่าของ Mail Server = 4 + 4 + 4 = 12 (มีความสำคัญในระดับสูงสุด (critical))

มูลค่าของ Client Hosts = 2 + 2+ 3 = 7 (มีความสำคัญในระดับปานกลาง (not critical))

3.2 การระบุและจำแนกภัยคุกคาม (Threat Identification)

ระบบฯได้กำหนดถึงภัยคุกคามที่จะเกิดขึ้นกับทรัพย์สินของระบบเทคโนโลยีสารสนเทศ ดังตารางที่ 3.4 (Government Chief Information Office. 2007 : 62-77)

ตารางที่ 3.4 ตารางแสดงภัยคุกคามที่สามารถเกิดขึ้นกับเทคโนโลยีสารสนเทศ

ลำดับที่	ภัยคุกคาม
1	แผ่นดินไหว
2	ลมภายุ
3	ไฟ
4	ระบบน้ำขัดข้อง
5	ระเบิด
6	ระบบไฟฟ้าขัดข้อง
7	ก่อความเสียหายอย่างจงใจ
8	ใช้ซอฟต์แวร์โดยผู้ที่ไม่ได้รับอนุญาต (Use of software by unauthorized users)
9	ใช้ซอฟต์แวร์ผิดกฎหมาย (Illegal use of software)
10	ซอฟต์แวร์ประสงค์ร้าย (Malicious software)
11	ฮาดแวร์ขัดข้อง (Hardware failures)
12	เข้าถึงเครือข่ายโดยผู้ที่ไม่ได้รับอนุญาต (Network access by unauthorized users)
13	อุณหภูมิและความชื้นสูง/ต่ำมาก (Extremes of temperature and humidity)
14	การกระจายรังสีอิเลคโตรแมคเนติค (Electromagnetic radiation)
15	ประจุไฟฟ้าสถิต (Electrostatic charging)
16	ดักฟัง (Eavesdropping)
17	ใช้สื่อเก็บข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized use of storage media)
18	Deterioration of storage media
19	ความผิดพลาดของเจ้าหน้าที่ปฏิบัติการ (Operational staff error)
20	ความผิดพลาดในการบำรุงรักษา (Maintenance error)
21	ปฏิเสธตัวตน ความรับผิดชอบ (Repudiation)
22	ใช้ทรัพยากรไม่ถูกต้อง (Misuse of resources)
23	ขาดแคลนบุคคลากร (Staff shortage)
24	น้ำท่วม

ตารางที่ 3.4 (ต่อ)

ลำดับที่	ภัยคุกคาม
25	ฟ้าผ่า
26	ฝุ่น
27	ระบบปรับอากาศขัดข้อง
28	ใช้กำลัง-อาวุธ
29	ไฟฟ้ากระเพื่อม (Power fluctuation)
30	โจร-ขโมย
31	ใช้ซอฟต์แวร์ในทางที่ไม่ได้รับอนุญาต (Use of software in an unauthorized way)
32	นำเข้า-ส่งออกซอฟต์แวร์อย่างผิดกฎหมาย (Illegal import/export of software)
33	ปลอมแปลงตัวตนผู้ใช้ (Masquerading of user identity)
34	ซอฟต์แวร์ขัดข้อง (Software Failure)
35	ใช้ network facilities ในทางที่ไม่ได้รับอนุญาต (Use of network facilities in an unauthorized way)
36	ขัดข้องทางเทคนิคของเครือข่าย (Technical failure of network components)
37	ข้อผิดพลาดของการรับส่ง (Transmission errors)
38	สายเสียหาย-ถูกทำลาย (Damage to lines)
39	Traffic overloading
40	ดุกคาม-ยึดครองการสื่อสาร (Communications infiltration)
41	วิเคราะห์เพื่อหาทางโจมตีการรับส่งข้อมูล (Traffic analysis)
42	ส่งข้อความผิดเส้นทาง (Misrouting of messages)
43	เปลี่ยนเส้นทางข้อความ (Rerouting of messages)
44	Failure of communications services (i.e. network services)
45	ความผิดพลาดของผู้ใช้ (User errors)
46	Industrial Action

3.3 การระบุและจำแนกช่องโหว่ หรือความอ่อนแอของระบบ (Vulnerability Identification)

ระบบได้กำหนดช่องโหว่ของระบบเทคโนโลยีสารสนเทศตามตารางที่ 3.5 (Government Chief Information Office. 2007 : 77-82)

ตารางที่ 3.5 ตารางแสดงช่องโหว่ของระบบสารสนเทศ

Environment and Infrastructure	
Vulnerability	**Possible exploitation**
ขาดการป้องกัน ประตู หน้าต่าง (Lack of physical protection of the building, doors, and windows)	ภัยจากการโจรกรรม (The threat of theft)
ระบบควบคุมการเข้าออกอาคาร-ห้อง ขาดการเอาใจใส่/ไม่เพียงพอ (Inadequate or careless use of physical access control to buildings, rooms)	ภัยจากผู้ประสงค์ร้าย (The threat of willful damage)
ระบบไฟฟ้าไม่มีเสถียรภาพ (Unstable power grid)	ภัยจากกำลังไฟฟ้าเปลี่ยนแปลงสูง-ต่ำมากเกินไป (The threat of power fluctuation)
สถานที่ตั้งอยู่ในพื้นที่เสี่ยงต่อการถูกน้ำท่วม (Location in an area susceptible to flood)	ภัยจากน้ำท่วม (The threat of flooding)
Hardware	
Vulnerability	**Possible exploitation**
ขาดแบบแผนในการเปลี่ยนอุปกรณ์ตามระยะอายุการใช้งาน (Lack of periodic replacement schemes)	ภัยจากสื่อบันทึก (ข้อมูล) เสื่อมสภาพ (The threat of deterioration of storage media)
ความอ่อนไหวต่อการถูกกระทบกระเทือนจากศักดิ์ไฟฟ้าที่ผันแปร (Susceptibility to voltage variations)	ภัยจากกำลังไฟฟ้าเปลี่ยนแปลงสูง-ต่ำมากเกินไป (The threat of power fluctuation)
ความอ่อนไหวต่อการถูกกระทบกระเทือนจากอุณหภูมิที่ผันแปร (Susceptibility to temperature variations)	ภัยจากอุณหภูมิสูง-ต่ำมากๆ (The threat of extremes of temperature)
ความอ่อนไหวต่อการถูกกระทบกระเทือนจากความชื้น ฝุ่น ดิน (Susceptibility to humidity, dust, soiling)	ภัยจากฝุ่น (The threat of dust)
ไวต่อการแผ่คลื่นแม่เหล็กไฟฟ้า (Sensitivity to electromagnetic radiation)	ภัยจากการแผ่คลื่นแม่เหล็กไฟฟ้า (The threat of electromagnetic radiation)

ตารางที่ 3.5 (ต่อ)

ขาดการควบคุมการเปลี่ยนการคอนฟิคอย่างมีประสิทธิภาพ (Lack of efficient configuration change control)	ภัยจากความผิดพลาดของเจ้าหน้าที่ปฏิบัติการ (The threat of operational staff error)
Software	
Vulnerability	**Possible exploitation**
ข้อกำหนดสำหรับผู้พัฒนา(ระบบ) ไม่ชัดเจน หรือ ไม่ครบถ้วน (Unclear or incomplete specifications for developers)	ภัยจากซอฟต์แวร์ล้มเหลว (The threat of software failure)
การทดสอบ ซอฟต์แวร์ไม่มี หรือ ไม่เพียงพอ (No or insufficient software testing)	ภัยจากการใช้ ซอฟต์แวร์โดยผู้ใช้ที่ไม่ได้รับอนุญาต (The threat of use of software by unauthorized users)
ยูสเซอร์อินเตอร์เฟส ซับซ้อน (ใช้งานยาก) (Complicated user interface)	ภัยจากความผิดพลาดของเจ้าหน้าที่ปฏิบัติการ (The threat of operational staff error)
ขาดกลไกเพื่อระบุและยืนยันตัวตน เช่น การยืนยันตัวตนผู้ใช้ (Lack of identification and authentication mechanisms like user authentication)	ภัยจากการปลอมแปลงตัวตนผู้ใช้ (The threat of masquerading of user identity)
ขาด บันทึกเพื่อการตรวจสอบ (Lack of audit-trail)	ภัยจากการใช้ ซอฟต์แวร์ในทางที่ไม่ได้รับอนุญาต (The threat of use of software in an unauthorized way)
จุดบกพร่องของ ซอฟต์แวร์ ที่เป็นที่ทราบกันดี (Well-known flaws in the software)	ภัยจากการใช้ ซอฟต์แวร์โดยผู้ใช้ที่ไม่ได้รับอนุญาต (The threat of use of software by unauthorized users)
ไม่ป้องกันตาราง (password Unprotected password tables)	Tภัยจากการปลอมแปลงตัวตนผู้ใช้ (the threat of masquerading of user identity)
บริหารพาสเวิร์ด ไม่ดี (Poor password management easily guessable passwords, storing of passwords in clear, insufficient frequency of change)	ภัยจากการปลอมแปลงตัวตนผู้ใช้ (The threat of masquerading of user identity)

ตารางที่ 3.5 (ต่อ)

จัดสรรสิทธิการเข้าถึงไม่ถูกต้อง (Wrong allocation of access rights)	ภัยจากการใช้ ซอฟต์แวร์ในทางที่ไม่ได้รับอนุญาต (The threat of use of software in an unauthorized way)
ไม่มีการควบคุมการดาวน์โหลด และการใช้ซอฟต์แวร์ (Uncontrolled downloading and using software)	ภัยจาก ซอฟต์แวร์ร้าย (The threat of malicious software)
ไม่ล็อกเอาท์เมื่อไม่อยู่ที่เครื่อง (No 'logout' when leaving the workstation)	ภัยจากการใช้ ซอฟต์แวร์โดยผู้ใช้ที่ไม่ได้รับอนุญาต (Unauthorized users)
ขาดการควบคุมการเปลี่ยนแปลงที่มีประสิทธิภาพ (Lack of effective change control)	ภัยจาก ซอฟต์แวร์ล้มเหลว (The threat of software failure)
ขาดการจัดทำเอกสาร (Lack of documentation)	ภัยจากความผิดพลาดของเจ้าหน้าที่ปฏิบัติการ (The threat of operational staff error)
ขาด ซอฟต์แวร์สำรอง (สำเนา) (Lack of back-up copies)	ภัยจาก ซอฟต์แวร์ร้าย หรืออัคคีภัย (The threat of malicious software or the threat of fire)
สื่อบันทึก (ข้อมูล)ทิ้ง-นำมาใช้ใหม่ โดยมิได้ลบข้อมูลเก่าอย่างเหมาะสม (Disposal or reuse of storage media without proper erasure)	ภัยจากการใช้ ซอฟต์แวร์โดยผู้ใช้ที่ไม่ได้รับอนุญาต (The threat of use of software by unauthorized users)
Communications	
Vulnerability	**Possible exploitation**
สาย (เส้นทางการสื่อสาร) ที่ไม่มีการป้องกัน (Unprotected communication lines)	ภัยจากการลอบดักฟัง (The threat of eavesdropping)
เชื่อมต่อสายไม่ดี(Poor joint cabling)	ภัยจากการแทรกซึมการสื่อสาร(The threat of communications infiltration)
ขาดการระบุและยืนยันตัวตนของผู้รับ-ผู้ส่ง (lack of identification and authentication of sender and receiver)	ภัยจากการปลอมแปลงตัวตนผู้ใช้ (The threat of masquerading of user identity)
ส่งพาสเวิร์ดเป็นข้อความธรรมดา(ไม่เข้ารหัส) (Transfer of passwords in clear)	ภัยจากการใช้เครือข่ายโดยผู้ใช้ที่ไม่ได้รับอนุญาต (The threat of network access by unauthorized users)

ตารางที่ 3.5 (ต่อ)

ขาดหลักฐาน (ที่ใช้พิสูจน์) การรับ-ส่งข่าวสาร (Lack of proof of sending or receiving a message)	ภัยจากการปฏิเสธ การกระทำ/ผู้กระทำ (The threat of repudiation)
การเชื่อมต่อทางสายโทรศัพท์ (Dial-up lines)	ภัยจากการใช้เครือข่ายโดยผู้ใช้ที่ไม่ได้รับอนุญาต (The threat of network access by unauthorized users)
การรับ-ส่งข้อมูลข่าวสารที่ละเอียดอ่อนโดยไม่มีการป้องกัน (Unprotected sensitive traffic)	ภัยจากการลอบดักฟัง (The threat of eavesdropping)
การบริหารจัดการเส้นทางเครือข่ายให้พร้อมใช้ไม่ดีพอ(Inadequate network management resilience of routing)	ภัยจากความคับคั่งในการรับ-ส่งข้อมูลข่าวสาร (The threat of traffic overloading)
การเชื่อมต่อกับเครือข่ายสาธารณะโดยไม่มีการป้องกัน (อินเทอร์เน็ต โดยไม่มี ไฟร์วอลล์) (Unprotected public network connections)	ภัยจากการใช้ ซอฟต์แวร์โดยผู้ใช้ที่ไม่ได้รับอนุญาต (The threat of use of software by unauthorized users)
Documents	
Vulnerability	**Possible exploitation**
ที่เก็บไม่มีการป้องกัน (Unprotected storage)	ภัยจากการโจรกรรม (The threat of theft)
ขาดการดูแลที่ทิ้งเอกสาร (Lack of care at disposal)	ภัยจากการโจรกรรม (The threat of theft)
ไม่มีการควบคุมการทำสำเนา (Uncontrolled copying)	ภัยจากการโจรกรรม (The threat of theft)
Personnel	
Vulnerability	**Possible exploitation**
บุคลากรไม่อยู่ (Absence of personnel)	ภัยจากการขาดพนักงาน (The threat of staff shortage)
ขาดการสอดส่องดูแลการทำงานของบุคคลภายนอก หรือ พนง.ทำความสะอาด (Unsupervised work by outside or cleaning staff)	ภัยจากการโจรกรรม (The threat of theft)

ตารางที่ 3.5 (ต่อ)

ฝึกอบรมทางด้านความมั่นคงปลอดภัยที่ไม่เพียงพอ (Insufficient security training)	ภัยจากความผิดพลาดของเจ้าหน้าที่ปฏิบัติการ (The threat of operational staff error)
ขาดการตระหนักถึงเรื่องความมั่นคงปลอดภัย (security Lack of security awareness)	ภัยจากความผิดพลาดของผู้ใช้ (The threat of user errors)
ใช้ ซอฟต์แวร์ และ ฮาร์ดแวร์ ไม่ถูกต้อง (Incorrect use of software and hardware)	ภัยจากความผิดพลาดของเจ้าหน้าที่ปฏิบัติการ (The threat of operational staff error)
ขาดกลไกการดูแล-เตือนภัย (Lack of monitoring mechanisms)	ภัยจากการใช้ ซอฟต์แวร์ในทางที่ไม่ได้รับอนุญาต (The threat of use of software in an unauthorized way)
ขาด นโยบาย การใช้งานสื่อโทรคมนาคมและข่าวสารที่ถูกต้อง (Lack of policies for the correct use of telecommunications media and massaging)	ภัยจากการใช้เครื่องมือสื่อสารในทางที่ไม่ได้รับอนุญาต (The threat of use of network facilities in an unauthorized way)
ขบวนการคัดสรรไม่รัดกุมเพียงพอ (Inadequate recruitment procedures)	ภัยจากผู้ประสงค์ร้าย (The threat of willful damage)
Generally applying vulnerabilities	
Vulnerability	**Possible exploitation**
ขาดระบบสำรอง-ทดแทน (Single point of failure)	ภัยจากบริการสื่อสารขัดข้อง (The threat of failure of communications services)
ขาดการตอบสนองการบำรุงรักษาการให้บริการอย่างพอเพียง (Inadequate service maintenance response)	ภัยจากระบบฮาร์ดแวร์ล้มเหลว (The threat of hardware failures)

3.4 การพิจารณาโอกาสที่จะเกิดเหตุการณ์ที่ถือว่าเป็นภัยคุกคาม (Likelihood Determination)

การพิจารณาอัตราของโอกาสที่จะเกิดเหตุการณ์จะพิจารณาจากความน่าจะเป็น หรือความเป็นไปได้จากช่องโหว่ของระบบที่เป็นต้นเหตุที่จะทำให้เกิดภัยคุกคามขึ้น สำหรับระบบฯที่พัฒนาขึ้นนั้นจะทำการจัดระดับของโอกาสที่จะเกิดเหตุการณ์ โดยพิจารณาจากความถี่ของ

เหตุการณ์ที่เกิดขึ้น สามารถอธิบายลำดับของโอกาสที่จะเกิดภัยคุกคามนั้น ตามตารางที่ 3.6 (Government Chief Information Office. 2007 : 58-59)

ตารางที่ 3.6 ตารางแสดงระดับของโอกาสที่จะเกิดเหตุการณ์

likelihood Level	Likelihood Description	Indicative Frequency
Improbable	Practically impossible	In any time frame
Remote	Not expected to occur	In a 10 year period
Occasional	May occur	In a 5 year period
Probable	Isolated incidents	In a 3 year period
Frequent	Repeated incidents	In a year

3.5 การพิจารณาผลกระทบที่เกิดขึ้น (Consequences Determination)

การวิเคราะห์ผลกระทบที่เกิดขึ้นจากเหตุการณ์โดยวิเคราะห์ผลกระทบจากมูลค่าความสำคัญของทรัพย์สิน และความเสียหายที่จะเกิดขึ้นกับทรัพย์สินจากเหตุการณ์ที่เกิดขึ้น โดยได้ทำการจัดระดับของผลกระทบที่จะเกิดจากเหตุการณ์นั้นๆ ตามตารางที่ 3.7 (Government Chief Information Office. 2007 : 59-60)

ตารางที่ 3.7 ตารางแสดงระดับของผลกระทบ

Type of Consequence	Consequence Severity				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Loss of Financial	Minimal	Insignificant	Significant	Very Significant	Critical
Damage to reputation	Minimal	Insignificant	Damage	Significant	Very Significant
Degrade to operate critical Infrastructure	No degradation	Minimal	Noticeable	Significant	Very Significant

3.6 การพิจารณาความเสี่ยง (Risk Determination)

การพิจารณาความเสี่ยงจะทำการพิจารณาจากโอกาสที่จะเกิดเหตุการณ์รวมกับผลกระทบที่จะเกิดขึ้น โดยเป็นการพิจารณาในลักษณะที่เป็นเมตริกซ์ เพื่อจัดระดับความเสี่ยงที่จะเกิดขึ้น (Government Chief Information Office. 2007 : 61)

ตารางที่ 3.8 ตารางแสดงระดับความเสี่ยง (Risk level)

Likelihood	Consequence Severity				
	Negligible	Minor	Moderate	Major	Extreme
Frequent	Medium	High	High	Very High	Very High
Probable	Medium	Medium	High	High	Very High
Occasional	Low	Medium	High	High	High
Remote	Low	Low	Medium	Medium	High
Improbable	Low	Low	Medium	Medium	High

จากตารางที่ 3.8 จะแสดงถึงระดับความเสี่ยงโดยเป็นความสัมพันธ์ระหว่างผลกระทบ และโอกาสที่จะเกิด โดยแบ่งระดับของความเสี่ยงออกเป็น 4 ระดับ ดังนี้

Low คือ ระดับความเสี่ยงต่ำ

Medium คือ ระดับความเสี่ยงปานกลาง

High คือ ระดับความเสี่ยงสูง

Very High คือ ระดับความเสี่ยงสูงมาก

3.7 การประเมินความเสี่ยง (Risk Analysis)

การพิจารณาความเสี่ยงโดยเป็นการวิเคราะห์ความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลที่จะตามมาจากเหตุการณ์ที่เกิดขึ้น ดังนี้ (Shon. 2005 : 70)

Annualized loss expectancy (ALE) คือ ค่าความสูญเสียที่เกิดขึ้นจากความเสี่ยง โดยสามารถคำนวณได้จาก ค่า SLE คูณกับอัตราโอกาสที่จะเกิดความเหตุการณ์ต่อหนึ่งปี ซึ่งค่า SLE สามารถหาได้จาก มูลค่าของทรัพย์สินคูณเปอร์เซ็นต์ความเสียหายของทรัพย์สินจากเหตุการณ์นั้น

$$ALE = SLE * \text{annualized rate of occurrence (ARO)} \quad (6.1)$$

$$SLE = \text{asset value} * \text{exposure factor (EF)} \quad (6.2)$$

บทที่ 4
การออกแบบระบบการบริหารจัดการความเสี่ยงทางด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

ในการพัฒนาระบบการวิเคราะห์ความเสี่ยงทางด้านความปลอดภัยในการใช้งานระบบสารสนเทศได้ทำการวิเคราะห์และออกแบบระบบงานตามทฤษฎีของ SDLC (System Development Life Cycle) ประกอบด้วยแผนบริบท (Context Diagram) แผนภาพกระแสการไหลของข้อมูล (Data Flow Diagram) และผังโครงสร้าง (Structure Chart)

4.1 แผนภาพบริบท (Context Diagram)

การออกแบบระบบฯ นั้นจะทำการออกแบบระบบตามที่ได้มีการกำหนดรูปแบบสำหรับการวิเคราะห์ความเสี่ยงในการใช้งานระบบสารสนเทศที่ได้กล่าวไว้แล้วในบทที่ 3 โดยการนำแผนภาพบริบท (Context Diagram) มาใช้ในการอธิบายถึงขอบเขตของระบบและผู้ที่มีส่วนเกี่ยวข้องกับระบบ ซึ่งสามารถดูแผนภาพบริบท(Context diagram) ได้จากรูปที่ 4.1 แผนภาพบริบทจะได้แสดงถึงไหลของข้อมูลในภาพรวมว่าแต่ละผู้ที่เกี่ยวข้องกับระบบมีความสัมพันธ์อะไรกับระบบ ทำการกำหนดข้อมูลใดบ้างให้กับระบบและได้รับข้อมูลอะไรบ้างจากระบบ ผู้ที่เกี่ยวข้องจะประกอบด้วย 4 ผู้เกี่ยวข้อง คือ ผู้กำหนดการวิเคราะห์ความเสี่ยง ผู้รับผิดชอบต่อทรัพย์สิน เจ้าหน้าที่สารสนเทศ และผู้บริหาร โดยหน้าที่ความสัมพันธ์และความเกี่ยวข้องของผู้ที่เกี่ยวข้องมีรายละเอียดดังนี้

- **ผู้กำหนดการวิเคราะห์ความเสี่ยง**

  <u>บทบาท</u> : เป็นผู้ที่มีความชำนาญทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Security Specialist)

  <u>ความเกี่ยวข้องกับระบบ</u> : ทำการกำหนดข้อมูลทรัพย์สิน ข้อมูลช่องโหว่และข้อมูลภัยคุกคามให้กับระบบ รวมถึงการกำหนดช่องโหว่ให้กับทรัพย์สิน การกำหนดภัยคุกคามให้กับช่องโหว่ และการกำหนดการควบคุมความเสี่ยงให้กับภัยคุกคาม

- **ผู้รับผิดชอบต่อทรัพย์สิน**

  <u>บทบาท</u> : เป็นคนดูแลทรัพย์สินหรือเป็นเจ้าของทรัพย์สิน ซึ่งจะทราบถึงรายละเอียดของทรัพย์สินที่ดูแลหรือรับผิดชอบ

ความสัมพันธ์กับระบบ : จะทำการระบุทรัพย์สินของบริษัทรวมถึงรายละเอียดต่างๆ ของทรัพย์สินของบริษัทให้กับระบบ และระบบจะทำการออกรายงานความเสี่ยงของทรัพย์สินให้กับผู้รับผิดชอบต่อทรัพย์สิน

- **เจ้าหน้าที่สารสนเทศ**

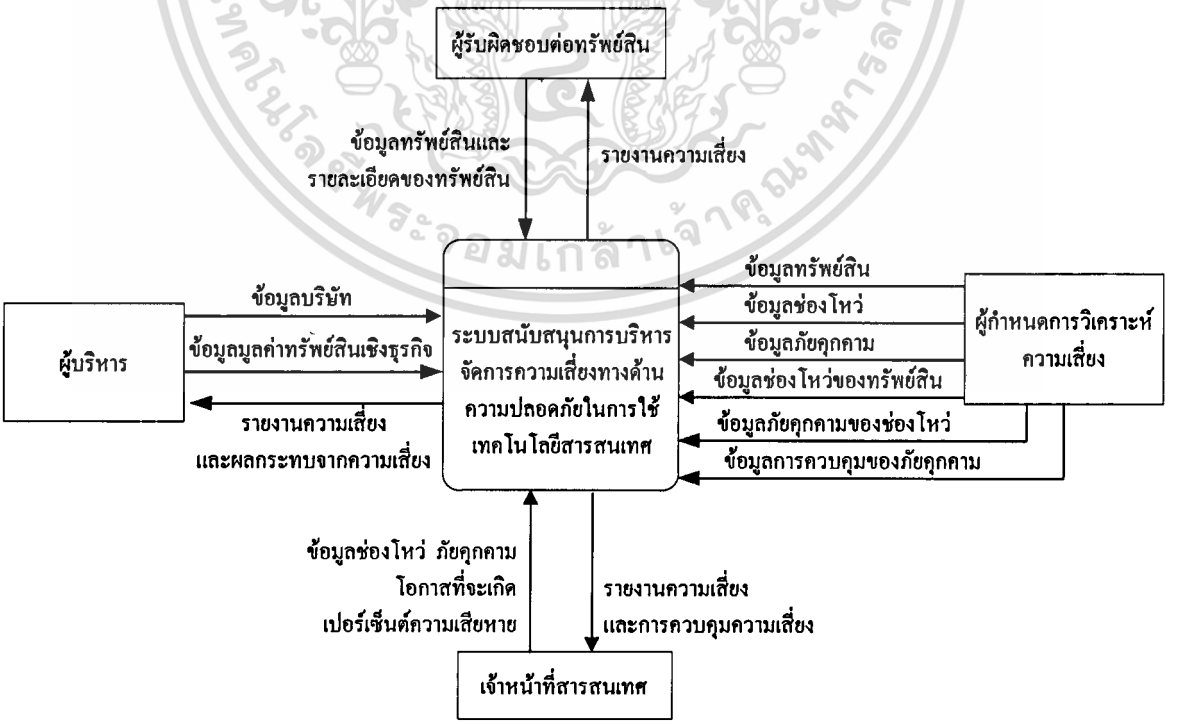
บทบาท : ผู้ที่ดูแลระบบสารสนเทศขององค์กร ซึ่งจะเป็นผู้ที่ทราบถึงข้อมูลของระบบสารสนเทศที่ได้มีการใช้งาน มีความรู้พื้นฐานทางด้านสารสนเทศ และความมั่นคงปลอดภัยของระบบสารสนเทศ

ความสัมพันธ์กับระบบ : จะทำการระบุข้อมูลช่องโหว่ และข้อมูลภัยคุกคามที่คาดว่าหรือมีโอกาสที่จะเกิดขึ้นกับทรัพย์สินของบริษัท รวมถึงโอกาสที่จะเกิดช่องโหว่และภัยคุกคามนั้นภายใน 1 ปี เปอร์เซ็นต์ความเสียหายที่จะเกิดขึ้นจากช่องโหว่และภัยคุกคามนั้น

- **ผู้บริหาร**

บทบาท : ผู้ที่สามารถกำหนด หรือทราบถึงความสำคัญและมูลค่าของทรัพย์สินทั้งทางด้านการทำกำไรให้กับบริษัท ผลกระทบต่อธุรกิจของบริษัท หรือต่อระบบอื่นๆ

ความสัมพันธ์กับระบบ : จะทำทำการระบุข้อมูลมูลค่าของทรัพย์สินของบริษัทให้กับระบบ



รูปที่ 4.1 แสดงแผนภาพบริบท (Context Diagram)

4.2 แผนภาพกระแสการไหลของข้อมูล

จากแผนภาพบริบท (Context Diagram) สามารถนำมาออกแบบแผนภาพกระแสการไหลของข้อมูล โดยประกอบด้วย 7 กระบวนการทำงานหลักๆ ของระบบ ดังรูปที่ 4.2 ซึ่งแสดงข้อมูลที่เกี่ยวข้องกับแต่ละกระบวนการและความสัมพันธ์กับผู้ที่เกี่ยวข้อง ทำให้ทราบว่าระบบมีลำดับการทำงานอย่างไรและมีการรับส่งข้อมูลอย่างไร การออกแบบแผนภาพการไหลของข้อมูลได้ทำการออกแบบกระบวนการทำงานหลักๆ นั้นคือ แผนภาพกระแสการไหลของข้อมูลในระดับ 0 และได้ทำการออกแบบเป็นแผนภาพกระแสการไหลของข้อมูลที่เป็นการแตกจากกระบวนการหลักๆ จากแผนผังการไหลของข้อมูลในระดับ 0 ไปเป็นกระบวนการย่อยๆ โดยเป็นแผนภาพกระแสการไหลของข้อมูลระดับ 1 จนถึงระดับ 3 ซึ่งการอธิบายแผนภาพกระแสการไหลของข้อมูลสามารถอธิบายได้ดังนี้

4.2.1 แผนภาพกระแสการไหลของข้อมูลระดับ 0 (DFD Diagram 0)

แผนภาพกระแสการไหลของข้อมูลในระดับที่ 0 จะประกอบด้วยกระบวนการหลักๆ ทั้งหมด 7 กระบวน สามารถอธิบายกระบวนการต่างๆ ตามรูปที่ 4.2 ได้ดังนี้

<u>กระบวนการที่ 1</u> การจัดการข้อมูลทรัพย์สิน ภัยคุกคาม และช่องโหว่ให้กับระบบ

- ระบบดึงข้อมูลทรัพย์สิน จากตารางข้อมูลทรัพย์สิน ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการกำหนดข้อมูลทรัพย์สิน แล้ว ระบบจะทำการบันทึก แก้ไข หรือลบข้อมูลทรัพย์สินนั้นลงตารางข้อมูลทรัพย์สิน
- ระบบเรียกดึงข้อมูลช่องโหว่ จากตารางข้อมูลช่องโหว่ ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการกำหนดข้อมูลช่องโหว่ของระบบสารสนเทศให้กับระบบ แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบข้อมูลช่องโหว่ลงในตารางข้อมูลช่องโหว่
- ระบบดึงข้อมูลภัยคุกคาม จากตารางข้อมูลภัยคุกคาม ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการกำหนดข้อมูลภัยคุกคามที่มีโอกาสจะเกิดขึ้นกับทรัพย์สินของระบบสารสนเทศให้กับระบบ แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบข้อมูลภัยคุกคามลงในตารางข้อมูลภัยคุกคาม

<u>กระบวนการที่ 2</u> การจัดการการวิเคราะห์ความเสี่ยงและการควบคุม

- ระบบดึงข้อมูลทรัพย์สิน จากตารางข้อมูลทรัพย์สิน และข้อมูลช่องโหว่ จากตารางข้อมูลช่องโหว่ ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการกำหนดช่อง

โหว่ให้กับทรัพย์สิน แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบข้อมูลช่องโหว่ที่กำหนดให้กับทรัพย์สินลงในตารางข้อมูลช่องโหว่ของแต่ละทรัพย์สิน

- ระบบดึงข้อมูลช่องโหว่ จากตารางข้อมูลช่องโหว่ และข้อมูลภัยคุกคาม จากตารางข้อมูลภัยคุกคาม ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการกำหนดภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบภัยคุกคามที่กำหนดให้กับช่องโหว่ลงในตารางข้อมูลภัยคุกคามของแต่ละช่องโหว่

- ระบบดึงข้อมูลภัยคุกคาม จากตารางข้อมูลภัยคุกคาม และดึงข้อมูลการควบคุมความเสี่ยง จากตารางข้อมูลการควบคุมความเสี่ยง ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการกำหนดการควบคุมความเสี่ยงของทรัพย์สินให้กับภัยคุกคาม แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบการควบคุมที่กำหนดให้กับภัยคุกคามลงในตารางข้อมูลการควบคุมความเสี่ยงของภัยคุกคาม

<u>กระบวนการที่ 3</u> การลงทะเบียนและจัดเก็บข้อมูลบริษัท

- ถ้า ผู้บริหารทำการลงทะเบียนข้อมูลบริษัท (เช่น ชื่อบริษัท ที่อยู่ เป็นต้น) แล้ว ระบบจะทำการบันทึกข้อมูลของบริษัทลงในตารางข้อมูลของบริษัท

<u>กระบวนการที่ 4</u> การจัดการการระบุทรัพย์สินและรายละเอียดของทรัพย์สิน

- ระบบดึงข้อมูลของบริษัท จากตารางข้อมูลของบริษัท และดึงข้อมูลทรัพย์สิน จากตารางข้อมูลทรัพย์สิน ที่ผู้กำหนดการวิเคราะห์ความเสี่ยงได้กำหนดไว้ ถ้า ผู้รับผิดชอบต่อทรัพย์สินทำการกรอกข้อมูลทรัพย์สินของบริษัทและรายละเอียดของทรัพย์สิน (ประเภททรัพย์สิน คลาสทรัพย์สิน จำนวน สถานที่ตั้ง เจ้าของ เป็นต้น) แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบข้อมูลทรัพย์สินของบริษัทลงในตาราง

<u>กระบวนการที่ 5</u> การจัดการการระบุช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท

- ระบบดึงข้อมูลทรัพย์สินของบริษัท จากตารางข้อมูลทรัพย์สินของบริษัท ดึงข้อมูลช่องโหว่ของแต่ละทรัพย์สิน จากตารางข้อมูลช่องโหว่ของแต่ละทรัพย์สิน และดึงข้อมูลภัยคุกคามของแต่ละช่องโหว่ จากตารางข้อมูลภัยคุกคามของแต่ละช่องโหว่ ถ้า เจ้าหน้าที่สารสนเทศระบุข้อมูลช่องโหว่ ภัยคุกคาม โอกาสที่จะเกิดภัยคุกคาม และเปอร์เซ็นต์ความเสียหายของทรัพย์สิน แล้ว ระบบจะทำการการบันทึก แก้ไข หรือลบข้อมูลช่องโหว่ ภัยคุกคาม

โอกาสที่จะเกิดภัยคุกคาม และเปอร์เซ็นต์ความเสียหายของทรัพย์สินลงในตารางข้อมูลช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท

<u>กระบวนการที่ 6</u> การจัดการมูลค่าทรัพย์สินและคำนวณค่าความเสี่ยง

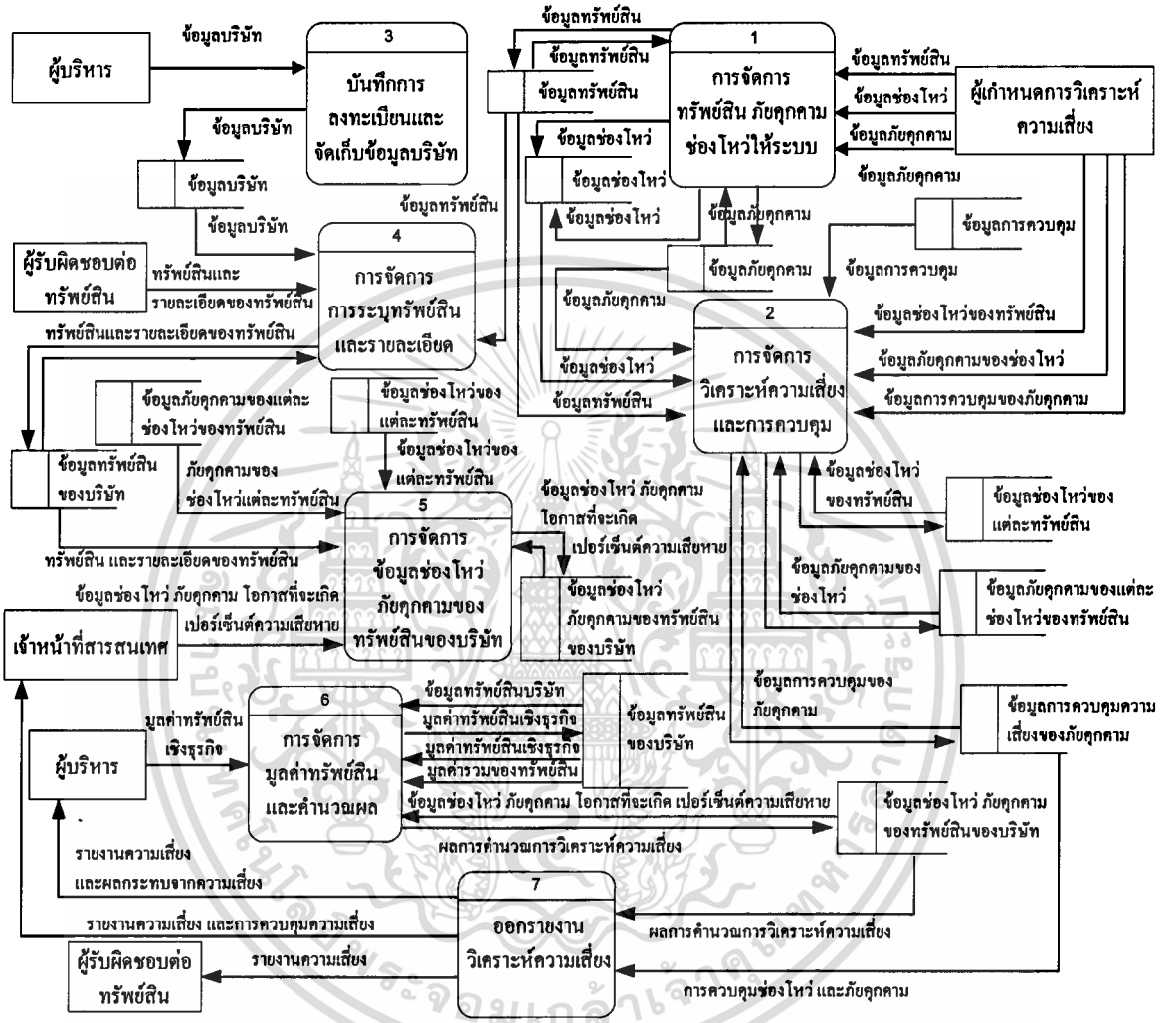
- ระบบดึงข้อมูลทรัพย์สินของบริษัท จากตารางข้อมูลทรัพย์สินของบริษัท และดึงข้อมูลช่องโหว่ ภัยคุกคามของบริษัท จากตารางข้อมูลช่องโหว่ ภัยคุกคามของบริษัท ถ้า ผู้บริหารทำการตรวจสอบการกรอกข้อมูลของผู้รับผิดชอบต่อทรัพย์สินและเจ้าหน้าที่สารสนเทศ แล้วถ้า ผู้บริหารทำการระบุข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจ แล้ว ระบบทำการการบันทึก แก้ไข หรือลบข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจลงในตารางข้อมูลทรัพย์สินของบริษัท
- ระบบดึงข้อมูลทรัพย์สินของบริษัท จากตารางข้อมูลทรัพย์สินของบริษัท ดึงข้อมูลช่องโหว่ ภัยคุกคาม โอกาสที่จะเกิดภัยคุกคาม และเปอร์เซ็นต์ความเสียหายของทรัพย์สินจากตารางข้อมูลช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท ถ้า ข้อมูลที่ระบบดึงขึ้นมาทั้งหมดมีค่า แล้ว ระบบจะทำการประมวลผลหาค่าความเสี่ยง และความเสียหายที่จะเกิดขึ้นกับทรัพย์สินในแต่ละช่องโหว่ และภัยคุกคาม แล้ว ทำการการบันทึก แก้ไข หรือลบผลการคำนวณค่าความเสี่ยงลงในตารางตารางข้อมูลช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท

<u>กระบวนการที่ 7</u> การออกรายงาน และแนวทางในการลดความเสี่ยง

- ถ้า ผู้บริหารต้องการรายงานค่าความเสี่ยงและผลกระทบจากความเสี่ยง แล้ว ระบบจะทำการออกรายงานค่าความเสี่ยงและผลกระทบจากความเสี่ยง โดยดึงข้อมูลผลการคำนวณค่าความเสี่ยงจากตารางข้อมูลช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท
- ถ้า เจ้าหน้าที่สารสนเทศต้องการรายงานค่าความเสี่ยงและการควบคุมความเสี่ยง แล้ว ระบบจะทำการออกรายงานค่าความเสี่ยงและการควบคุมความเสี่ยง โดยดึงข้อมูลข้อมูลผลการคำนวณค่าความเสี่ยงจากตารางข้อมูลช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท และดึงข้อมูลการควบคุมภัยคุกคามของช่องโหว่ของทรัพย์สิน จากตารางข้อมูลการควบคุมความเสี่ยงของภัยคุกคาม
- ถ้า ผู้รับผิดชอบต่อทรัพย์สินต้องการรายงานค่าความเสี่ยง แล้ว ระบบจะทำการออกรายงานค่าความเสี่ยงและการควบคุมความเสี่ยง โดยดึงข้อมูลข้อมูล

ผลการคำนวณค่าความเสี่ยงจากตารางข้อมูลช่องโหว่ ภัยคุกคามของทรัพย์สินของบริษัท

DFD 0 : ระบบสนับสนุนการบริหารจัดการความเสี่ยงทางด้านความปลอดภัยในการใช้เทคโนโลยีสารสนเทศ

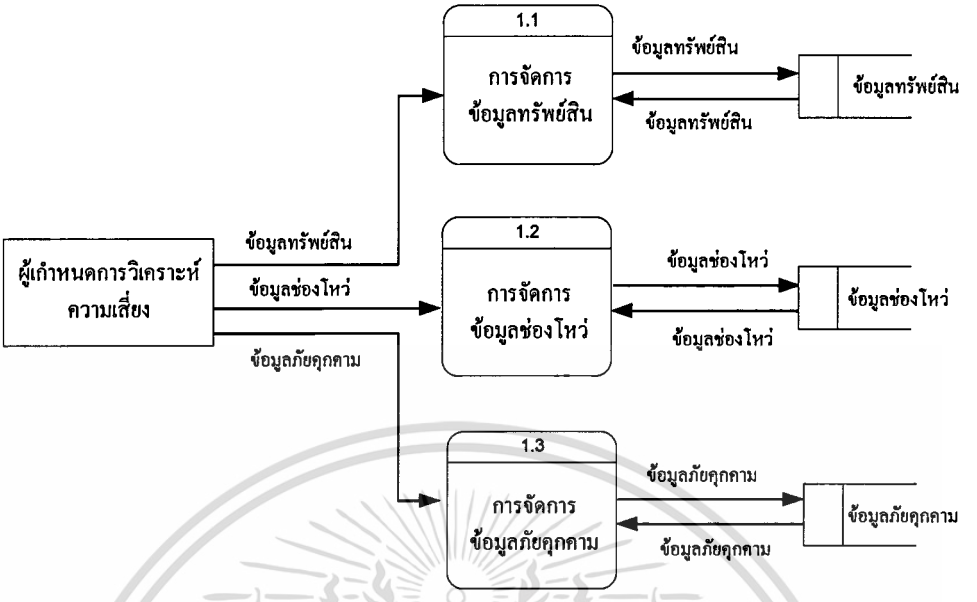


รูปที่ 4.2 แสดงแผนภาพการไหลข้อมูล แผนภาพที่ 0 ของระบบ

4.2.2 แผนภาพกระแสการไหลของข้อมูลระดับ 1 (DFD Diagram 1)

จากกระบวนการที่ 1 การจัดการข้อมูลทรัพย์สิน ภัยคุกคาม และช่องโหว่ให้กับระบบ โดยทำการแตกกระบวนการที่ 1 เป็นกระบวนการย่อยๆ ได้ 3 กระบวนการย่อย ดังรูปที่ 4.3 และสามารถทำการอธิบายกระบวนการต่าง ๆ ได้ดังนี้

DFD Diagram 1 : การจัดการข้อมูลทรัพย์สิน ข้อมูลช่องโหว่ ข้อมูลภัยคุกคาม



รูปที่ 4.3 แสดงแผนภาพการไหลข้อมูล แผนภาพที่ 1 : การจัดการข้อมูลทรัพย์สิน ช่องโหว่ และภัยคุกคาม

<u>กระบวนที่ 1.1</u> การจัดการข้อมูลทรัพย์สิน

- ระบบดึงข้อมูลทรัพย์สิน จากตารางข้อมูลทรัพย์สิน
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการบันทึกข้อมูลทรัพย์สินของให้กับระบบ แล้ว ระบบจะทำการบันทึกข้อมูลทรัพย์สินลงในตารางข้อมูลทรัพย์สิน
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการแก้ไขข้อมูลของทรัพย์สิน แล้วระบบจะทำการบันทึกข้อมูลทรัพย์สินที่ทำการแก้ไขลงในตารางข้อมูลทรัพย์สิน
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการลบข้อมูลของทรัพย์สิน แล้วระบบจะทำการลบข้อมูลทรัพย์สินออกจากตารางข้อมูลทรัพย์สิน

<u>กระบวนที่ 1.2</u> การจัดการข้อมูลช่องโหว่

- ระบบเรียกดังข้อมูลช่องโหว่ จากตารางข้อมูลช่องโหว่
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการบันทึกข้อมูลช่องโหว่ของให้กับระบบ แล้ว ระบบจะทำการบันทึกข้อมูลช่องโหว่ลงในตารางข้อมูลช่องโหว่
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการแก้ไขข้อมูลของช่องโหว่ แล้วระบบจะทำการบันทึกข้อมูลช่องโหว่ที่ทำการแก้ไขลงในตารางข้อมูลช่องโหว่
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการลบข้อมูลของช่องโหว่ แล้วระบบจะทำการลบข้อมูลช่องโหว่ออกจากตารางข้อมูลช่องโหว่

<u>กระบวนที่ 1.3</u> การจัดการข้อมูลภัยคุกคาม

- ระบบเรียกดังข้อมูลภัยคุกคาม จากตารางข้อมูลภัยคุกคาม
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการบันทึกข้อมูลภัยคุกคามของให้กับระบบ แล้ว ระบบจะทำการบันทึกข้อมูลภัยคุกคามลงในตารางข้อมูลภัยคุกคาม
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการแก้ไขข้อมูลของภัยคุกคาม แล้ว ระบบจะทำการบันทึกข้อมูลภัยคุกคามที่ทำการแก้ไขลงในตารางข้อมูลภัยคุกคาม
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการลบข้อมูลของภัยคุกคาม แล้ว ระบบจะทำการลบข้อมูลภัยคุกคามออกจากตารางข้อมูลภัยคุกคาม

4.2.3 แผนภาพกระแสการไหลของข้อมูลระดับ 2 (DFD Diagram 2)

จากกระบวนการที่ 2 การจัดการการวิเคราะห์ความเสี่ยงและการควบคุม โดยจะทำการแตกกระบวนการที่ 2 เป็นกระบวนการย่อยๆ ได้ 3 กระบวนการย่อย ดังรูปที่ 4.4 และสามารถทำการอธิบายกระบวนการต่าง ๆ ได้ดังนี้

<u>กระบวนที่ 2.1</u> การจัดการการกำหนดช่องโหว่ให้กับทรัพย์สิน

- ระบบดึงข้อมูลทรัพย์สิน จากตารางข้อมูลทรัพย์สิน และข้อมูลช่องโหว่ จากตารางข้อมูลช่องโหว่
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการบันทึกข้อมูลช่องโหว่ให้กับทรัพย์สิน แล้ว ระบบจะทำการบันทึกข้อมูลช่องโหว่ที่กำหนดให้กับทรัพย์สินลงในตารางข้อมูลช่องโหว่ของแต่ละทรัพย์สิน
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการแก้ไขข้อมูลช่องโหว่ให้กับทรัพย์สิน แล้ว ระบบจะทำการบันทึกข้อมูลช่องทรัพย์สิน ข้อมูลช่องโหว่ที่ทำการแก้ไขลงในตารางข้อมูลช่องโหว่ของแต่ละทรัพย์สิน
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการลบข้อมูลช่องโหว่ให้กับทรัพย์สิน แล้ว ระบบจะทำการลบข้อมูลช่องโหว่ที่กำหนดให้กับทรัพย์สินออกจากตารางข้อมูลช่องโหว่ของแต่ละทรัพย์สิน

<u>กระบวนที่ 2.2</u> การจัดการการกำหนดภัยคุกคามให้กับช่องโหว่

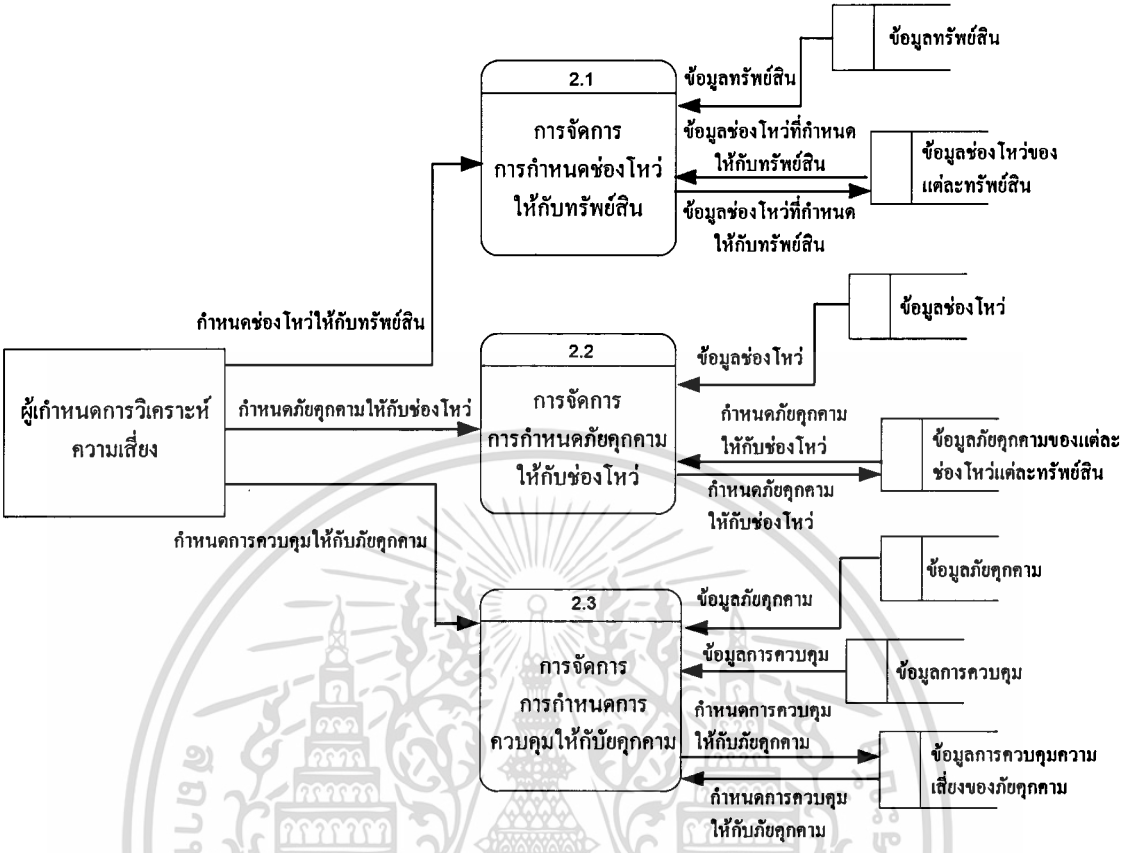
- ระบบดึงข้อมูลช่องโหว่ จากตารางข้อมูลช่องโหว่ และข้อมูลภัยคุกคาม จากตารางข้อมูลภัยคุกคาม

- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการบันทึกการกำหนดภัยคุกคามให้กับช่องโหว่ แล้ว ระบบจะทำการการบันทึกภัยคุกคามที่กำหนดให้กับช่องโหว่ลงในตารางข้อมูลภัยคุกคามของแต่ละช่องโหว่
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการแก้ไขการกำหนดภัยคุกคามให้กับช่องโหว่ แล้ว ระบบจะทำการการบันทึกภัยคุกคามที่กำหนดให้กับช่องโหว่ที่ได้ทำการแก้ไขลงในตารางข้อมูลภัยคุกคามของแต่ละช่องโหว่
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการลบการกำหนดภัยคุกคามให้กับช่องโหว่ แล้ว ระบบจะทำการการลบภัยคุกคามที่กำหนดให้กับช่องโหว่ออกจากตารางข้อมูลภัยคุกคามของแต่ละช่องโหว่

<u>กระบวนที่ 2.3</u> การจัดการการกำหนดการควบคุมให้กับภัยคุกคาม

- ระบบดึงข้อมูลภัยคุกคาม จากตารางข้อมูลภัยคุกคาม และดึงข้อมูลการควบคุมความเสี่ยง จากตารางข้อมูลการควบคุมความเสี่ยง
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการบันทึกการกำหนดการควบคุมความเสี่ยงให้กับภัยคุกคาม แล้ว ระบบจะทำการการบันทึกการกำหนดการควบคุมให้กับภัยคุกคามลงในตารางข้อมูลการควบคุมความเสี่ยงของภัยคุกคาม
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการแก้ไขการกำหนดการควบคุมความเสี่ยงให้กับภัยคุกคาม แล้ว ระบบจะทำการการบันทึกการกำหนดการควบคุมให้กับภัยคุกคามที่ได้ทำการแก้ไขลงในตารางข้อมูลการควบคุมความเสี่ยงของภัยคุกคาม
- ถ้า ผู้กำหนดการวิเคราะห์ความเสี่ยงทำการลบการกำหนดการควบคุมความเสี่ยงให้กับภัยคุกคาม แล้ว ระบบจะทำการการลบการกำหนดการควบคุมให้กับภัยคุกคามออกจากตารางข้อมูลการควบคุมความเสี่ยงของภัยคุกคาม

DFD Diagram 2 : การกำหนดการวิเคราะห์ความเสี่ยง



รูปที่ 4.4 แสดงแสดงแผนภาพการไหลข้อมูล แผนภาพที่ 2 : การจัดการการวิเคราะห์ความเสี่ยง

4.2.4 การจัดการทรัพย์สินเชิงธุรกิจ และคำนวณผลค่าความเสี่ยง

จากกระบวนการที่ 6 การจัดการทรัพย์สินเชิงธุรกิจและคำนวณค่าความเสี่ยง โดยสามารถทำการแตกกระบวนการที่ 6 เป็นกระบวนการย่อยๆ ได้ 3 กระบวนการย่อย ดังรูปที่ 4.5 และสามารถทำการอธิบายกระบวนการต่าง ๆ ได้ดังนี้

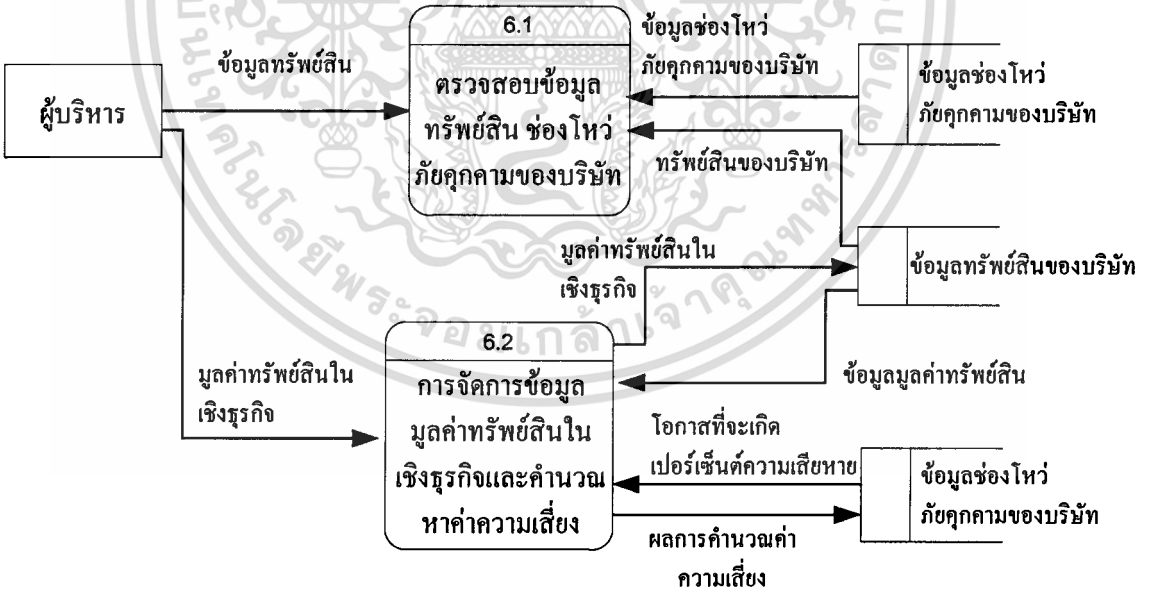
<u>กระบวนที่ 6.1</u> ตรวจสอบข้อมูลได้มีการระบุไว้

- ถ้า ผู้บริหารทำการตรวจสอบการข้อมูลทรัพย์สินของบริษัท แล้ว ระบบดึงข้อมูลทรัพย์สินของบริษัท จากตารางข้อมูลทรัพย์สินของบริษัทขึ้นมาแสดง
- ถ้า ผู้บริหารทำการตรวจสอบการข้อมูลช่องโหว่ ภัยคุกคามของบริษัท แล้ว ระบบดึงข้อมูลข้อมูลช่องโหว่ ภัยคุกคามของบริษัท จากตารางข้อมูลช่องโหว่ ภัยคุกคามของบริษัทขึ้นมาแสดง

<u>กระบวนที่ 6.2</u> **การจัดการมูลค่าของทรัพย์สินในเชิงธุรกิจ**

- ระบบดึงข้อมูลทรัพย์สินของบริษัท จากตารางข้อมูลทรัพย์สินของบริษัท
- ถ้า ผู้บริหารทำการบันทึกข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจ แล้ว ระบบทำการการบันทึกข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจลงในตารางข้อมูลทรัพย์สินของบริษัท
- ถ้า ผู้บริหารทำการแก้ไขข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจ แล้ว ระบบทำการการแก้ไขข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจลงในตารางข้อมูลทรัพย์สินของบริษัท
- ถ้า ผู้บริหารทำการลบข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจ แล้ว ระบบทำการการลบข้อมูลมูลค่าทรัพย์สินเชิงธุรกิจลงในตารางข้อมูลทรัพย์สินของบริษัท
- ถ้า ผู้บริหารยืนยันข้อมูลที่ได้มีการระบุไว้ แล้ว ระบบจะทำการดึงข้อมูลมูลค่าทรัพย์สินจากตารางข้อมูลทรัพย์สินของบริษัท แลดึงค่าข้อมูลโอกาสที่จะเกิด เปอร์เซ็นต์ความเสียหายที่จะเกิดช่องโหว่และภัยคุกคาม จากตารางข้อมูลช่องโหว่ ภัยคุกคามของบริษัท มาทำการคำนวณหาค่าความเสี่ยง แล้วทำการบันทึกค่าความเสี่ยงลงในตารางช่องโหว่ ภัยคุกคามของบริษัท

DFD Diagram 3 : การจัดการข้อมูลมูลค่าทรัพย์สินและคำนวณผลค่าความเสี่ยง



รูปที่ 4.5 แสดงแสดงแผนภาพการไหลข้อมูล แผนภาพที่ 3 : การจัดการข้อมูลมูลค่าทรัพย์สิน

4.3 ผังโครงสร้าง (Structure Chart)

จากแผนภาพการไหลของข้อมูลในหัวข้อที่ 4.2 สามารถนำมาออกแบบเป็นผังโครงสร้างเพื่อออกแบบถึงหน้าที่การทำงานของระบบ ซึ่งผังโครงสร้างจะนำข้อมูลในแต่ละกระบวนการทำงานของแผนภาพกระแสการไหลของข้อมูลมานำเสนอในรูปแบบเป็นโมดูลการทำงาน โดยจะเป็นการออก แบบในส่วนของการกำหนดรายละเอียดและการกำหนดการส่งผ่านข้อมูลในแต่ละโมดูล สามารถเขียนผังโครงสร้างได้ตามรูปที่ 4.6 ถึงรูปที่ 4.12

4.3.1 ผังโครงสร้างของระบบ

จากรูปที่ 4.6 แสดงโมดูลหลักของระบบทั้งหมด ซึ่งจากผังโครงสร้างจะประกอบ ด้วยโมดูลหลักดังนี้

- **โมดูลจัดการข้อมูลทรัพย์สิน ช่องโหว่ ภัยคุกคามและการกำหนดการวิเคราะห์ความเสี่ยง** เป็นโมดูลที่จัดการข้อมูลทรัพย์สิน ช่องโหว่ และภัยคุกคามที่จะนำมาใช้ในการกำหนดการวิเคราะห์ความเสี่ยง โดยข้อมูลที่ได้จากโมดูลนี้จะประกอบด้วย

  เอ้าท์พุทของโมดูล : ข้อมูลทรัพย์สิน ข้อมูลช่องโหว่ ข้อมูลภัยคุกคาม และ ข้อมูลการวิเคราะห์ความเสี่ยง

  ซึ่งจะประกอบด้วยโมดูลย่อยที่เป็นลักษณะเงื่อนไขดังนี้

  - โมดูลย่อยการจัดการข้อมูลทรัพย์สิน ช่องโหว่ ภัยคุกคาม
  - โมดูลการบันทึก แก้ไข ลบการกำหนดการวิเคราะห์ความเสี่ยง และการควบคุม

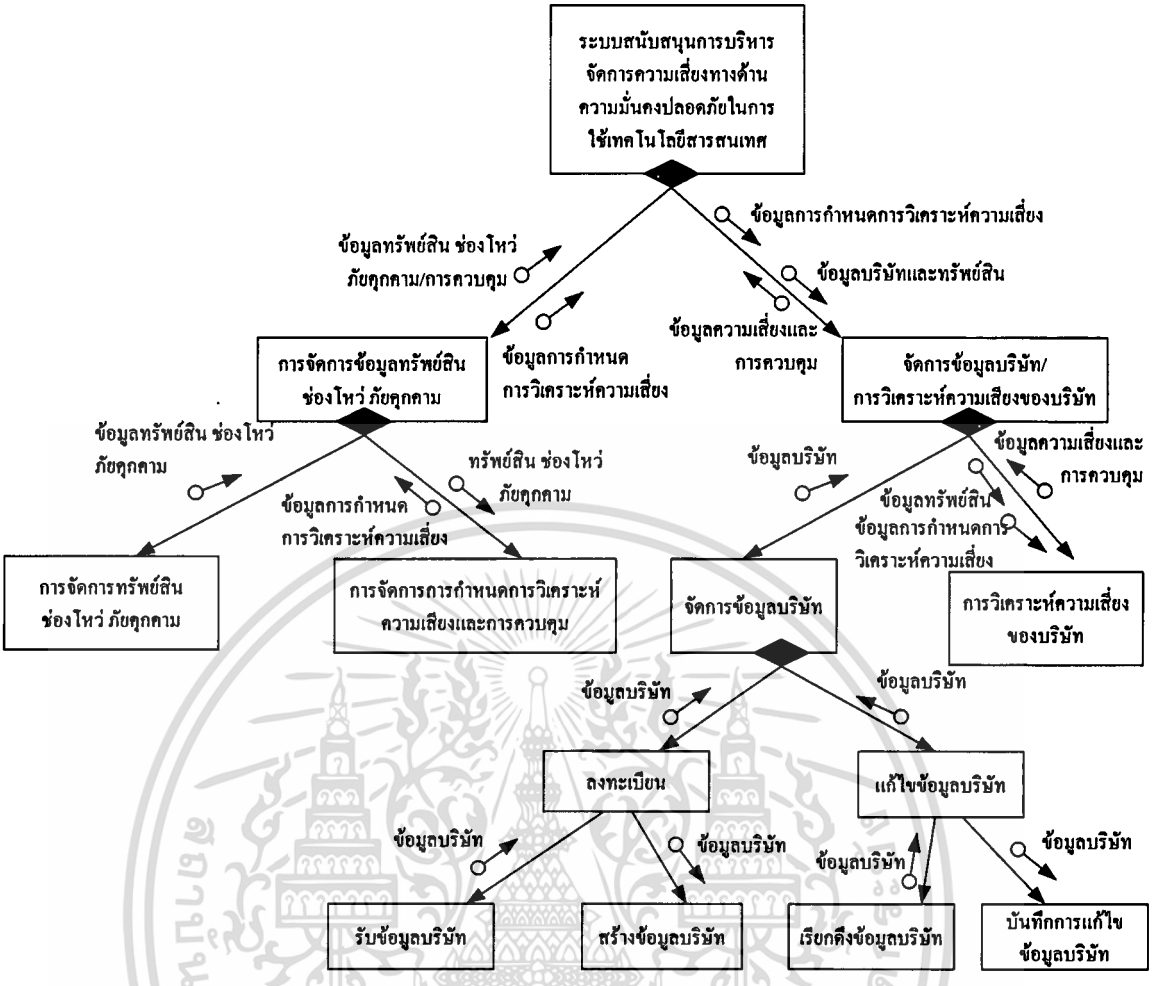
- **โมดูลจัดการข้อมูลบริษัทและการวิเคราะห์ความเสี่ยงของบริษัท**

  อินพุทของโมดูล : ข้อมูลการกำหนดการวิเคราะห์ความเสี่ยง ข้อมูลบริษัทและทรัพย์สินของบริษัท

  เอ้าท์พุทของโมดูล : ข้อมูลความเสี่ยงและการควบคุมของบริษัท

  ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

  - โมดูลการจัดการข้อมูลบริษัท จะประกอบด้วยโมดูลย่อย คือ โมดูลการลทะเบียน สำหรับบริษัทที่ยังไม่ได้ทำการลงทะเบียนเพื่อบันทึกข้อมูลของบริษัท โดยโมดูลจะทำการรับข้อมูลบริษัท แล้วมาทำการสร้างข้อมูลของบริษัทนั้น ซึ่งจะได้ข้อมูลของบริษัทที่ได้ทำการบันทึกเรียบร้อยแล้วเป็น เอาท์พุทของบริษัท

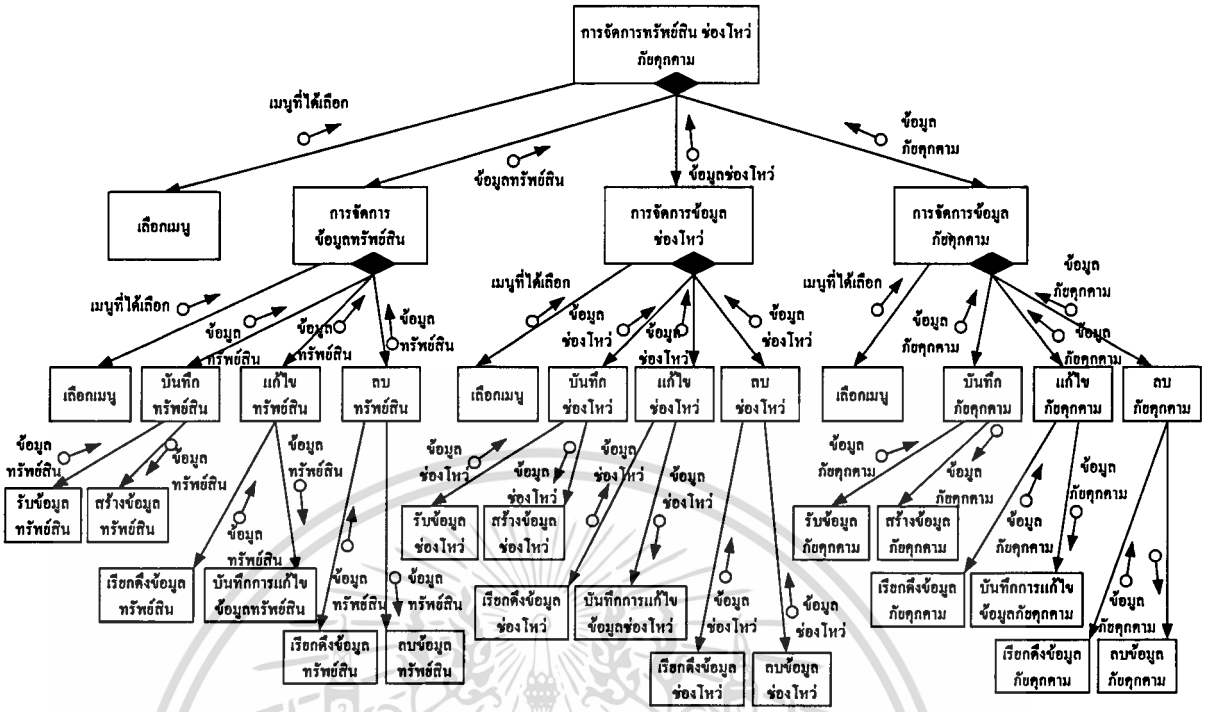


รูปที่ 4.6 แสดงผังโครงสร้างการจัดการข้อมูลบริษัทและการวิเคราะห์ความเสี่ยงของบริษท

- <u>โมดูลการวิเคราะห์ความเสี่ยงของบริษัท</u> จะรับข้อมูลทรัพย์สินของบริษัท และการกำหนดการวิเคราะห์ข้อมูลการกำหนดความเสี่ยงและเอาท์พุทที่ได้เป็นข้อมูลความเสี่ยงและการควบคุม

4.3.2 ผังโครงสร้างการจัดการข้อมูลทรัพย์สิน ช่องโหว่ ภัยคุกคาม

จากรูปที่ 4.7 จะแสดงผังโครงสร้างของโมดูลการจัดการข้อมูลทรัพย์สิน ช่องโหว่และภัยคุกคามซึ่งจากผังโครงสร้างจะประกอบด้วยโมดูลหลักดังนี้



รูปที่ 4.7 ผังโครงสร้างการจัดการข้อมูลทรัพย์สิน ช่องโหว่ ภัยคุกคาม

- **โมดูลเมนู** ในการเลือกการจัดการทรัพย์สิน การจัดการช่องโหว่ และการจัดการภัยคุกคาม
- **โมดูลการจัดการข้อมูลทรัพย์สิน**

<u>เอ้าท์พุทของโมดูล</u> : ข้อมูลทรัพย์สิน

ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

- <u>โมดูลเมนู</u> ในการเลือกการบันทึกข้อมูลทรัพย์สิน การแก้ไขข้อมูลทรัพย์สิน การลบข้อมูลทรัพย์สิน
- <u>โมดูลการจัดการการบันทึกข้อมูลทรัพย์สิน</u> ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลทรัพย์สิน จะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน โดยเอาท์พุทของโมดูลการรับข้อมูลทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลทรัพย์สิน ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว
- <u>โมดูลการจัดการการแก้ไขข้อมูลทรัพย์สิน</u> ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลทรัพย์สิน จะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน โดยเอาท์พุทของโมดูลการรับข้อมูลทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลทรัพย์สิน ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว

- โมดูลการจัดการการลบข้อมูลทรัพย์สิน ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลทรัพย์สิน จะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน โดยเอาท์พุทของโมดูลการเรียกดึงข้อมูลทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการลบข้อมูลทรัพย์สิน ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์สินที่ได้ทำการลบข้อมูลเรียบร้อยแล้ว

■ **โมดูลการจัดการข้อมูลช่องโหว่**

เอ้าท์พุทของโมดูล : ข้อมูลช่องโหว่

ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

- โมดูลเมนู ในการเลือกการบันทึกข้อมูลช่องโหว่ การแก้ไขข้อมูลช่องโหว่ การลบข้อมูลช่องโหว่

- โมดูลการจัดการการบันทึกข้อมูลช่องโหว่ ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลช่องโหว่ จะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่ โดยเอาท์พุทของโมดูลการรับข้อมูลช่องโหว่จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลช่องโหว่ที่ได้ทำการบันทึกเรียบร้อยแล้ว

- โมดูลการจัดการการแก้ไขข้อมูลช่องโหว่ ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลช่องโหว่จะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่ โดยเอาท์พุทของโมดูลการรับข้อมูลช่องโหว่ จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลช่องโหว่ที่ได้ทำการบันทึกเรียบร้อยแล้ว

- โมดูลการจัดการการลบข้อมูลช่องโหว่ ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลช่องโหว่ จะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่ โดยเอาท์พุทของโมดูลการเรียกดึงข้อมูลช่องโหว่ จะเป็นอินพุทของโมดูลย่อยการลบข้อมูลช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลช่องโหว่ที่ได้ทำการลบข้อมูลเรียบร้อยแล้ว

■ **โมดูลการจัดการข้อมูลภัยคุกคาม**

เอ้าท์พุทของโมดูล : ข้อมูลภัยคุกคาม

ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

- โมดูลเมนู ในการเลือกการบันทึกข้อมูลภัยคุกคาม การแก้ไขข้อมูลภัยคุกคาม การลบข้อมูลภัยคุกคาม

- โมดูลการจัดการการบันทึกข้อมูลภัยคุกคาม ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลช่องโหว่ จะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่ โดยเอาท์พุทของโมดูลการรับข้อมูลช่องโหว่จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลช่องโหว่ที่ได้ทำการบันทึกเรียบร้อยแล้ว

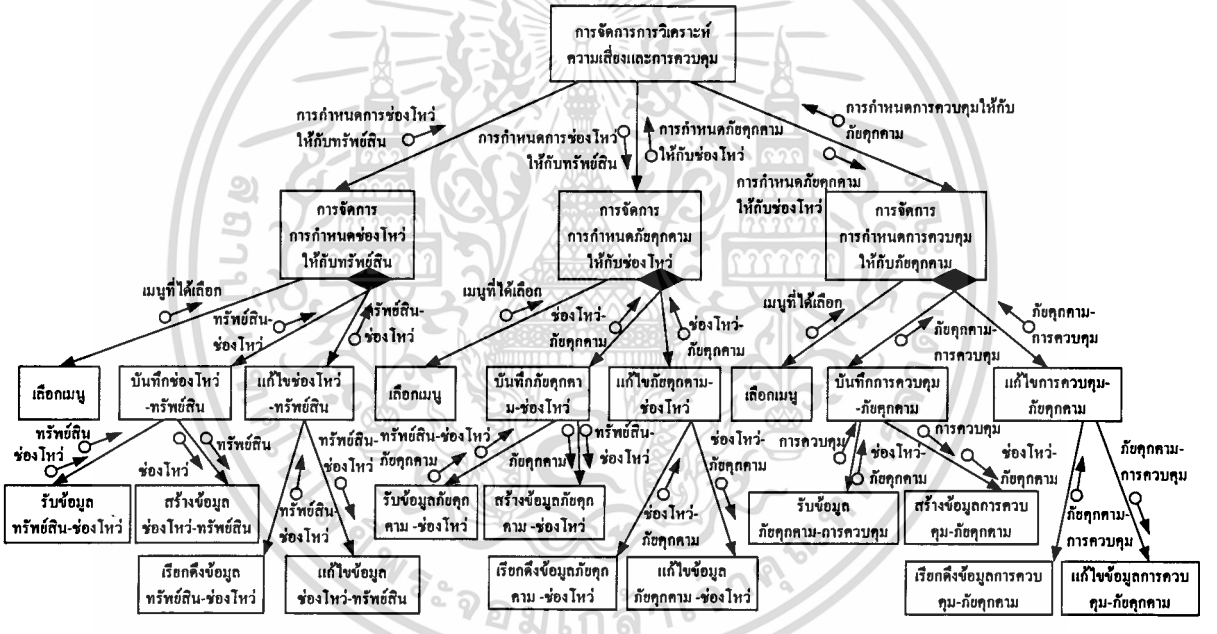
- โมดูลการจัดการการแก้ไขข้อมูลภัยคุกคาม ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลภัยคุกคามจะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่โดยเอาท์พุทของโมดูล

การรับข้อมูลภัยคุกคาม จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลภัยคุกคาม ซึ่งจะได้เอาท์พุทเป็นข้อมูลภัยคุกคามที่ได้ทำการบันทึกเรียบร้อยแล้ว

- <u>โมดูลการจัดการการลบข้อมูลภัยคุกคาม</u> ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลภัยคุกคามจะมีเอาท์พุทของโมดูลเป็นข้อมูลภัยคุกคาม โดยเอาท์ พุทของโมดูลการเรียกดึงข้อมูลภัยคุกคาม จะเป็นอินพุทของโมดูลย่อยการลบข้อมูลภัยคุกคาม ซึ่งจะได้เอาท์พุทเป็นข้อมูลภัยคุกคามที่ได้ทำการลบข้อมูลเรียบ ร้อยแล้ว

4.3.3 ผังโครงสร้างการจัดการการกำหนดการวิเคราะห์ความเสี่ยงและการควบคุม

จากรูปที่ 4.8 จะแสดงโมดูลการจัดการการกำหนดการวิเคราะห์ความเสี่ยงและการควบคุม ซึ่งจากผังโครงสร้างจะประกอบด้วยโมดูลหลักดังนี้



รูปที่ 4.8 ผังโครงสร้างการจัดการการกำหนดการวิเคราะห์ความเสี่ยงและการควบคุม

- **โมดูลจัดการการกำหนดช่องโหว่ให้กับทรัพย์สิน**

<u>เอ้าท์พุทของโมดูล</u> : การกำหนดช่องโหว่ให้กับทรัพย์สิน

ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

- <u>โมดูลเมนู</u> ในการเลือกการจัดการการบันทึกช่องโหว่ให้กับทรัพย์สิน การจัดการการแก้ไขภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน

- โมดูลการจัดการการบันทึกช่องโหว่ให้กับทรัพย์สิน ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลทรัพย์สิน ข้อมูลช่องโหว่ โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่ที่กำหนดให้กับทรัพย์สิน โดยเอาท์พุทของโมดูลการรับข้อมูลทรัพย์สิน-ช่องโหว่ จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลทรัพย์สิน-ช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลช่องโหว่ที่กำหนดให้กับทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว

- โมดูลการจัดการการแก้ไขการกำหนดช่องโหว่ให้กับทรัพย์สิน ประกอบด้วยโมดูลย่อยคือ โมดูลการเรียกดึงข้อมูลทรัพย์สิน ช่องโหว่ โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน-ช่องโหว่ โดยเอาท์พุทของโมดูลการรับข้อมูลทรัพย์สิน-ช่องโหว่ จะเป็นอินพุทของโมดูลย่อยการแก้ไขข้อมูลช่องโหว่-ทรัพย์สิน ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์สิน-ช่องโหว่ ที่ได้ทำการบันทึกเรียบร้อยแล้ว

■ **โมดูลจัดการการกำหนดภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน**

อินพุทของโมดูล : การกำหนดช่องโหว่ให้กับทรัพย์สิน

เอ้าท์พุทของโมดูล : การกำหนดภัยคุกคามให้กับช่องโหว่

ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

- โมดูลเมนู ในการเลือกการจัดการการบันทึกภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน การจัดการการแก้ไขภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน

- โมดูลการจัดการการบันทึกภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลภัยคุกคาม-ช่องโหว่ โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน-ช่องโหว่และภัยคุกคาม โดยเอาท์พุทของโมดูลการรับข้อมูลภัยคุกคาม-ช่องโหว่ จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลภัยคุกคาม-ช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลภัยคุกคามที่กำหนดให้กับช่องโหว่ของทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว

- โมดูลการจัดการการแก้ไขภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลภัยคุกคาม-ช่องโหว่ โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน-ช่องโหว่และภัยคุกคาม โดยเอาท์พุทของโมดูลการรับข้อมูลภัยคุกคาม-ช่องโหว่ จะเป็นอินพุทของโมดูลย่อยการแก้ไขข้อมูลภัยคุกคาม-ช่องโหว่ ซึ่งจะได้เอาท์พุทเป็นข้อมูลภัยคุกคามที่กำหนดให้กับช่องโหว่ของทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว

■ **โมดูลจัดการการกำหนดการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน**

อินพุทของโมดูล : การกำหนดภัยคุกคามให้กับช่องโหว่

เอ้าท์พุทของโมดูล : การกำหนดการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน

ซึ่งจะประกอบด้วยโมดูลย่อยดังนี้

- <u>โมดูลเมนู</u> ในการเลือกการจัดการการบันทึกการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน การจัดการการแก้ไขการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน

- <u>โมดูลการจัดการการบันทึกการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน</u> ประกอบด้วยโมดูลย่อยคือ โมดูลการรับข้อมูลการควบคุม-ภัยคุกคาม โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่-ภัยคุกคาม และการควบคุม โดยเอาท์พุทของโมดูลการรับข้อมูลการควบคุม-ภัยคุกคาม จะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลการควบคุม-ภัยคุกคาม ซึ่งจะได้เอาท์พุทเป็นข้อมูลการควบคุมที่กำหนดให้กับช่องโหว่และภัยคุกคามของทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว

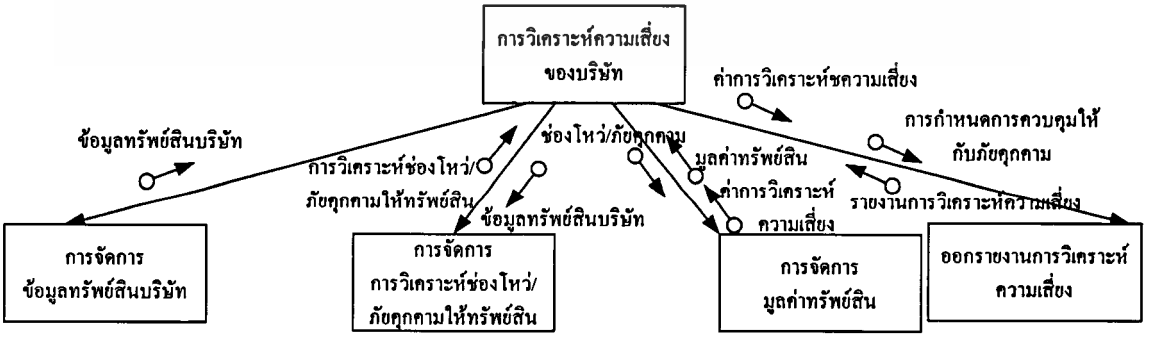
- <u>โมดูลการจัดการการแก้ไขการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน</u> ประกอบด้วยโมดูลย่อยคือโมดูลการรับข้อมูลการควบคุม-ภัยคุกคาม โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลช่องโหว่-ภัยคุกคาม และการควบคุม โดยเอาท์พุทของโมดูลการรับข้อมูลการควบคุม-ภัยคุกคาม จะเป็นอินพุทของโมดูลย่อยการแก้ไขข้อมูลการควบคุม-ภัยคุกคาม ซึ่งจะได้เอาท์พุทเป็นข้อมูลการควบคุมที่กำหนดให้กับช่องโหว่และภัยคุกคามของทรัพย์สินที่ได้ทำการบันทึกเรียบร้อยแล้ว

4.3.4 ผังโครงสร้างการวิเคราะห์ความเสี่ยงของบริษัท

จากรูปที่ 4.9 จะแสดงโมดูลของการจัดการการกำหนดการวิเคราะห์ความเสี่ยงของบรษัท ซึ่งจากผังโครงสร้างจะประกอบด้วยโมดูลหลักดังนี้

- **โมดูลจัดการข้อมูลทรัพย์สินบริษัท** เป็นโมดูลที่ทำหน้าที่ในการรับค่าข้อมูลทรัพย์สินของบริษัท แล้วนำทรัพย์สินของบริษัทมาทำการบันทึกลงฐานข้อมูลข้องระบบ และทำการเรียกดึงข้อมูลทรัพย์สินของบริษัทเพื่อมาทำการแก้ไข หรือลบทรัพย์สินนั้น

<u>เอ้าท์พุทของโมดูล</u> : ข้อมูลทรัพย์สินของบริษัท



รูปที่ 4.9 ผังโครงสร้างการวิเคราะห์ความเสี่ยงของบริษัท

- **โมดูลจัดการการวิเคราะห์ช่องโหว่และภัยคุกคามให้กับทรัพย์สินของบริษัท** เป็นโมดูลที่ทำหน้าที่ในการรับข้อมูลช่องโหว่และภัยคุกคามที่คาดว่าจะเกิดกับทรัพย์สิน แล้วทำการสร้างและบันทึกข้อมูลช่องโหว่และภัยคุกคามให้กับทรัพย์สิน รวมถึงการเรียกข้อมูลช่องโหว่และภัยคุกคามที่คาดว่าจะเกิดกับทรัพย์สินเพื่อมาทำการแก้ไขและลบข้อมูล

  อินพุทของโมดูล : ข้อมูลทรัพย์สินของบริษัท

  เอ้าท์พุทของโมดูล : ข้อมูลช่องโหว่และภัยคุกคามของทรัพย์สินบริษัท

- **โมดูลจัดการมูลค่าทรัพย์สินของบริษัท** เป็นโมดูลที่ทำหน้าที่ในการรับข้อมูลมูลค่าทรัพย์สินแล้วทำการสร้างและบันทึกข้อมูลมูลค่าทรัพย์สินของบริษัทให้กับระบบ พร้อมทั้งเรียกข้อมูลมูลค่าทรัพย์สินของบริษัทเพื่อมาทำการแก้ไข เมื่อทำการบันทึกหรือแก้ไขข้อมูลมูลค่าทรัพย์สินของบริษัทเรียบร้อยแล้ว โมดูลจะทำการเรียกดึงข้อมูลทรัพย์สินบริษัท และข้อมูลช่องโหว่และภัยคุกคามของทรัพย์สินบริษัทเพื่อมาใช้ในการคำนวณหาค่าความเสี่ยงของทรัพย์สิน

  อินพุทของโมดูล : ข้อมูลมูลค่าทรัพย์สินของบริษัท, ข้อมูลช่องโหว่และภัยคุกคามของทรัพย์สินบริษัท, ข้อมูลทรัพย์สินบริษัท

  เอ้าท์พุทของโมดูล : ค่าการวิเคราะห์ความเสี่ยง

- **โมดูลจัดการการออกรายงานการวิเคราะห์ความเสี่ยง** เป็นโมดูลที่ทำหน้าที่ในการเรียกดึงข้อมูลค่าการวิเคราะห์ความเสี่ยง และข้อมูลการกำหนดการควบคุมให้กับช่องโหว่และภัยคุกคามของทรัพย์สิน เพื่อมาทำการออกรายงานตามประเภททรัพย์สิน คลาสทรัพย์สิน และมูลค่าความเสียหายที่มากที่สุดจากภัยคุกคามใดบ้าง

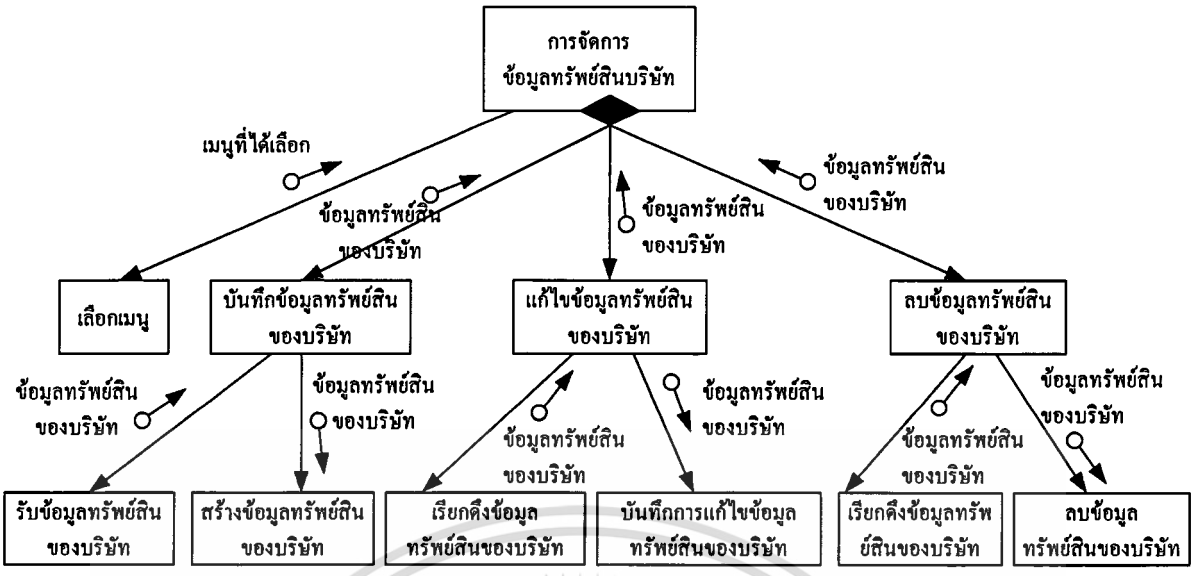
  อินพุทของโมดูล : ค่าการวิเคราะห์ความเสี่ยง

  เอ้าท์พุทของโมดูล : รายงานการวิเคราะห์ความเสี่ยงและการควบคุม

4.3.5 ผังโครงสร้างการจัดการข้อมูลทรัพย์สินของบริษัท

จากรูปที่ 4.10 จะแสดงโมดูลของการจัดการข้อมูลทรัพย์สินของบริษัท ซึ่งจากผังโครงสร้างจะประกอบด้วยโมดูลหลักดังนี้

- **โมดูลเมนู** ในการเลือกการบันทึกข้อมูลทรัพย์สินของบริษัท การแก้ไขข้อมูลทรัพย์สินของบริษัท การลบข้อมูลทรัพย์สินของบริษัท



รูปที่ 4.10 ผังโครงสร้างการจัดการทรัพย์สินของบริษัท

- **โมดูลการจัดการการบันทึกข้อมูลทรัพย์สินของบริษัท**

  เอ้าท์พุทของโมดูล : ข้อมูลทรัพย์สินของบริษัท

  ประกอบด้วยโมดูลย่อยคือ

  - โมดูลการรับข้อมูลทรัพย์สินของบริษัท โมดูลจะรับข้อมูลจากหน้าจอโดยมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สินของบริษัท และเอาท์พุทของโมดูลการรับข้อมูลทรัพย์ สินจะเป็นอินพุทของโมดูลย่อยการสร้างข้อมูลทรัพย์สินของบริษัท
  - โมดูลย่อยการสร้างข้อมูลทรัพย์สินของบริษัท ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์สินของบริษัทที่ได้ทำการบันทึกเรียบร้อยแล้ว

- **โมดูลการจัดการการแก้ไขข้อมูลทรัพย์สินของบริษัท**

  เอ้าท์พุทของโมดูล : ข้อมูลทรัพย์สินของบริษัท

  ประกอบด้วยโมดูลย่อยคือ

  - โมดูลการเรียกดึงข้อมูลทรัพย์สินของบริษัท โมดูลจะทำการเรียกดึงข้อมูลทรัพย์สินของบริษัทโดยมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สินของบริษัท และเอาท์พุทของโมดูลการเรียกดึงข้อมูลทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการแก้ไขข้อมูลทรัพย์สินของบริษัท
  - โมดูลย่อยการแก้ไขข้อมูลทรัพย์สินของบริษัท ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์ สินของบริษัทที่ได้ทำการแก้ไขและบันทึกเรียบร้อยแล้ว

- **โมดูลการจัดการการลบข้อมูลทรัพย์สินของบริษัท**

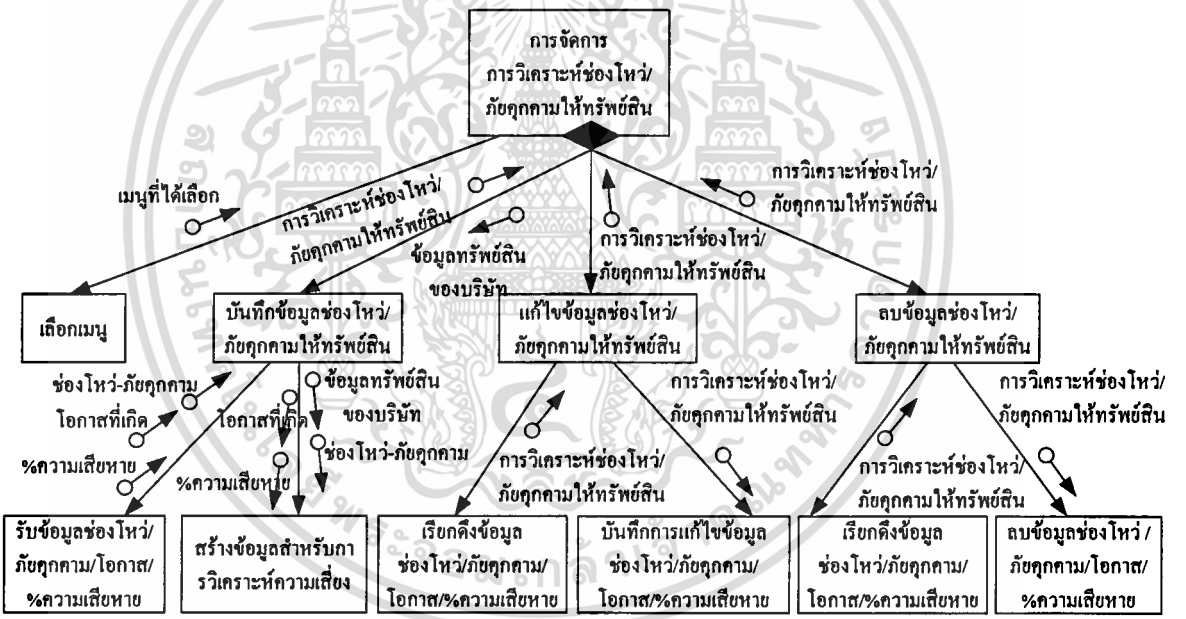
  เอ้าท์พุทของโมดูล : ข้อมูลทรัพย์สินของบริษัท

ประกอบด้วยโมดูลย่อยคือ

- <u>โมดูลการเรียกดึงข้อมูลทรัพย์สินของบริษัท</u> โมดูลจะทำการเรียกดึงข้อมูลทรัพย์สินของบริษัทโดยมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สินของบริษัท และเอาท์พุทของโมดูลการเรียกดึงข้อมูลทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการลบข้อมูลทรัพย์สินของบริษัท
- <u>โมดูลย่อยการลบข้อมูลทรัพย์สินของบริษัท</u> ซึ่งจะได้เอาท์พุทเป็นข้อมูลทรัพย์สินของบริษัทที่ได้ทำการลบเรียบร้อยแล้ว

4.3.6 ผังโครงสร้างการจัดการการวิเคราะห์ช่องโหว่ ภัยคุกคามให้กับทรัพย์สิน

จากรูปที่ 4.11 จะแสดงโมดูลของการจัดการการวิเคราะห์ช่องโหว่ ภัยคุกคามให้กับทรัพย์สินของบริษัท ซึ่งจากผังโครงสร้างจะประกอบด้วยโมดูลหลักดังนี้



รูปที่ 4.11 ผังโครงสร้างการจัดการการวิเคราะห์ช่องโหว่ ภัยคุกคามให้กับทรัพย์สิน

- **โมดูลเมนู** ในการเลือกการจัดการการบันทึกช่องโหว่ให้กับทรัพย์สินของบริษัท การจัดการการแก้ไขภัยคุกคามให้กับช่องโหว่ของทรัพย์สินของบริษัท และการจัดการการลบภัยคุกคามให้กับช่องโหว่ของทรัพย์สินของบริษัท
- **โมดูลการจัดการการบันทึกช่องโหว่-ภัยคุกคามให้กับทรัพย์สินของบริษัท**

  <u>อินพุทของโมดูล</u> : ข้อมูลทรัพย์สินของบริษัท

  <u>เอ้าท์พุทของโมดูล</u> : การวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน

  ประกอบด้วยโมดูลย่อยคือ

- โมดูลการรับข้อมูล โดยจะมีเอาท์พุทของโมดูลเป็นข้อมูลทรัพย์สิน, ข้อมูลช่องโหว่, ข้อมูลภัยคุกคาม, ข้อมูลโอกาสที่จะเกิดช่องโหว่และภัยคุกคาม และข้อมูลเปอร์เซ็นต์ความเสียหายที่เกิดจากช่องโหว่และภัยคุกคาม โดยเอาท์พุทของโมดูลการรับข้อมูลจะเป็นอินพุทของโมดูลย่อยการสร้างการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน
- โมดูลย่อยการสร้างการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน โมดูลจะทำการนำข้อมูลจากโมดูลการรับข้อมูลมาทำการสร้างข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินและทำการบันทึกข้อมูลลงฐานข้อมูล

- **โมดูลการจัดการการแก้ไขการกำหนดช่องโหว่ให้กับทรัพย์สินของบริษัท**

  เอ้าท์พุทของโมดูล : การวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน

  ประกอบด้วยโมดูลย่อยคือ

  - โมดูลการเรียกดึงข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน โดยจะมีเอาท์พุทของโมดูลข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินและเอาท์พุทของโมดูลการการเรียกดึงข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการแก้ไขการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน
  - โมดูลย่อยการแก้ไขการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน โมดูลจะทำการนำข้อมูลจากโมดูลการเรียกดึงข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์ สิน มาทำการแก้ไขข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินและทำการบันทึกข้อมูลลงฐานข้อมูล

- **โมดูลการจัดการการแก้ไขการกำหนดช่องโหว่ให้กับทรัพย์สินของบริษัท**

  เอ้าท์พุทของโมดูล : การวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน

  ประกอบด้วยโมดูลย่อยคือ

  - โมดูลการเรียกดึงข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน โดยจะมีเอาท์พุทของโมดูลข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินและเอาท์พุทของโมดูลการการเรียกดึงข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการลบการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน
  - โมดูลย่อยการลบการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สิน โมดูลจะทำการนำข้อมูลจากโมดูลการเรียกดึงข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์ สิน มาทำการลบข้อมูลการวิเคราะห์ช่องโหว่-ภัยคุกคามให้กับทรัพย์สินจากฐานข้อมูล

4.3.7 ผังโครงสร้างการการจัดการมูลค่าทรัพย์สินของบริษัท

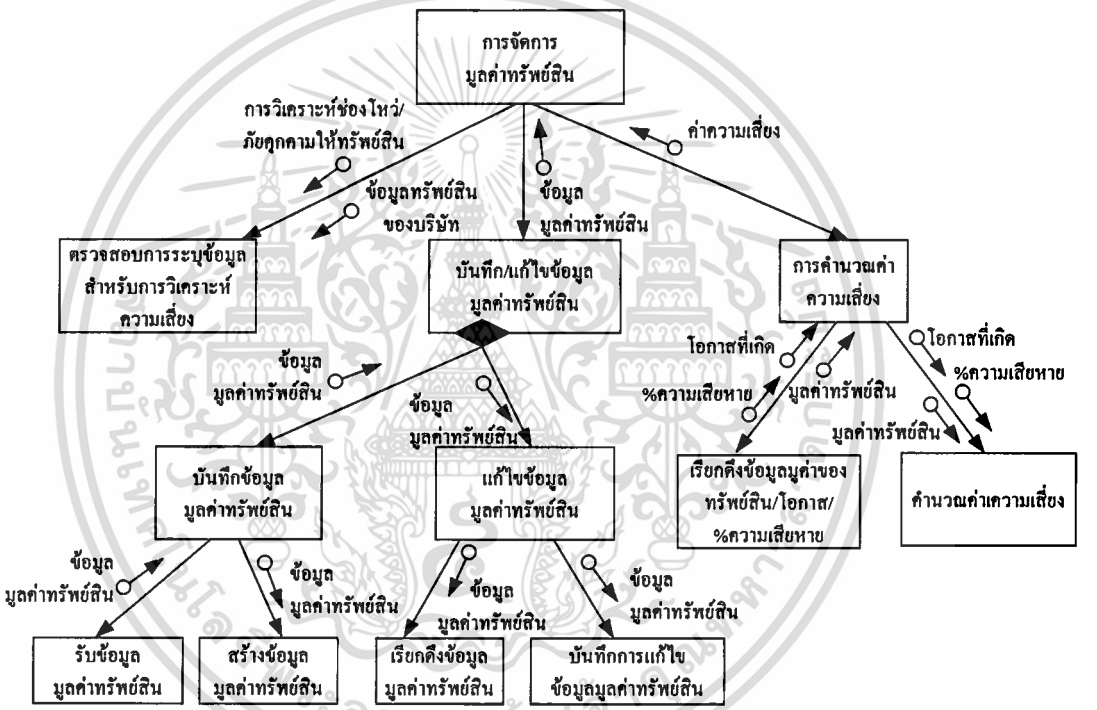
จากรูปที่ 4.12 แสดงโมดูลของการจัดการข้อมูลทรัพย์สินของบริษัทซึ่ง จากผังโครงสร้างจะประกอบด้วยโมดูลหลักดังนี้

- **โมดูลการจัดการข้อมูลทรัพย์สินของบริษัท**

  <u>เอ้าท์พุทของโมดูล</u> : ข้อมูลมูลค่าทรัพย์สินของบริษัท

  ประกอบด้วยโมดูลย่อยคือ

  - <u>โมดูลการบันทึกข้อมูลมูลค่าทรัพย์สินของบริษัท</u> จะประกอบด้วยโมดูลการรับข้อมูลมูลค่าทรัพย์สินซึ่งได้เอาท์พุทเป็นมูลค่าทรัพย์สินของบริษัท และโมดูลการสร้างข้อมูลมูลค่าทรัพย์สินของบริษัท โดยจะนำข้อมูลมูลค่าทรัพย์สินของบริษัทจากโมดูลการรับข้อมูลมูลค่าทรัพย์สินมาทำการสร้างข้อมูลมูลค่าทรัพย์สินและทำการบันทึกลงฐานข้อมูล



รูปที่ 4.12 ผังโครงสร้างการจัดการข้อมูลมูลค่าทรัพย์สิน

- <u>โมดูลการแก้ไขข้อมูลมูลค่าทรัพย์สินของบริษัท</u> จะประกอบด้วยโมดูลการเรียกดึงข้อมูลมูลค่าทรัพย์สิน โมดูลจะทำการเรียกดึงข้อมูลทรัพย์สินของบริษัทโดยมีเอาท์พุทของโมดูลเป็นข้อมูลมูลค่าทรัพย์สินของบริษัท และเอาท์พุทของโมดูลการเรียกดึงข้อมูลมูลค่าทรัพย์สินจะเป็นอินพุทของโมดูลย่อยการแก้ไขข้อมูลมูลค่าทรัพย์สินของบริษัท โมดูลย่อยการแก้ไขข้อมูลทรัพย์สินของบริษัทจะทำการนำเอาท์พุทเป็นข้อมูลมูลค่าทรัพย์สินของบริษัทที่จากการโมดูลการเรียกดึงข้อมูลมูลค่าทรัพย์สินมาทำการแก้ไขและบันทึกลงฐานข้อมูล

- **โมดูลการการคำนวณค่าความเสี่ยง**

  <u>เอ้าท์พุทของโมดูล</u> : ค่าความเสี่ยง

  ประกอบด้วยโมดูลย่อยคือ

  - <u>โมดูลการเรียกดึงข้อมูล</u> โมดูลจะทำการเรียกดึงข้อมูลมูลค่าของทรัพย์สิน โอกาสที่จะเกิดและเปอร์เซ็นต์ความเสียหาย โดยค่าที่ได้จากการเรียกดึงจะเป็นเอาท์พุทของโมดูลการเรียกดึงข้อมูล ซึ่งจะนำค่าไปเป็นอินพุทของโมดูลการคำนวณค่าความเสี่ยง

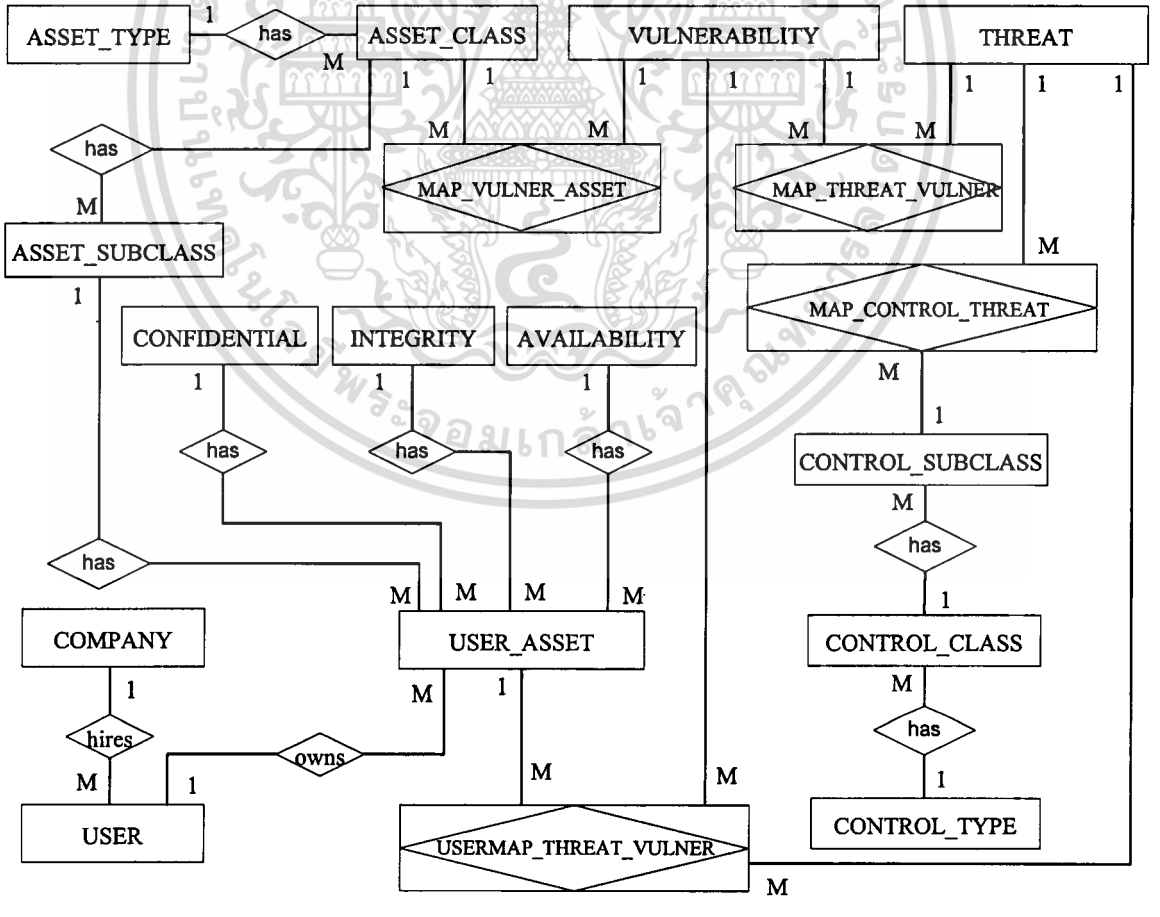
  - <u>โมดูลการคำนวณค่าความเสี่ยง</u> โมดูลจะทำการนำค่าที่ได้จากโมดูลการเรียกดึงข้อมูลมาทำการคำนวณหาค่าความเสี่ยงของทรัพย์สิน และได้เอาท์พุทของโมดูลเป็นค่าความเสี่ยงของทรัพย์สิน

บทที่ 5
การออกแบบฐานข้อมูล

การออกแบบจำลองข้อมูลเชิงตรรกะ โดยใช้โมเดลความสัมพันธ์ระหว่างเอนติทีสามารถแสดงความสัมพันธ์ของข้อมูลต่างๆ ที่มีต่อกันในระบบฐานข้อมูลเป็นการนำข้อมูลที่เกี่ยวข้องมากำหนดเป็นเอนทิตีและผ่านกระบวนการนอร์มอลไลเซชันแล้ว จึงนำมาเชื่อมความสัมพันธ์ตามกระบวนการของระบบงาน และกำหนดลักษณะของข้อมูลในพจนานุกรมข้อมูล

5.1 แผนภาพแสดงความสัมพันธ์ของเอนทิตี

ในหัวข้อนี้จะแสดงการออกแบบระบบงานเกี่ยวกับกลุ่มของข้อมูลที่สัมพันธ์กันด้วยแบบจำลองข้อมูล โดยเครื่องมือที่จะนำมาใช้ในการวิเคราะห์ คือ แผนภาพแสดงความสัมพันธ์ของเอนทิตี (Entity-Relationship Diagram) ดังรูปที่ 5.1



รูปที่ 5.1 แบบจำลองความสัมพันธ์ระหว่างเอนทิตี

รายละเอียดของแต่ละเอนทิตีแสดงพจนานุกรมข้อมูล ดังตารางที่ 5.1 ถึง ตารางที่ 5.18

ตารางที่ 5.1 รายละเอียดข้อมูลของตาราง ASSET_TYPE

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Asset_ID	int(11)	PK		รหัสประเภททรัพย์สิน
Asset_Name	varchar(100)			ชื่อประเภททรัพย์สิน
Asset_desc	text			คำอธิบายประเภททรัพย์สิน
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.2 รายละเอียดข้อมูลของตาราง ASSET_CLASS

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Class_ID	int(11)	PK		รหัสคลาสทรัพย์สิน
Class_Name	varchar(1000)			ชื่อคลาสทรัพย์
Class_Desc	varchar(2000)			คำอธิบายคลาสทรัพย์สิน
Class Intype	varchar(2000)	FK	ASSET_TYPE	รหัสผู้กำหนดการวิเคราะห์ฯ
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.3 รายละเอียดข้อมูลของตาราง ASSET_SUBCLASS

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Subclass_ID	int(11)	PK		รหัสคลาสย่อยทรัพย์สิน
Subclass_Name	varchar(100)			ชื่อคลาสย่อยทรัพย์สิน
Subclass_Desc	text			คำอธิบายคลาสย่อย
Subclass_Intype	int(11)	FK	ASSET_CLASS	คีย์อ้างอิง
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.4 รายละเอียดข้อมูลของตาราง COMPANY

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Company_ID	int(11)	PK		รหัสบริษัท
Company_Name	varchar(100)			ชื่อบริษัท
Company_Address	text			เลขที่อยู่
CompanyCity	varchar(50)			เมือง
Company_Province	varchar(50)			จังหวัด
Company_Zip	varchar(50)			รหัสไปรษณีย์
CompanyCountry	varchar(50)			ประเทศ
Company_Phone	varchar(50)			เบอร์โทรศัพท์
Company_Fax	varchar(50)			หมายเลขแฟ็ก
Company_Email	varchar(100)			E-mail
Company_Desc	text			รายละเอียดของบริษัท
Company_Suser	varchar(50)			Username ของบริษัท
Company_Spass	varchar(50)			Password ของบริษัท
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.5 รายละเอียดข้อมูลของตาราง USER

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
User_ID	int(11)	PK		รหัสผู้รับผิดชอบต่อทรัพย์สิน
User_Title	varchar(50)			คำนำหน้า
User_Fname	varchar(100)			ชื่อ
User_Lname	varchar(50)			นามสกุล
User_Nickname	varchar(50)			ชื่อเล่น
User_Position	varchar(100)			ตำแหน่ง

ตารางที่ 5.5 (ต่อ)

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
User_Phone	varchar(50)			เบอร์โทรศัพย์
User_Mobile	varchar(50)			เบอร์มือถือ
User_Email	varchar(50)			E-mail
User_Suser	varchar(50)			Username สำหรับล็อกอิน
User_Spass	varchar(50)			Password สำหรับล็อกอิน
Company_ID	int(11)	FK	COMPANY	รหัสบริษัท
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.6 รายละเอียดข้อมูลของตาราง VULNERABILITY

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Vul_ID	int(11)	PK		รหัสช่องโหว่
Vul_Name	varchar(1000)			ชื่อช่องโหว่
Vul_Desc	varchar(1500)			คำอธิบาย
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.7 รายละเอียดข้อมูลของตาราง THREAT

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Threat_ID	int(11)	PK		รหัสภัยคุกคาม
Threat_Name	varchar(1000)			ชื่อของภัยคุกคาม
Threat_desc	varchar(1500)			รายละเอียดภัยคุกคาม
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.8 รายละเอียดข้อมูลของตาราง CONTROL_TYPE

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Ctrltype_ID	int(11)	PK		รหัสประเภทการควบคุม
Ctrltype_Name	varchar(100)			ชื่อประเภทการควบคุม
Ctrltype_Desc	text			คำอธิบาย
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.9 รายละเอียดข้อมูลของตาราง CONTROL_CLASS

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Ctrlclass_ID	int(11)	PK		รหัสคลาสการควบคุม
Ctrlclass_Name	varchar(100)			ชื่อคลาสการควบคุม
Ctrlclass_Desc	text			คำอธิบาย
Ctrlclass_Intype	int(11)	FK	CONTROL_TYPE	รหัสประเภทการควบคุม

ตารางที่ 5.10 รายละเอียดข้อมูลของตาราง CONTROL_SUBCLASS

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Ctrlsubclass_ID	varchar(10)	PK		รหัสคลาสย่อยการควบคุม
Ctrlsubclass _Name	varchar(100)			ชื่อคลาสย่อยการควบคุม
Ctrlsubclass _Desc	text			คำอธิบาย
Ctrlsubclass _Inclass	int(11)	FK	CONTROL_CLASS	รหัสคลาสการควบคุม

ตารางที่ 5.11 รายละเอียดข้อมูลของตาราง MAP_VULNER_ASSET

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Class_ID	int(11)	PK,FK	ASSET_CLASS	รหัสคลาสทรัพย์สิน
Vul_ID	int(11)	PK,FK	VULNERABILITY	รหัสช่องโหว่
Mapav_Name	varchar(100)			ชื่อผูกทรัพย์สิน-ช่องโหว่
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.12 รายละเอียดข้อมูลของตาราง MAP_THREAT_VULNER

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Vul_ID	int(11)	PK,FK	VULNERABILITY	รหัสช่องโหว่
Threat_ID	int(11)	PK,FK	THREAT	รหัสภัยคุกคาม
Mapvt_Name	varchar(100)			ชื่อผูกช่องโหว่-ภัยคุกคาม
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.13 รายละเอียดข้อมูลของตาราง MAP_CONTROL_THREAT

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Threat_ID	varchar(100)	PK,FK	THREAT	รหัสภัยคุกคาม
Ctrlsubclass_ID	varchar(10)	PK,FK	CONTROL_SUBCLASS	รหัสคลาสย่อยการควบคุม
Maptc_Name	varchar(100)			วันที่มีการแก้ไขล่าสุด
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.14 รายละเอียดข้อมูลของตาราง USER_ASSET

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Userasset_ID	varchar(10)	PK		รหัสการะบุทรัพย์สิน
Userasset_Subclass	varchar(50)	FK	ASSET_SUBCLASS	รหัสคลาสย่อยการควบคุม
User_ID	int(11)	PK	USER	รหัสผู้รับผิดชอบต่อทรัพย์สิน
Userasset_ID	varchar(10)	PK		รหัสทรัพย์สินของบริษัท
Userasset_Company	varchar(10)	FK	COMPANY	รหัสบริษัท
Userasset_Subclass	varchar(50)	FK	ASSET_SUBCLASS	รหัสคลาสย่อยทรัพย์สิน
User_ID	int(11)	PK	USER	รหัสผู้รับผิดชอบต่อทรัพย์สิน
Userasset_Location	varchar(200)			สถานที่ตั้งทรัพย์สิน
Userasset_Owner	varchar(200)			ผู้เป็นเจ้าของทรัพย์สิน
Userasset_Quantity	int(11)			จำนวนทรัพย์สิน
Userasset_Department	varchar(10)			แผนก

ตารางที่ 5.14 (ต่อ)

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Userasset_Cost	float			ราคาที่ซื้อ
Userasset_Year	varchar(10)			จำนวนปีที่ใช้
Userasset_expire	varchar(500)			อายุการใช้งาน
Userasset_Profit_Value	float			มูลค่าเชิงธุรกิจ
Userasset_Other_Value	float			มูลค่าในด้านอื่นๆ
Userasset-Description	text			คำอธิบาย
Userasset_Recreate	float			มูลค่าการกู้คืน
Userasset_Rizvalue	float			มูลค่าเชิงธุรกิจ
Userasset_Othervalue	float			มูลค่าต่อส่วนอื่น
Userasset_Confidentiality	int(11)	FK	CONFIDENTIAL	รหัสค่า Confidential
Userasset_Integrity	int(11)	FK	INTEGRITY	รหัสค่า Integrity
Userasset_Availability	int(11)	FK	AVAILABILITY	รหัสค่า Availability
Lastedit	date			วันที่มีการแก้ไขล่าสุด

ตารางที่ 5.15 รายละเอียดข้อมูลของตาราง USERMAP_THREAT_VULNER

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Userasset_ID	varchar(10)	PK,FK	USER_ASSET	รหัสทรัพย์สินของบริษัท
Vul_ID	int(11)	PK,FK	VULNERABILITY	รหัสช่องโหว่
Threat_ID	int(11)	PK,FK	THREAT	รหัสภัยคุกคาม
Usermap-Freq	int(50)			โอกาสที่จะเกิด
Usermap_Per	double			เปอร์เซ็นต์ความเสียหาย
Risk_Impact	double			ผลการวิเคราะห์

ตารางที่ 5.16 รายละเอียดข้อมูลของตาราง INTEGRITY

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Integrity_ID	varchar(50)	PK		รหัสค่า Integrity
Integrity_Value	varchar(200)			ค่าของ Integrity

ตารางที่ 5.17 รายละเอียดข้อมูลของตาราง CONFIDENTIAL

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Confidential_ID	varchar(50)	PK		รหัสค่า Confidential
Confidential_ Value	varchar(200)			ค่าของ Confidential

ตารางที่ 5.18 รายละเอียดข้อมูลของตาราง AVAILABILIY

ชื่อแอททริบิวต์	ชนิดข้อมูล	คีย์	ตารางอ้างอิง	คำอธิบาย
Availability_ID	varchar(50)	PK		รหัสค่า Availability
Availability_ ID	varchar(200)			ค่าของ Availability

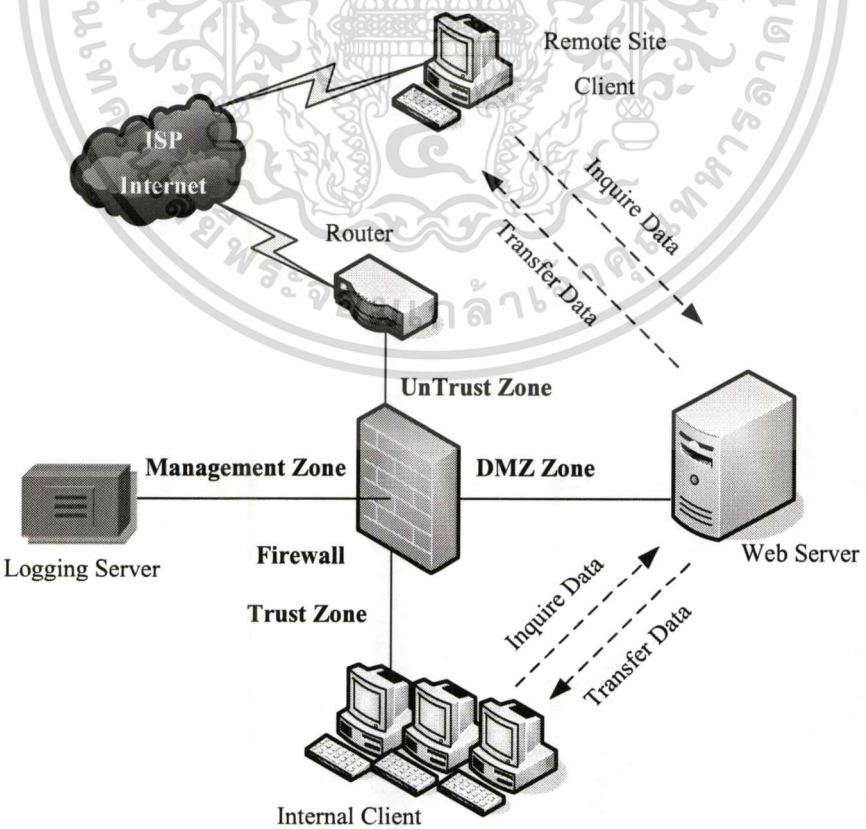
บทที่ 6
การออกแบบแอพพลิเคชัน

เมื่อทำการวิเคราะห์และออกแบบระบบเรียบร้อยแล้ว ขั้นตอนต่อไปจะเป็นการออกแบบส่วนติดต่อกับผู้ใช้ระบบ และการเขียนโปรแกรมพัฒนาระบบ ซึ่งแบ่งเป็นส่วนต่างๆ ได้ดังนี้

6.1 การออกแบบสถาปัตยกรรมของระบบ

สถาปัตยกรรมที่เลือกใช้ในการพัฒนาระบบเป็นแบบเว็บแอพพลิเคชัน เนื่องจากรูปแบบเว็บแอพพลิเคชันต้องอาศัยการเชื่อมต่อทีค่อนข้างมีความปลอดภัยเพราะต้องมีการเชื่อมต่อทั้งจากไคลเอนท์จากภายนอกและไคลเอนท์จากภายใน จึงต้องมีการกำหนดในการจัดตั้งเว็บเซิร์ฟเวอร์ให้มีความปลอดภัย โดยอาจจะต้องมีการนำไฟร์วอลล์มาทำการกั้นเพื่อป้องกันผู้ที่ไม่ประสงค์ดีที่จะทำการโจมตีเข้ามายังเซิร์ฟเวอร์

การทำงานของระบบเว็บแอพพลิเคชันมีฟังก์ชันการทำงานโดยมีการร้องของข้อมูล และการส่งผ่านข้อมูลต่างๆ ผ่านการเชื่อมโยงทางเครือข่ายคอมพิวเตอร์ ตามที่แสดงไว้ในรูปที่ 6.1



รูปที่ 6.1 แสดงกลไกการทำงานแบบเว็บแอพพลิเคชัน

ส่วนประกอบของสถาปัตยกรรมแบบไคลเอนท์-เซิรฟเวอร์ มีส่วนประกอบ 4 ส่วน คือ เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ไคล์เอนท์ เครือข่ายอินเตอร์เน็ต และอุปกรณ์เครือข่ายในการพัฒนาระบบช่วย ได้ใช้เครื่องมือและภาษาในการพัฒนาดังนี้

6.1.1 ฮาร์ดแวร์

เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาและทดสอบระบบงาน โดยมีคุณสมบัติดังนี้

- CPU : Pentium M 3.2 GHz
- RAM : 512 MB
- Hard Disk : 72 GB
- Network Interface : Fast Ethernet NIC

6.1.2 ซอฟต์แวร์

ซอฟต์แวร์ที่ใช้ในการพัฒนา และทดสอบระบบ มีดังนี้

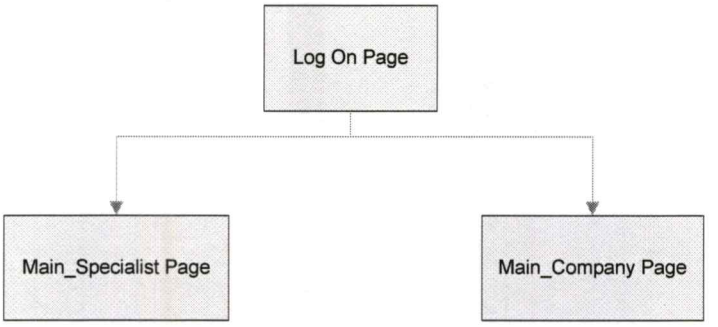
- Operation System : Microsoft Windows XP Professional
- Programming Language : PHP
- RDBMS : MySQL
- Web Browser : Internet Explorer 6.0

6.1.3 เครื่องมือ

- Web Development Tool : Dreamweaver CS 3
- UML Tool : Microsoft Visio 2003

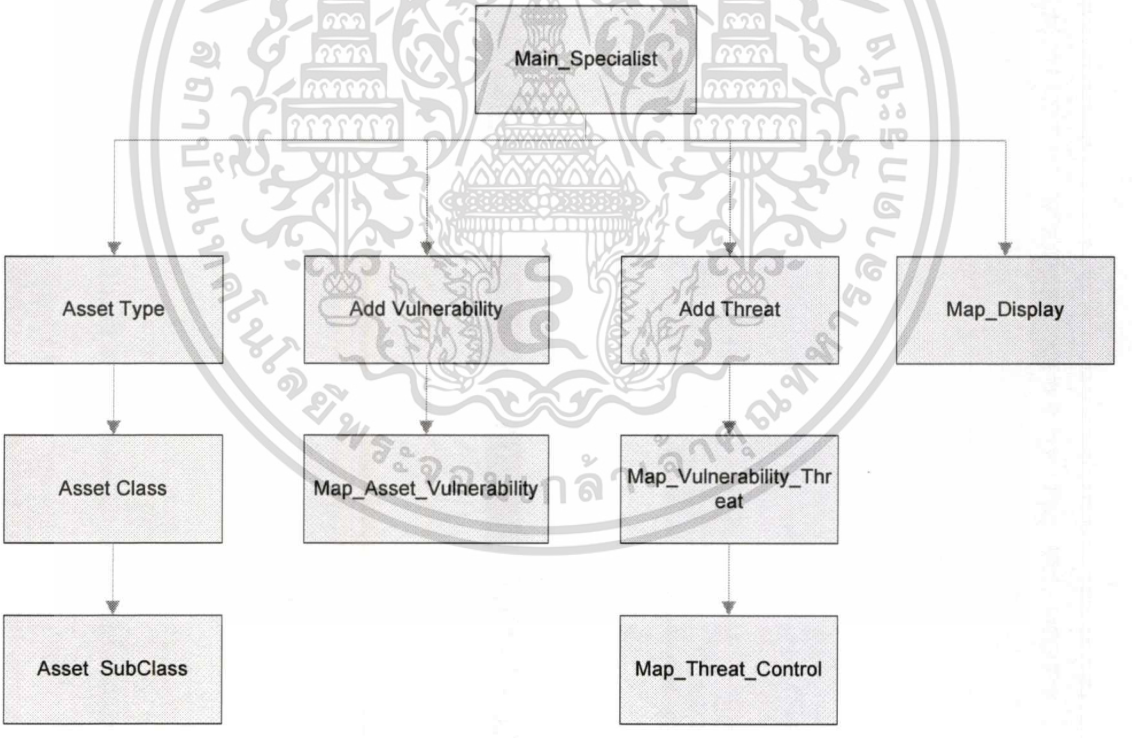
6.2 การออกแบบเว็บเพจ

สำหรับระบบที่ทำการพัฒนานั้น ได้ทำการออกแบบเว็บเพจซึ่งจะเป็นส่วนหน้าจอที่ใช้ติดต่อกับผู้ใช้งาน โดยจะเน้นการออกแบบให้แต่ละหน้าจอมีความสอดคล้องกัน และง่ายต่อการใช้งาน ดังนั้นจึงได้แบ่งโครงสร้างเว็บเพจออกเป็นส่วนๆ โดยมีโครงสร้างต่างๆ ภายในเว็บเพจดังรูปที่ 6.2 ซึ่งจะแสดงถึงเพจแรกที่ต้องทำการล็อกออนเข้าสู่ระบบ โดยชื่อ และรหัสผ่านที่กำหนด หลังจากทำการล็อกออนระบบจะทราบว่าผู้ที่ล็อกออนเป็นผู้กำหนดการวิเคราะห์ความเสี่ยงหรือไม่ ถ้าใช่ก็จะแสดงหน้าเพจ Main_Specialist เพื่อเข้าสู่การกำหนดการวิเคราะห์ความเสี่ยง แต่ถ้าเป็นผู้ใช้งานระบบก็จะเข้าสู่หน้าเพจ Main_Company เพื่อทำการลงทะเบียนและระบุข้อมูลทรัพย์สินของบริษัทต่อไป

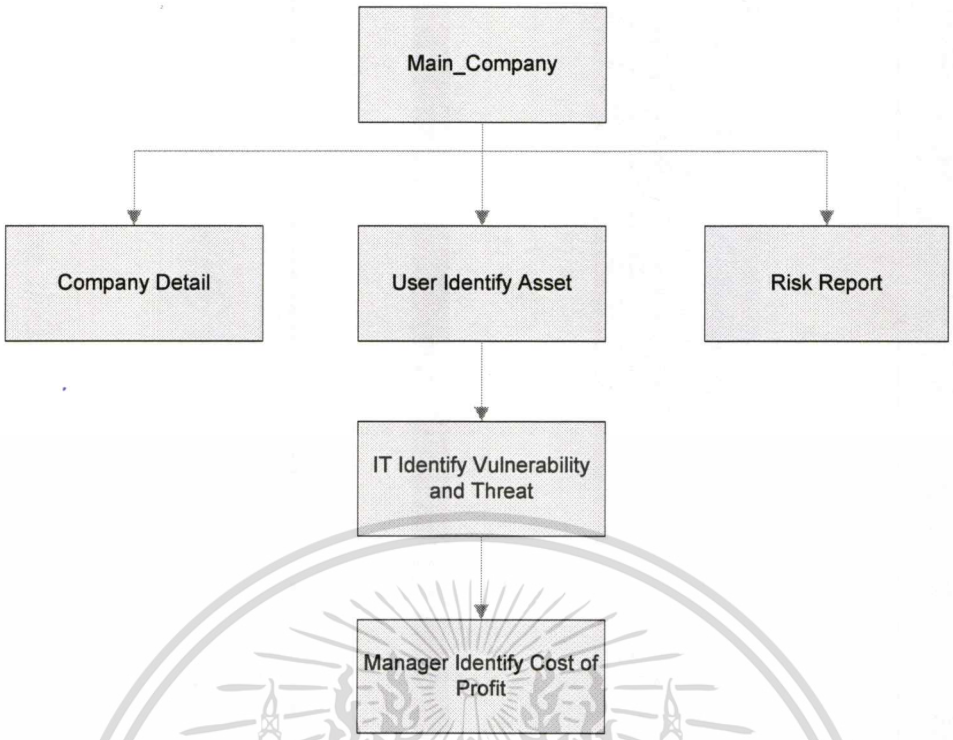


รูปที่ 6.2 แสดงออกแบบหน้าเว็บเพจ

จากรูปที่ 6.3 แสดงการลำดับการออกแบบหน้าเพจในส่วนของการกำหนดความเสี่ยง ซึ่งจะประกอบด้วยหน้าเพจสำหรับการกำหนดทรัพย์สิน (การกำหนดประเภทของทรัพย์สิน การกำหนดคลาสทรัพย์สิน การกำหนดคลาสย่อยทรัพย์สิน) หน้าเพจในการกำหนดช่องโหว่ หน้าเพจในการกำหนดภัยคุกคาม



รูปที่ 6.3 แสดงการลำดับการออกแบบหน้าเพจในส่วนของการกำหนดความเสี่ยง



รูปที่ 6.4 แสดงการลำดับการออกแบบหน้าเพจในส่วนของการวิเคราะห์ความเสี่ยงของบริษัท

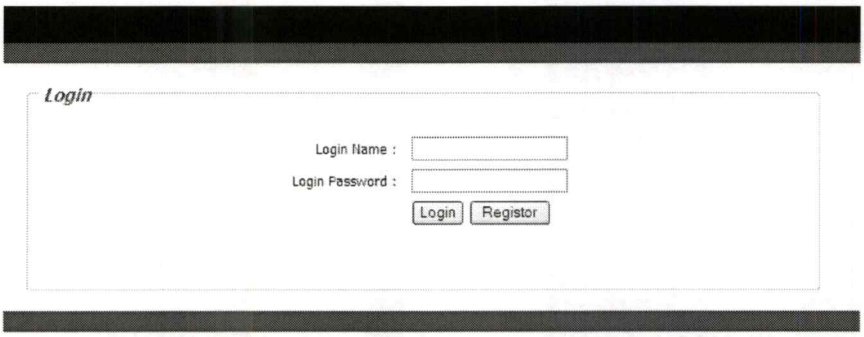
จากรูปที่ 6.4 จะได้ทำการออกแบบหน้าเพจของการวิเคราะห์ความเสี่ยงของบริษัท โดยแบ่งเป็นหน้าเพจการจัดการข้อมูลบริษัท การจัดการข้อมูลทรัพย์สินของบริษัท และการออกรายงานค่าความเสี่ยง

6.3 รายละเอียดการทำงานของระบบ

จากการออกแบบหน้าจอในข้อที่ 6.2 ถึง 6.4 ก็ได้ทำเขียนโปรแกรมตามการออกแบบที่ได้ทำการออกแบบไว้ซึ่งจะสามารถอธิบายการทำงานของระบบตามการออกแบบดังนี้

6.3.1 การตรวจสอบผู้ใช้งานและรหัสผ่านในการเข้าสู่ระบบ

ก่อนผู้ใช้งานจะเข้าใช้งานระบบ ผู้ใช้งานจะต้องกรอกชื่อผู้ใช้งาน และรหัสผ่านก่อนเสมอ เพื่อทำการล็อกอินเข้าสู่ระบบ ดังรูปที่ 6.5 ในกรณีที่ผู้ใช้งานกรอกรหัสผู้ใช้งานหรือรหัสผ่านไม่ถูกต้อง ระบบจะแสดงข้อความเตือนจนกว่าผู้ใช้จะกรอกรหัสผู้ใช้งานและรหัสผ่านถูกต้อง ผู้ใช้งานจึงจะสามารถเข้าใช้งานในระบบ

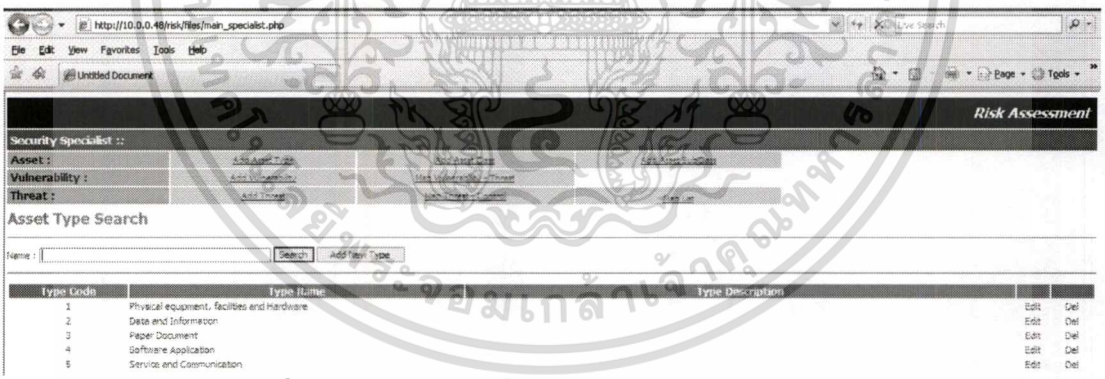


รูปที่ 6.5 หน้าเพจการล็อกอินเข้าสู่ระบบ

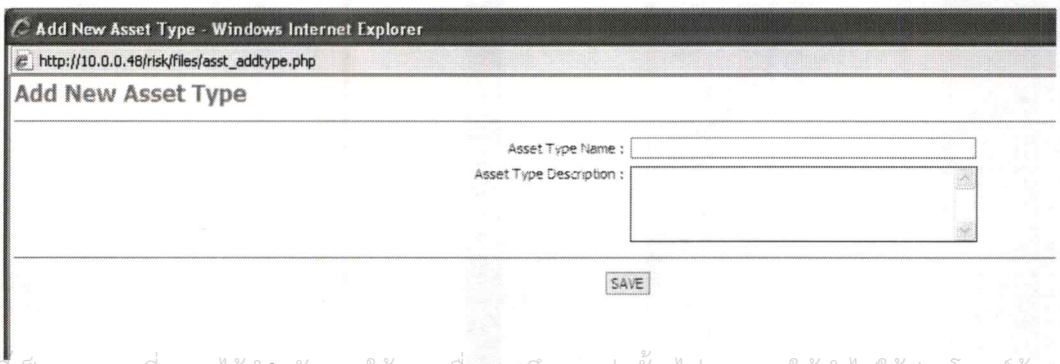
6.3.2 การจัดการข้อมูลทรัพย์สิน

หลังจากที่ได้มีการล็อกลินโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้กำหนดการวิเคราะห์ความเสี่ยงเสร็จสมบูรณ์แล้วระบบจะทำการแสดงหน้าเพจแสดงประเภทของทรัพย์สิน ดังรูปที่ 6.6 โดยประกอบด้วยหน้าเพจสำหรับการจัดการข้อมูลทรัพย์สินดังนี้

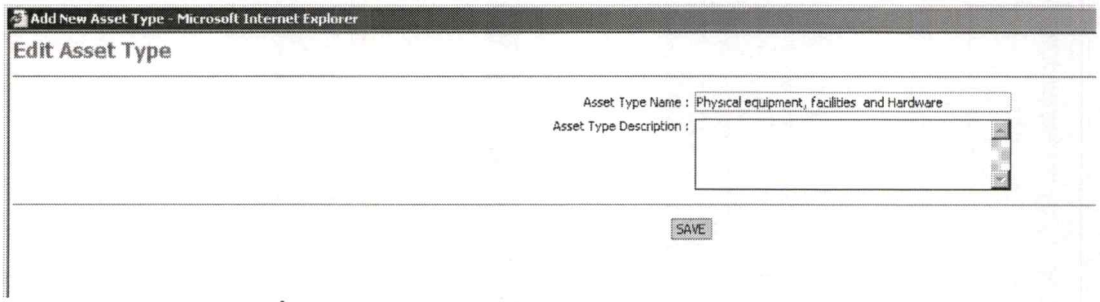
- **เมนู Add Asset Type** ทำหน้าที่เพิ่มข้อมูลของประเภทคลาสของทรัพย์สิน และรายละเอียด ดังรูปที่ 6.7 และถ้าคลิกในส่วนของ Edit จะแสดงหน้าเพจการแก้ไขข้อมูลประเภทของทรัพย์สินดังรูปที่ 6.8 และเมื่อคลิก Del จะแสดงหน้าเตือนก่อนการลบดังรูปที่ 6.9



รูปที่ 6.6 หน้าเพจการแสดงข้อมูลประเภทของทรัพย์สิน



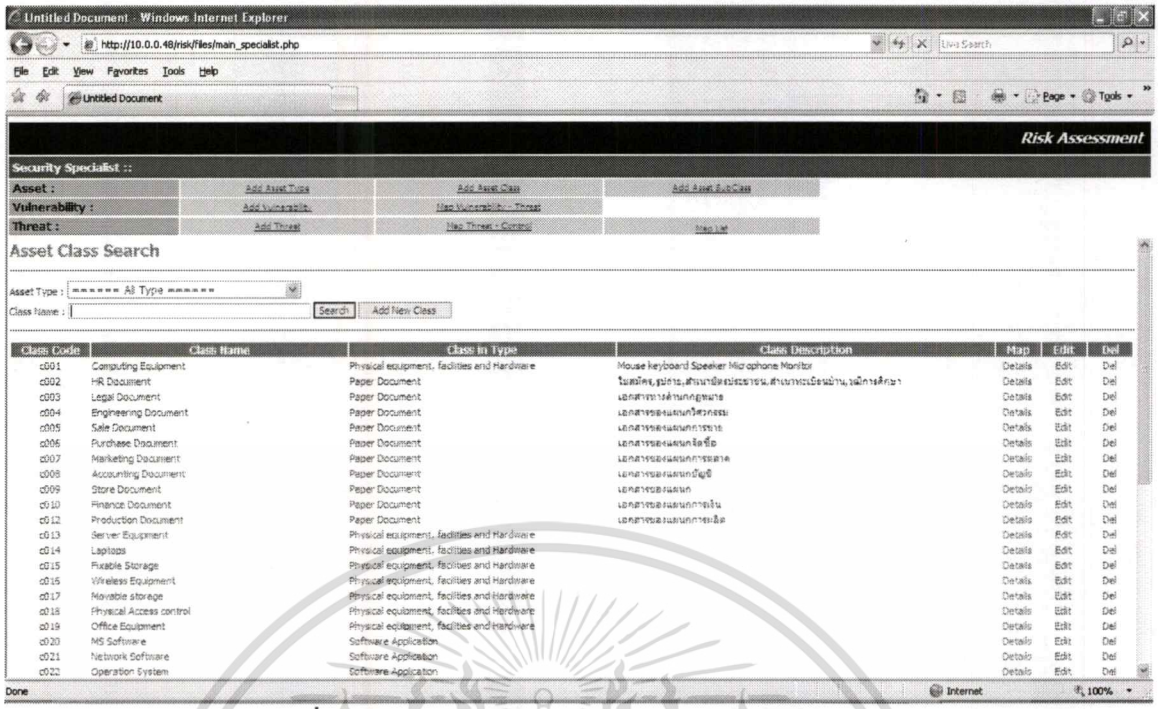
รูปที่ 6.7 หน้าเพจการเพิ่มข้อมูลประเภทของทรัพย์สิน



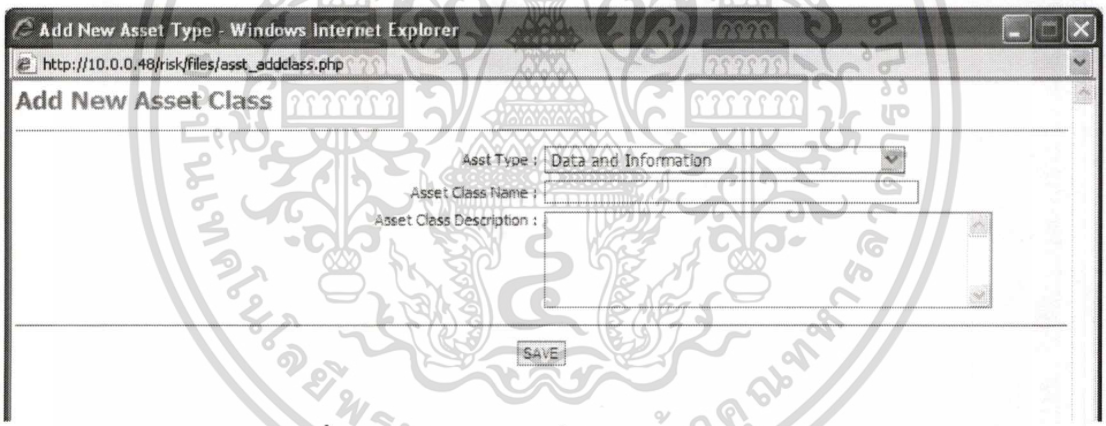
รูปที่ 6.8 หน้าเพจการแก้ไขข้อมูลประเภทของทรัพย์สิน

รูปที่ 6.9 หน้าเตือนก่อนการลบข้อมูลประเภทของทรัพย์สิน

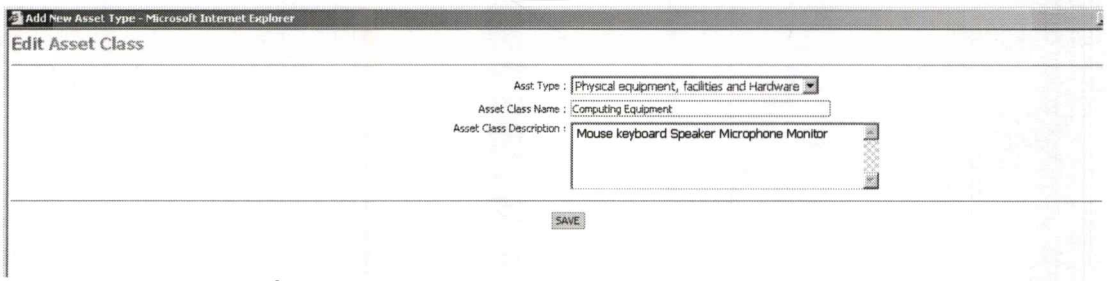
- **<u>เมนูย่อย Add Asset Class</u>** ทำหน้าที่ในการแสดงรายการคลาสทรัพย์สินที่มีอยู่ในระบบดังรูปที่ 6.10 ซึ่งจะสามารถทำการค้นหาคลาสของทรัพย์สินได้จากช่องการค้นหา และสามารถทำการเพิ่มคลาสทรัพย์สินโดยการคลิกที่ Add New Class ซึ่งจะแสดงหน้าเพจสำหรับการเพิ่มข้อมูลคลาสทรัพย์สินดังรูปที่ 6.11 ถ้า คลิกที่ Edit จะแสดงหน้าเพจสำหรับการแก้ไขข้อมูลคลาสทรัพย์สินดังรูปที่ 6.12 และถ้าคลิก Del จะแสดงดังรูปที่ 6.9



รูปที่ 6.10 หน้าเพจการแสดงข้อมูลคลาสทรัพย์สิน



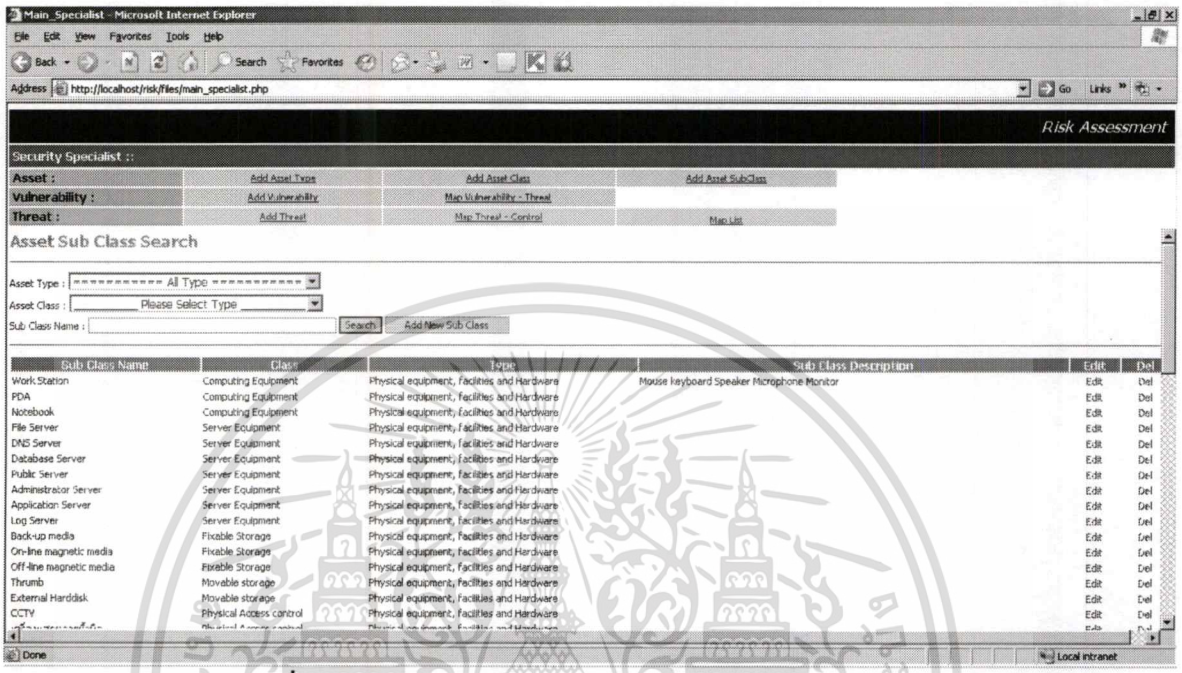
รูปที่ 6.11 หน้าเพจการเพิ่มข้อมูลคลาสทรัพย์สิน



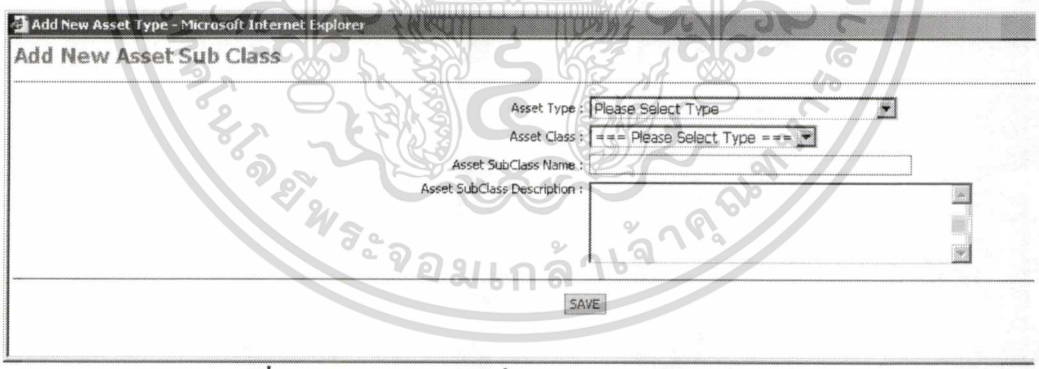
รูปที่ 6.12 หน้าเพจการแก้ไขข้อมูลประเภทของทรัพย์สิน

- **<u>เมนูย่อย Add Asset SubClass</u>** ทำหน้าที่ในการแสดงรายการคลาสย่อยทรัพย์สินที่มีอยู่ในระบบดังรูปที่ 6.13 ซึ่งจะสามารถทำการค้นหาคลาสย่อยทรัพย์สินได้จากช่องการค้นหา และสามารถทำการเพิ่มคลาสย่อยของทรัพย์สินโดยการคลิกที่ Add New SubClass ซึ่งจะแสดง

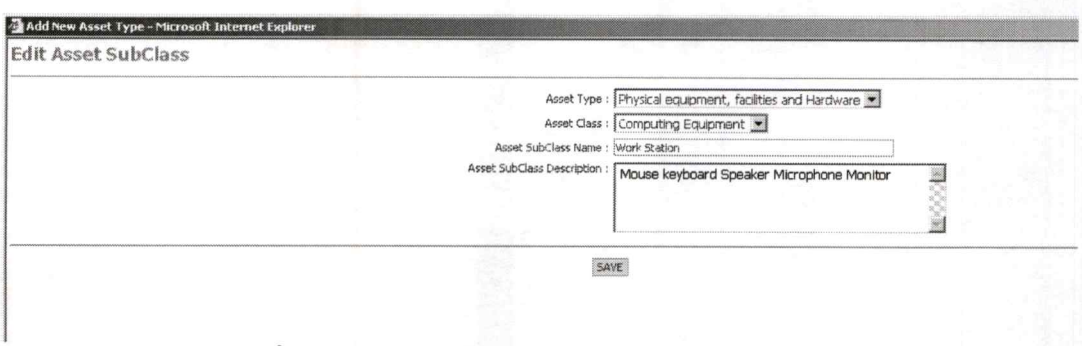
หน้าเพจสำหรับการเพิ่มข้อมูลคลาสย่อยทรัพย์สิน ดังรูปที่ 6.14 และคลิก Edit ในการแก้ไขข้อมูลคลาสย่อยทรัพย์สิน ดังรูปที่ 6.15 และถ้าคลิก Del จะแสดงดังรูปที่ 6.9



รูปที่ 6.13 หน้าเพจการแสดงข้อมูลคลาสย่อยทรัพย์สิน



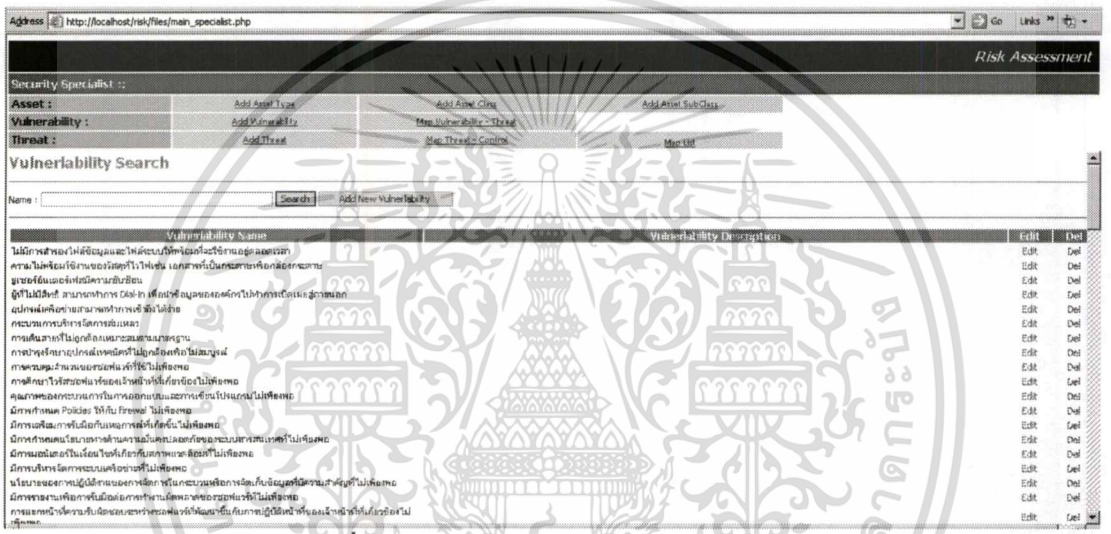
รูปที่ 6.14 หน้าเพจการเพิ่มข้อมูลคลาสย่อยทรัพย์สิน



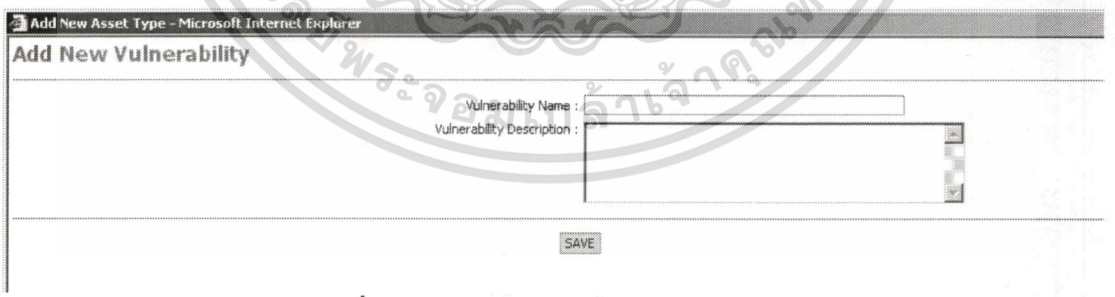
รูปที่ 6.15 หน้าเพจการแก้ไขข้อมูลคลาสย่อยทรัพย์สิน

6.3.3 การจัดการข้อมูลช่องโหว่

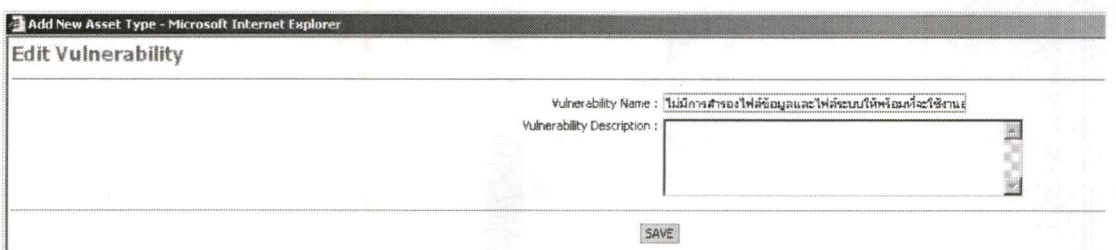
หลังจากที่ได้มีการล็อกลินโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้กำหนดการวิเคราะห์ความเสี่ยงเสร็จสมบูรณ์แล้วระบบจะทำการแสดงหน้าเพจแสดงประเภทของทรัพย์สิน คลิกที่ Add Vulnerability จะแสดงหน้าเพจการจัดการข้อมูลช่องโหว่ ดังรูปที่ 6.16 ซึ่งจะสามารถทำการค้นหาช่องโหว่จากส่วนของการค้นหา และทำการเพิ่มข้อมูลช่องโหว่โดยการคลิก Add New Vulnerability ซึ่งจะแสดงหน้าเพจในการเพิ่มข้อมูลช่องโหว่ ดังรูปที่ 6.17 และการแก้ไขข้อมูลช่องโหว่สามารถทำได้โดยคลิกที่ Edit จะแสดงหน้าจอการแก้ไขข้อมูลช่องโหว่ได้ดังรูปที่ 6.18 และถ้าคลิก Del จะแสดงดังรูปที่ 6.9



รูปที่ 6.16 หน้าเพจการแสดงข้อมูลช่องโหว่



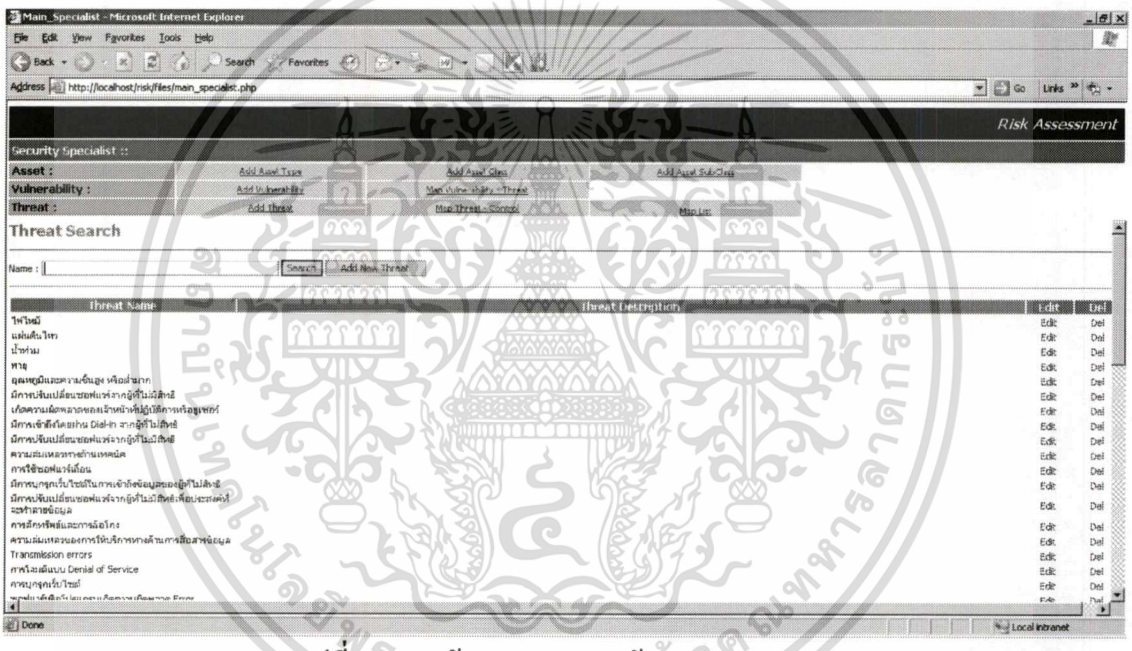
รูปที่ 6.17 หน้าเพจการเพิ่มข้อมูลช่องโหว่



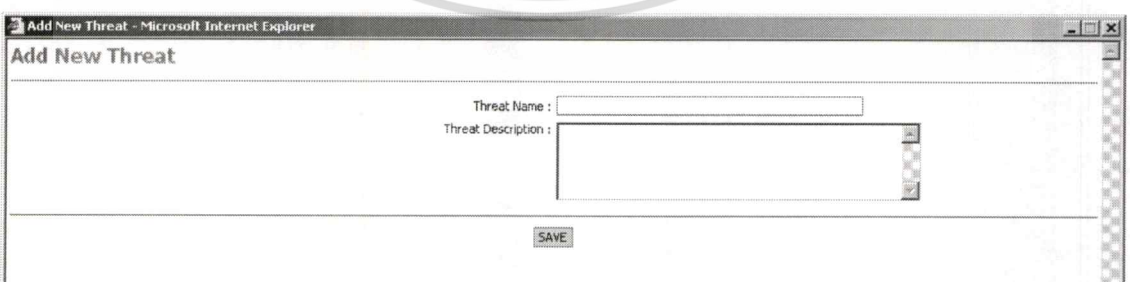
รูปที่ 6.18 หน้าเพจการแก้ไขข้อมูลช่องโหว่

6.3.4 การจัดการข้อมูลภัยคุกคาม

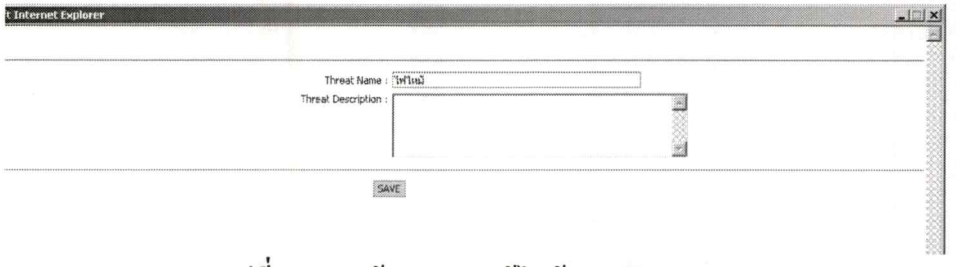
หลังจากที่ได้มีการล็อกลินโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้กำหนดการวิเคราะห์ความเสี่ยงเสร็จสมบูรณ์แล้วระบบจะทำการแสดงหน้าเพจแสดงประเภทของทรัพย์สิน คลิกที่ Add Threat จะแสดงหน้าเพจการจัดการข้อมูลภัยคุกคาม ดังรูปที่ 6.19 ซึ่งจะสามารถทำการค้นหาภัยคุกคามจากส่วนของการค้นหา และทำการเพิ่มข้อมูลภัยคุกคามโดยการคลิก Add New Vulnerability ซึ่งจะแสดงหน้าเพจในการเพิ่มข้อมูลภัยคุกคาม ดังรูปที่ 6.20 และการแก้ไขข้อมูลภัยคุกคามสามารถทำได้โดยคลิกที่ Edit จะแสดงหน้าจอการแก้ไขข้อมูลภัยคุกคามได้ ดังรูปที่ 6.21 และถ้าคลิก Del จะแสดงดังรูปที่ 6.9



รูปที่ 6.19 หน้าเพจการแสดงข้อมูลภัยคุกคาม



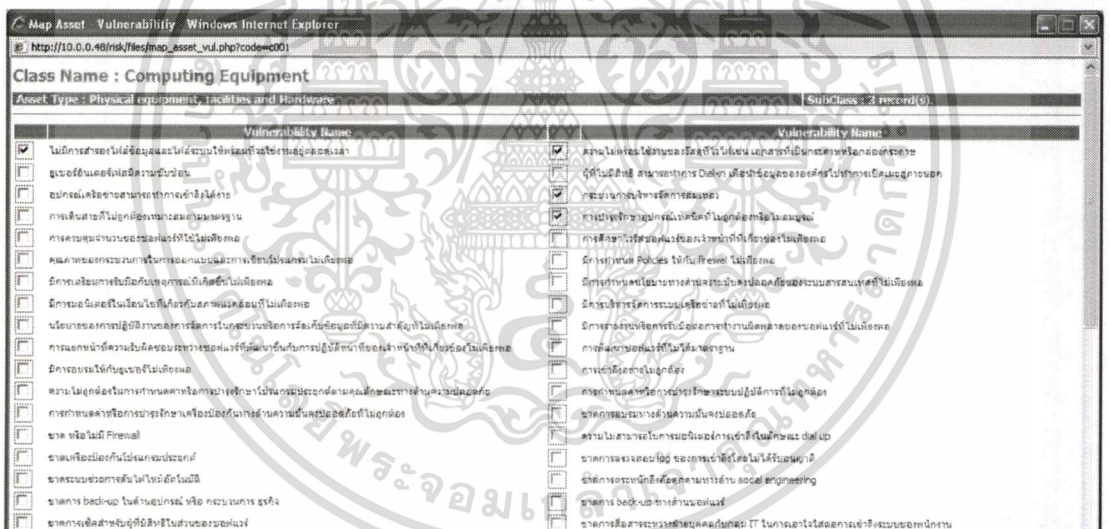
รูปที่ 6.20 หน้าเพจการเพิ่มข้อมูลภัยคุกคาม



รูปที่ 6.21 หน้าเพจการแก้ไขข้อมูลภัยคุกคาม

6.3.5 การจัดการการกำหนดช่องโหว่ให้กับทรัพย์สิน

หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้กำหนดการวิเคราะห์ความเสี่ยงเสร็จสมบูรณ์แล้วระบบจะทำการแสดงหน้าเพจแสดงประเภทของทรัพย์สิน ดังรูปที่ 6.10 คลิกที่ Add Asset Class ให้ทำการเลือกคลาสทรัพย์สินที่ต้องการจะกำหนดช่องโหว่ให้กับคลาสทรัพย์สินนั้น แล้วคลิกที่ Detail จากคอลัมน์ Map ซึ่งจะแสดงรายการของช่องโหว่ที่ได้ทำการเพิ่ม ดังรูปที่ 6.22 คลิก Save เพื่อทำการบันทึกข้อมูลและคลิก Close เพื่อปิดหน้าเพจ

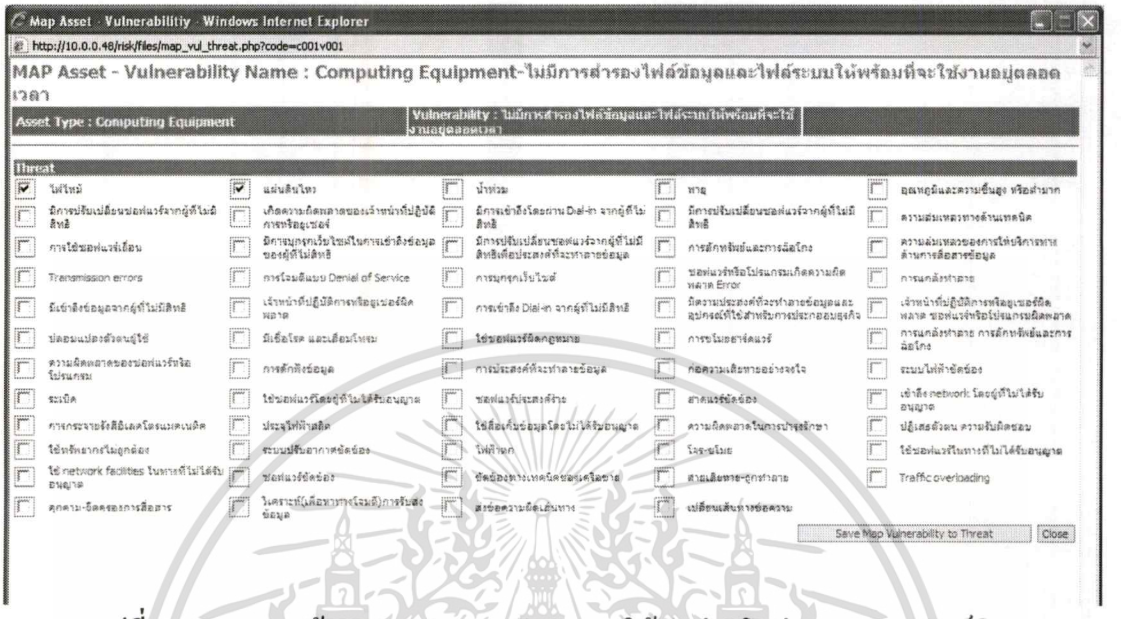


รูปที่ 6.22 แสดงหน้าเพจการกำหนดช่องโหว่ให้กับคลาสทรัพย์สิน

6.3.6 การจัดการการกำหนดภัยคุกคามให้กับช่องโหว่ของทรัพย์สิน

หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้กำหนดการวิเคราะห์ความเสี่ยงเสร็จสมบูรณ์แล้วระบบจะทำการแสดงหน้าเพจแสดงประเภทของทรัพย์สิน ดังรูปที่ 6.10 คลิกที่ Map Vulnerability-Threat ให้ทำการเลือกคลาสทรัพย์สินที่และช่องโหว่ที่ต้องการจะกำหนดภัยคุกคามให้กับคลาสทรัพย์สินนั้น แล้วคลิกที่ Detail จากคอลัมน์ Map ซึ่งจะแสดง

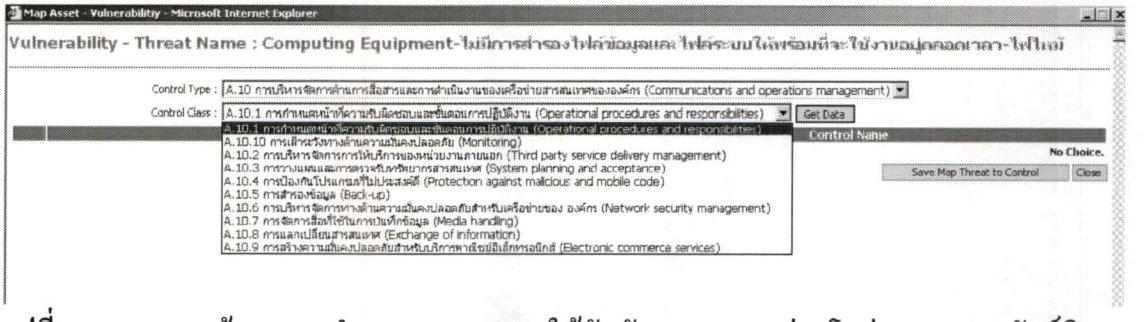
รายการของภัยคุกคามที่ได้ทำการเพิ่มไว้ ดังรูปที่ 6.23 คลิก Save เพื่อทำการบันทึกข้อมูลและคลิก Close เพื่อปิดหน้าเพจ



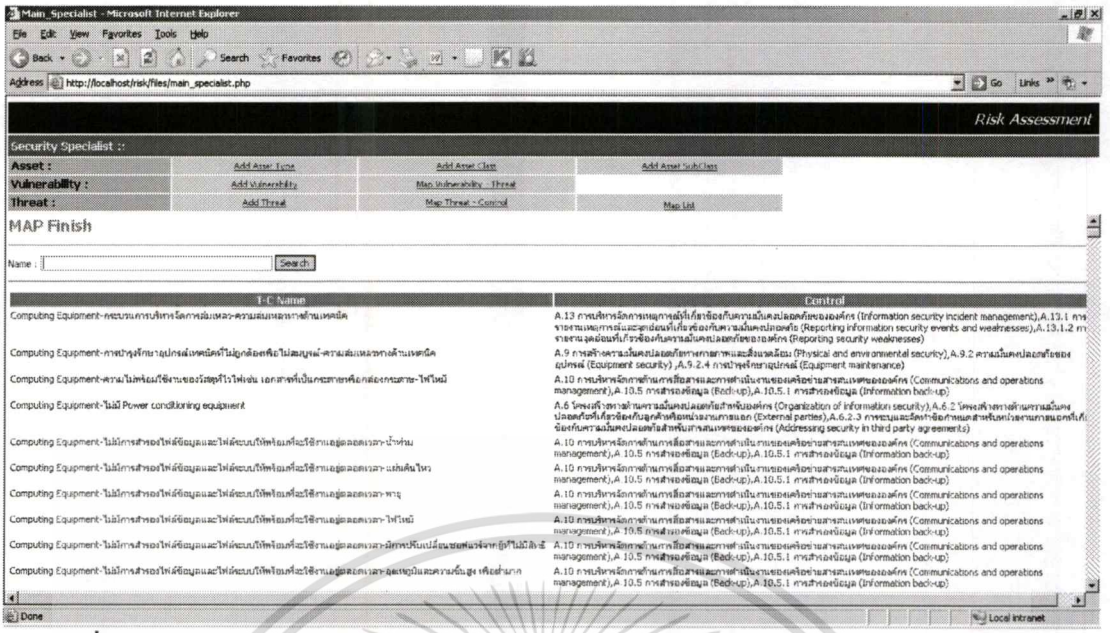
รูปที่ 6.23 แสดงหน้าเพจการกำหนดภัยคุกคามให้กับช่องโหว่ของคลาสทรัพย์สิน

6.3.7 การจัดการการกำหนดการควบคุมให้กับภัยคุกคามและช่องโหว่ของทรัพย์สิน

หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้กำหนดการวิเคราะห์ความเสี่ยงเสร็จสมบูรณ์แล้วระบบจะทำการแสดงหน้าเพจแสดงประเภทของทรัพย์สิน ดังรูปที่ 6.10 คลิกที่ Map Threat-Control ให้ทำการเลือกคลาสทรัพย์สิน-ช่องโหว่-ภัยคุกคามที่ต้องการจะกำหนดการควบคุม แล้วคลิกที่ Detail จากคอลัมน์ Map ซึ่งจะหน้าเพจในการกำหนดการควบคุม ดังรูปที่ 6.24 คลิก Save เพื่อทำการบันทึกข้อมูลและคลิก Close เพื่อปิดหน้าเพจ โดยจะสามารถดูข้อมูลการกำหนดการวิเคราะห์ความเสี่ยงทั้งหมดได้ที่ Map List จะแสดงหน้าเพจการกำหนดการวิเคราะห์ความเสี่ยงที่ได้กำหนดไว้ ดังรูปที่ 6.25



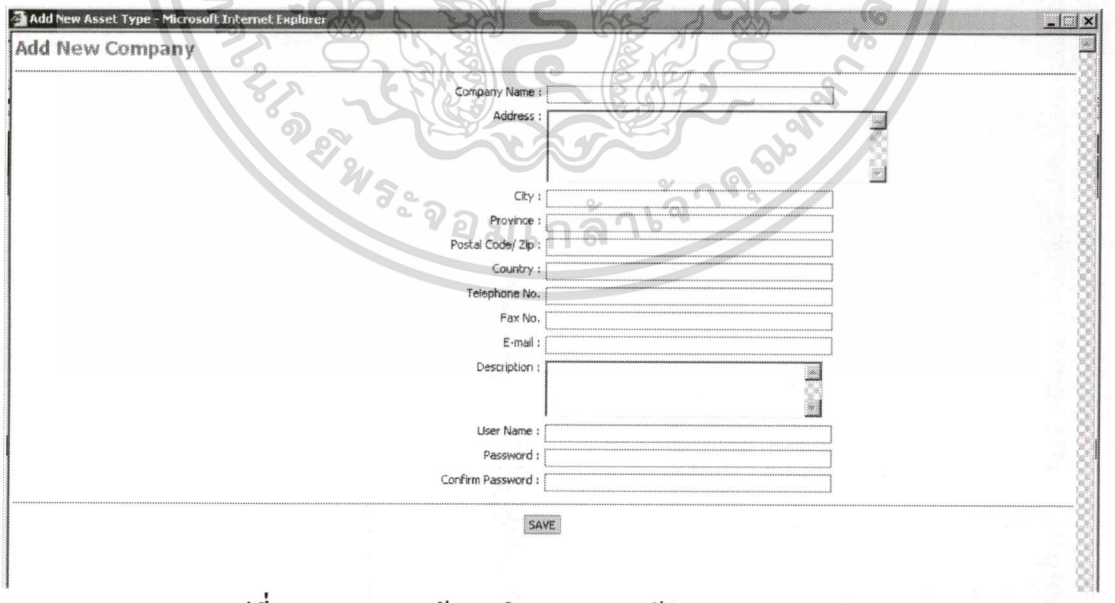
รูปที่ 6.24 แสดงหน้าเพจการกำหนดการควบคุมให้กับภัยคุกคามและช่องโหว่ของคลาสทรัพย์สิน



รูปที่ 6.25 รายการการกำหนดข้อมูลช่องโหว่ ภัยคุกคาม และการควบคุมให้กับทรัพย์สิน

6.3.8 การจัดการการลงทะเบียนของผู้ใช้งาน

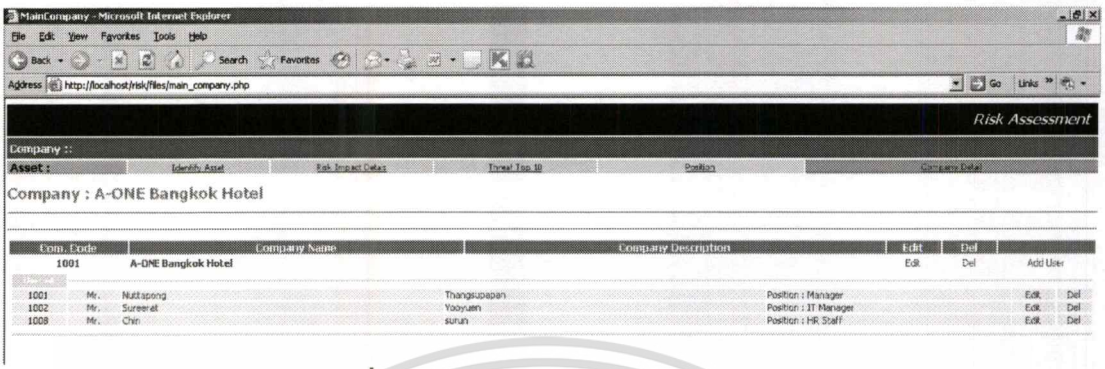
จากหน้าการล็อกอินผู้ใช้งานระบบสามารถทำการลงทะเบียนเพื่อใช้งานได้โดยคลิกที่ Register ดังรูปที่ 6.5 จะแสดงหน้าเพจในการกรอกข้อมูลการลงทะเบียนเพื่อใช้งานระบบดังรูปที่ 6.26



รูปที่ 6.26 แสดงหน้าเพจในการกรอกข้อมูลการลงทะเบียน

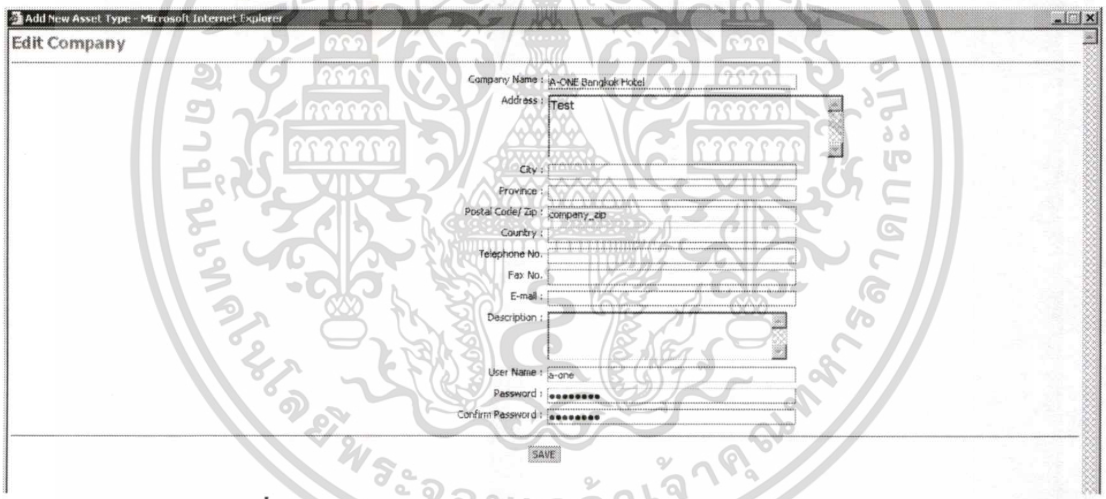
หลังจากทำการลงทะเบียนโดยกรอกข้อมูลและรายละเอียดของบริษัท และผู้ใช้งานแล้ว ให้ทำการล็อกอินเข้ามายังระบบด้วยชื่อผู้ใช้งาน และรหัสผ่านที่ทำการกำหนดไว้ในหน้าการ

ลงทะเบียน ซึ่งหลังจากการล็อกอินจะแสดงหน้าเพจหลักของบริษัทในแต่ละบริษัทที่ได้มีการลงทะเบียนไว้ ดังรูปที่ 6.27



รูปที่ 6.27 แสดงหน้าเพจหลักของบริษัท

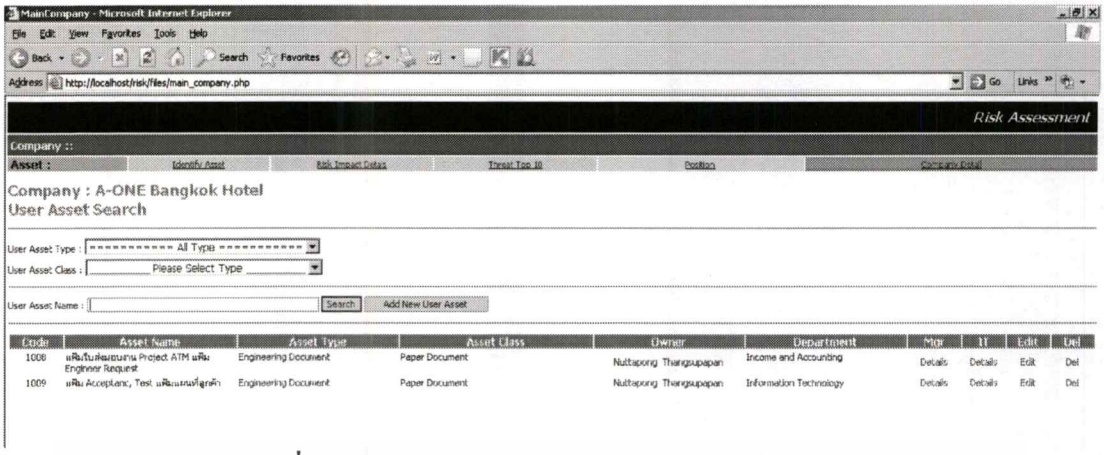
ถ้าต้องการแก้ไขข้อมูลของบริษัทให้คลิกที่ Edit ในช่องข้อมูลบริษัทจะแสดงหน้าเพจสำหรับการแก้ไขข้อมูลของบริษัท ดังรูปที่ 6.28



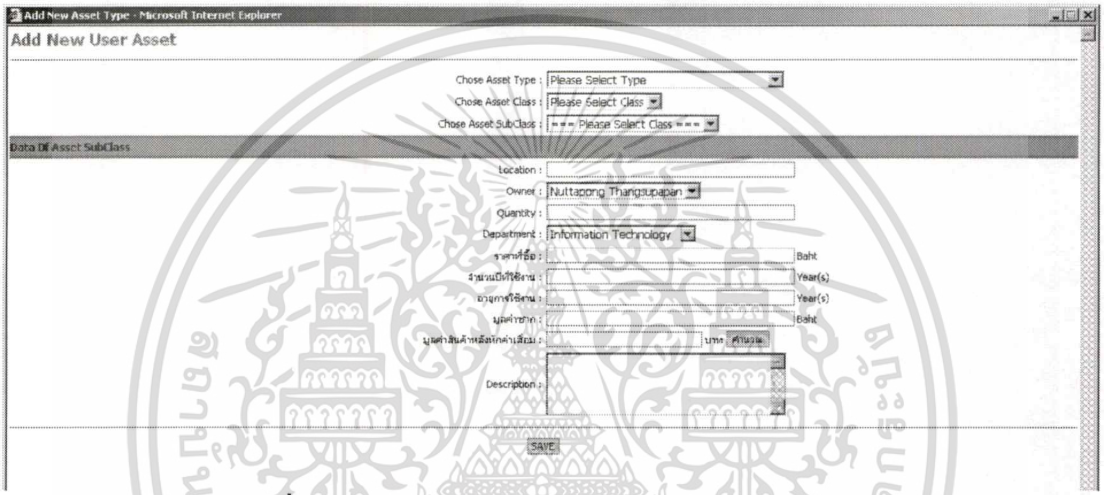
รูปที่ 6.28 แสดงหน้าเพจสำหรับการแก้ไขข้อมูลของบริษัท

6.3.9 การระบุทรัพย์สินของบริษัท

หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของบริษัทในแต่ละบริษัท ให้ทำการเลือกเมนู Identify Asset ซึ่งจะแสดงหน้าเพจรายการทรัพย์สินของบริษัทที่ได้มีการระบุไว้แล้วดังรูปที่ 6.29 โดยจะสามารถค้นหาได้จากการระบุประเภท และคลาสของทรัพย์สินที่ต้องการค้นหา และถ้าต้องการเพิ่มทรัพย์สินที่จะระบุให้กับบริษัทให้ทำการคลิกที่ Add New User Asset ดังรูปที 6.30

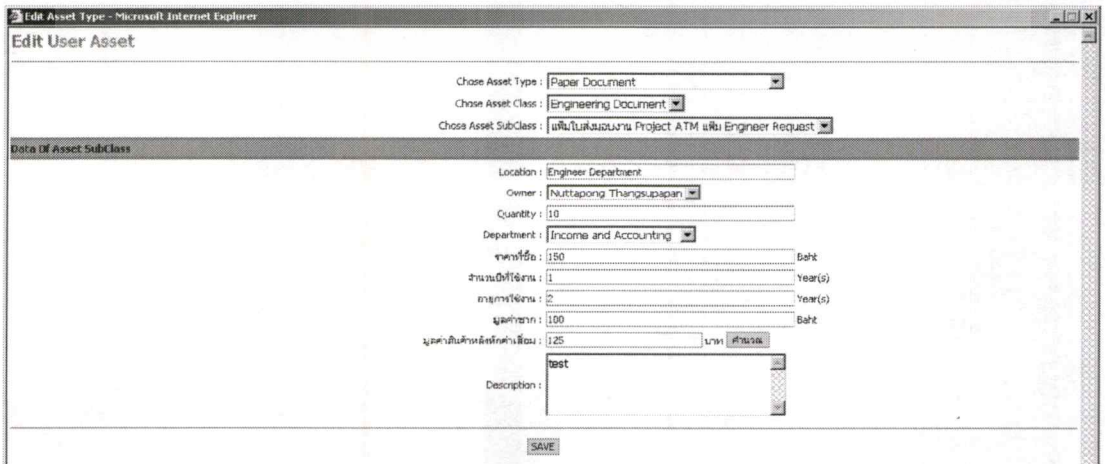


รูปที่ 6.29 แสดงหน้าเพจรายการทรัพย์สินของบริษัท



รูปที่ 6.30 แสดงหน้าเพจการระบุทรัพย์สินของบริษัท

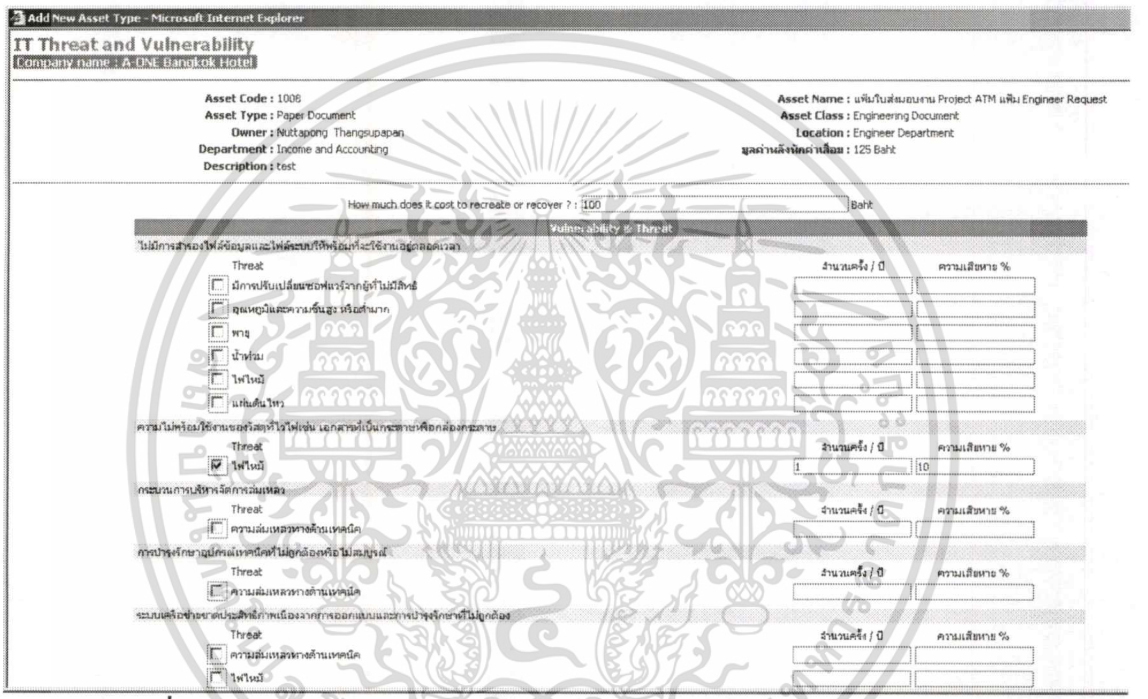
แต่ถ้าต้องการแก้ไขข้อมูลทรัพย์สินที่ได้ทำการระบุไว้แล้วนั้น ให้คลิก Edit จากหน้าเพจ รายการทรัพย์สินของบริษัทในรูปที่ 6.30 ซึ่งจะแสดงหน้าเพจสำหรับการแก้ไขข้อมูลทรัพย์สินของบริษัท ดังรูปที่ 6.31



รูปที่ 6.31 แสดงหน้าเพจสำหรับการแก้ไขข้อมูลทรัพย์สินของบริษัท

6.3.10 การระบุช่องโหว่และภัยคุกคามของทรัพย์สินบริษัท

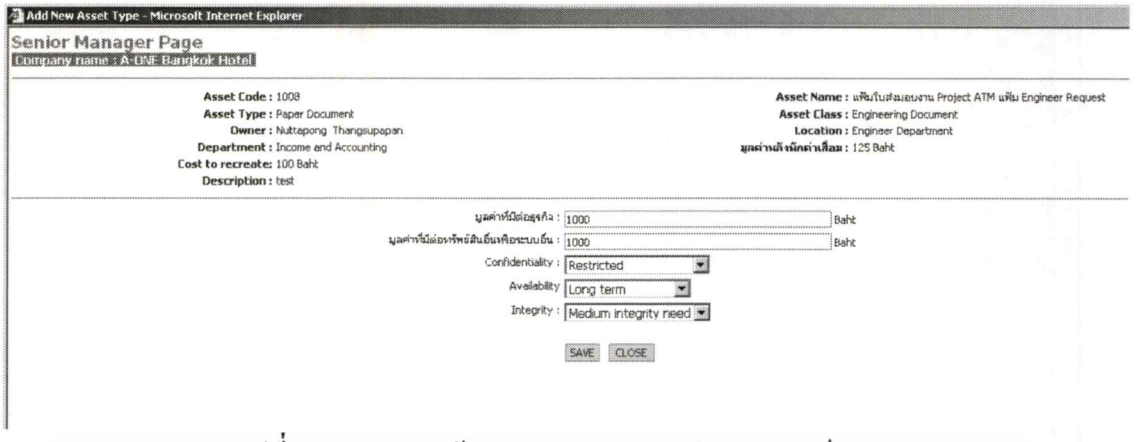
หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของบริษัทในแต่ละบริษัท ทำการเลือกเมนู Identify Asset ซึ่งจะแสดงหน้าเพจรายการทรัพย์สินของบริษัทที่ได้มีการระบุไว้แล้วดังรูปที่ 6.29 ให้คลิก Detail จากคอลัมน์ IT ซึ่งจะแสดงหน้าเพจการกำหนดช่องโหว่ และภัยคุกคามให้กับทรัพย์สิน ดังรูปที่ 6.32 โดยจะต้องระบุโอกาสที่จะเกิดภัยคุกคามและช่องโหว่เปอร์เซ็นต์ความเสียหายที่จะเกิดขึ้นจากช่องโหว่และภัยคุกคามนั้น ค่าใช้จ่ายในการกู้คืนหรือทำการสร้างใหม่



รูปที่ 6.32 แสดงหน้าเพจการกำหนดช่องโหว่ และภัยคุกคามให้กับทรัพย์สิน

6.3.11 การระบุมูลค่าของทรัพย์สินบริษัท

หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของบริษัทในแต่ละบริษัท ทำการเลือกเมนู Identify Asset ซึ่งจะแสดงหน้าเพจรายการทรัพย์สินของบริษัทที่ได้มีการระบุไว้แล้วดังรูปที่ 6.2ต ให้คลิก Detail จากคอลัมน์ Mgr ซึ่งจะแสดงหน้าเพจการกำหนดมูลค่าของทรัพย์สินดังรูปที่ 6.33

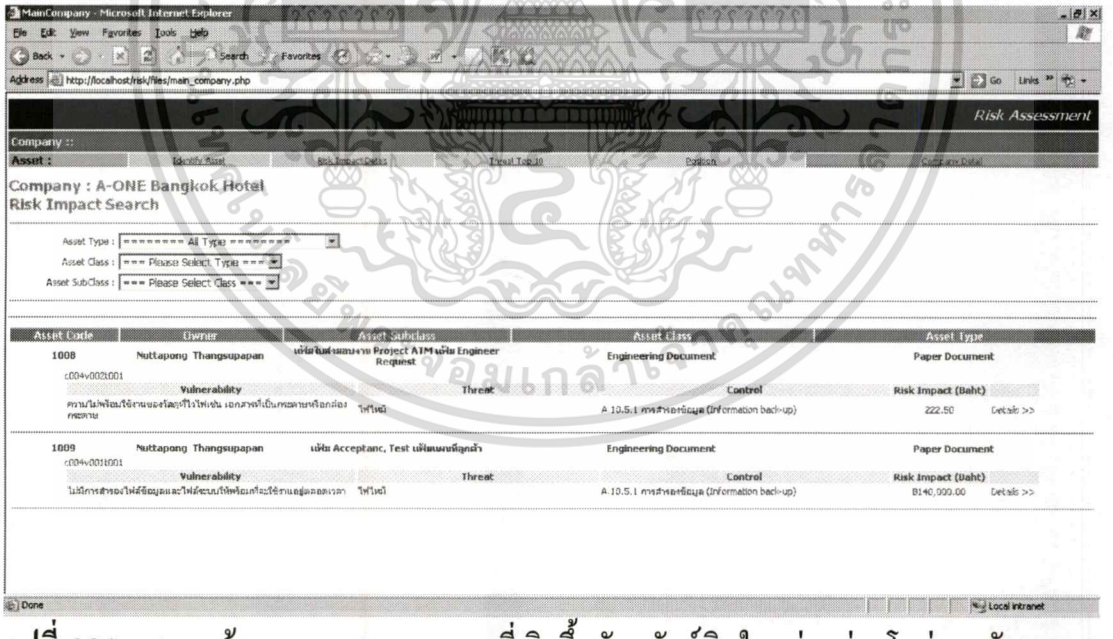


รูปที่ 6.33 แสดงหน้าเพจการกำหนดมูลค่าของทรัพย์สิน

6.3.12 การรออกรายงานการวิเคราะห์ความเสี่ยง และการควบคุม

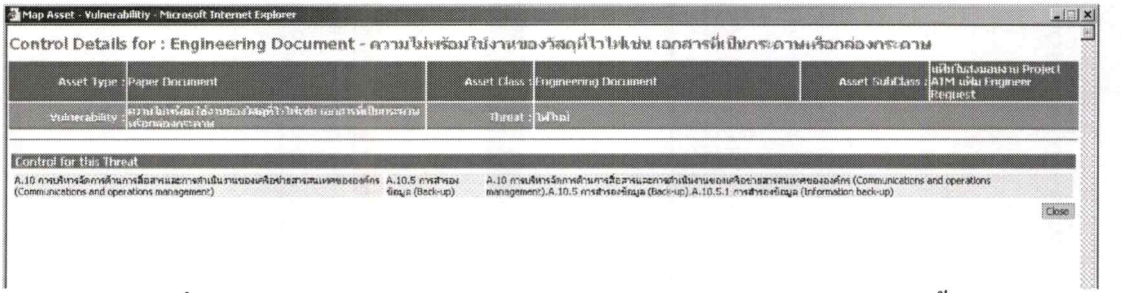
หลังจากที่ได้มีการล็อกอินโดยใช้ชื่อผู้ใช้และรหัสผ่านของบริษัทในแต่ละบริษัท สามารถทำการเลือกเมนูสำหรับแสดงรายงานดังนี้

- เมนู Risk Impact Detail จะแสดงหน้าเพจรายงานผลกระทบที่เกิดขึ้นกับทรัพย์สินในแต่ละช่องโหว่และภัยคุกคาม โดยสามารถดูได้จากประเภทของทรัพย์สิน หรือคลาสของทรัพย์สิน หรือคลาสย่อยของทรัพย์สิน ดังรูปที่ 6.34



รูปที่ 6.34 แสดงหน้าเพจรายงานผลกระทบที่เกิดขึ้นกับทรัพย์สินในแต่ละช่องโหว่และภัยคุกคาม

สามารถดูการควบคุมที่จะใช้กับช่องโหว่ และภัยคุกคาม ได้โดยคลิกที่ Detail จะแสดงข้อมูลการควบคุมสำหรับช่องโหว่และภัยคุกคามนั้น ดังรูปที่ 6.35



รูปที่ 6.35 แสดงเพจข้อมูลการควบคุมสำหรับช่องโหว่และภัยคุกคามนั้น

- เมนู Threat Top 10 จะแสดงหน้าเพจรายงานภัยคุกคามที่ก่อให้เกิดผลกระทบมากที่สุดในสิบรายการแรก โดยสามารถดูได้จากประเภทของทรัพย์สิน หรือคลาสของทรัพย์สิน หรือคลาสย่อยของทรัพย์สิน ดังรูปที่ 6.36

รูปที่ 6.36 แสดงหน้าเพจรายงานภัยคุกคามที่ก่อให้เกิดผลกระทบมากที่สุดในสิบรายการแรก

บทที่ 7
บทสรุป

7.1 สรุปโครงการ

เราไม่สามารถที่จะกำจัดความเสี่ยงให้หมดไปทั้ง 100 % และไม่อาจหลีกเลี่ยงความเสี่ยงได้เสมอไปในทุกสถานการณ์ แต่การมีระบบบริหารจัดการความเสี่ยงจะช่วยค้นหา ช่วยลดระดับความรุนแรง กำหนดการควบคุมและป้องกันความเสี่ยงต่างๆ ให้ลดน้อยลงในระดับหนึ่งที่เราสามารถยอมรับได้ หรืออย่างน้อยที่สุดก็ช่วยให้เรามีความตื่นตัว และมีความระมัดระวังอยู่เสมอ การตระหนักถึงความผิดพลาด และเตรียมแผนรองรับก่อนที่จะเกิดขึ้นจะช่วยลดความเสียสาย การสูญเสียที่จะเกิดขึ้น เป็นการแก้ปัญหาที่ปลายเหตุ ทำให้เสียค่าใช้จ่าย และทรัพยากรโดยไม่จำเป็น

7.2 สรุปผลการพัฒนา

1. ระบบเพิ่มความสามารถการจัดการการวิเคราะห์หาความเสี่ยงในการใช้งานสารสนเทศ
2. ระบบสามารถเพิ่มประสิทธิภาพในการกำหนดนโยบายทางด้านความมั่นคงปลอดภัยในการใช้สารสนเทศ
3. ระบบสามารถช่วยในการพัฒนาความรู้ความสามารถในการบริหารจัดการระบบสารสนเทศให้มีความมั่นคงปลอดภัย

7.3 ประโยชน์ที่ได้รับจากการออกแบบและพัฒนาระบบ

ประโยชน์ที่ได้รับจากการพัฒนาระบบในโครงการนี้สามารถสรุปได้ดังนี้

1. เป็นการศึกษาเรียนรู้ถึงข้อมูลเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศ การวิเคราะห์ความเสี่ยง การกำหนดรูปแบบการควบคุมความเสี่ยงที่จะเกิดขึ้นกับการใช้งานระบบสารสนเทศ
2. เป็นการนำความรู้ที่ได้จากการศึกษามาประยุกต์ใช้ในการวิเคราะห์ออกแบบ และพัฒนาระบบ เพื่อใช้งานจริง
3. เป็นการศึกษาเรียนรู้และประยุกต์ใช้เทคโนโลยีที่มีอยู่ในปัจจุบันมาใช้ในการสร้างระบบให้มีประสิทธิภาพ
4. รู้จักวิธีการวางแผนการพัฒนา การแก้ปัญหาที่เกิดขึ้นในการพัฒนาระบบ
5. ได้ระบบสารสนเทศเพื่อใช้ในการกำหนดความเสี่ยงของการใช้งานสารสนเทศ สามารถวิเคราะห์ถึงช่องโหว่ ภัยคุกคาม รวมถึงการกำหนดการควบคุมให้กับช่องโหว่ และภัยคุกคามเหล่านั้น

6. ได้เรียนรู้และเพิ่มทักษะการออกแบบและพัฒนาระบบงานด้วย UML โดยที่สามารถนำไปประยุกต์ใช้ในการออกแบบระบบงานอื่นได้
7. เรียนรู้การพัฒนาโปรแกรมด้วยภาษา PHP และสามารถนำมาประยุกต์ในการเขียนโปรแกรมได้เรียนรู้การจัดการฐานข้อมูล MySQL

บรรณานุกรม

คณะอนุกรรมการด้านความมั่นคง ใน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. 2549. **มาตราฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทาอิเล็กทรอนิกส์.** [Online]. เข้าถึงได้จาก : http://www.thaicert.nectec.or.th/event/Security Standard/ SecurityStandardV2-2549.pdf

AIRMIC, ALARM, and IRM. 2002. **A Risk Management Standard.** [Online]. Available : http://www.theirm.org/publications/documents/Risk_Management_Standard_030820 .pdf.

EBIOS Club. 2004. **EBIOS v2 – Section 3 – Techniques – 5 February 2004.** [Online]. Available : http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section3-techniques -2004-02-05_en.pdf

Government Chief Information Office. 2007. **Information Security Guide.** [Online]. Available : http://www.gcio.nsw.gov.au/documents/Information Security Guideline V1.1.pdf

National Institute of Standards and Technology. 2002. **Risk Management Guide for Information Technology Systems.** [Online]. Available : http://csrc.nist.gov/pub lications /nistpubs/800-30/sp800-30.pdf.

Queensland Government. 2005. **Minimum Asset Information Requirements for Non - Current Assets.** [Online]. Available : http://www.treasury.qld.gov.au/office / knowledge /docs /asset-planning/asset-information.pdf

Shon Harris. 2005. **All-In-One CISSP.** Osborne : McGraw-Hill.

ประวัติผู้เขียน

นางสาวศศิวิมล เนตรสูงเนิน เกิดเมื่อวันที่ 16 สิงหาคม พ.ศ.2516 ที่จังหวัดอุบลราชธานี สำเร็จการศึกษาปริญญาตรีวิทยาศาสตร์บัณฑิต สาขาวิทยาการคอมพิวเตอร์ จากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยรามคำแหง ในปีการศึกษา 2544 และเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิทยาการเทคโนโลยีสารสนเทศ ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2547 โดยในปี พ.ศ. 2544 ได้เข้าทำงานในตำแหน่งเจ้าหน้าที่ระบบงานคอมพิวเตอร์ โรงเรียนนานาชาติรีเจนท์ และในปี พ.ศ. 2545 ได้เข้าทำงานในตำแหน่งเจ้าหน้าที่อบรมที่บริษัท American Information System ปัจจุบันทำงานในตำแหน่ง Network Specialist ที่บริษัทพีพี ออนไทม์จำกัด