ระบบสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยง

INFORMATION SYSTEM FOR RISK MANAGEMENT

โดย

มนตรี ทองมา

MONTRI THONGMA

อาจารย์ที่ปรึกษา

ดร.สิงหะ ฉวีสุข

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิตสาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2555

INFORMATION SYSTEM FOR RISK MANAGEMENT

MONTRI THONGMA

A REPORT SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2012

Title	INFORMATION SYSTEM FOR RISK MANAGEMENT
Student	Mr. Montri Thongma
Student ID	54660771
Degree	Master of Science
Program	Information Technology
Major	Information Technology and Management
Academic Year	2012
Advisor	Dr.Singha Chaveesuk

ABSTRACT

This independent study is a study and building prototype of the information technology risk management at SPANSION (Thailand) Ltd. The project's objective is aimed to improve efficiency in the organization's risk management. Currently the company's procedure is recorded in document which is difficult to use.

The methodology for this study starts with the analysis of the current risk management in several ways. The project is developed by applying the NIST SP800-30 approach to analyze and design the system. It presents analyzing methods, risk evaluation, threat identification, system vulnerability, level of risk, impact, control plan, preventive action, and risk mitigation. The analysis and design use object-oriented approach with UML, .net framework for Web Application and Microsoft SQL server for database.

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญตาราง(ต่อ)

สารบัญรูป

สารบัญรูป(ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

ในบทนำนี้จะได้กล่าวถึง ความเป็นมาขององค์กร ประเด็นปัญหาสำคัญที่ประสบในปัจจุบัน ซึ่งนำมาสู่การพัฒนาระบบสารสนเทศตามโครงการ ซึ่งมีหัวข้อดังต่อไปนี้

1.1 ความเป็นมา

1.2 วัตถุประสงค์

1.3 ขอบเขตของการจัดทำระบบ

1.4 ผลคาดว่าจะได้รับ

1.1 ความเป็นมา

บริษัทสแปนชั่น (ไทยแลนด์) จำกัด เป็นองค์กรที่ดำเนินธุรกิจ ประเภทเซมิคอนดักเตอร์ หน่วยความจำ NOR FLASH สำนักงานใหญ่ อยู่ที่ประเทศสหรัฐอเมริกา มีฐานการผลิตใหญ่ ในประเทศไทย ก่อตั้งในปี พ.ศ. 2546 โดยองค์กรได้กำหนดวิสัยทัศน์ ไว้อย่างชัดเจนว่า "ลูกค้าคือหัวใจที่สำคัญของธุรกิจของเรา"

บริษัทได้นำเอาเทคโนโลยีสารสนเทศ ซึ่งถือว่าเป็นเครื่องมือสำคัญ มาประยุกต์และประสานการทำงานร่วมกันในด้านต่างๆ เป็นระบบคอมพิวเตอร์และเครือข่ายทั่วโลก เพื่อผลักดันให้ธุรกิจประสพความสำเร็จ เมื่อนำเทคโนโลยี เหล่านี้มาทำงานร่วมกัน อาจทำให้เกิดความเสี่ยงหรือโอกาสที่เกิดความเสียหาย หรือถูกรบกวน กับธุรกิจขององค์กรขึ้นได้ ทางองค์กรจึงได้มีการจัดการประเมินความเสี่ยง ของระบบเทคโนโลยีสารสนเทศ อย่างต่อเนื่องเสมอมา แต่ยังเป็นการประเมินในกระดาษ เป็นรูปแบบ Excel File และจัดเก็บขึ้น Intranet ขององค์กร การประเมินแต่ละครั้งจะประสพปัญหาความไม่สะดวก และไม่สามารถดูข้อมูลรายละเอียดได้ ไม่มีฐานข้อมูลกลาง ใช้ระยะเวลานานในการประเมินในแต่ละครั้ง

ดังนั้นการพัฒนาระบบสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยง จึงมีความจำเป็นและมีประโยชน์กับองค์กร สำหรับผู้บริหาร หรือผู้ดูแลระบบสารสนเทศให้มีความมั่นคงปลอดภัย

โดยวัตถุประสงค์ของการพัฒนาระบบบริหารจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศ มีรายละเอียดดังต่อไปนี้

1.2 วัตถุประสงค์

การจัดทำระบบสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยง มีวัตถุประสงค์ดังนี้

1) เพื่อใช้ในการรวบรวมข้อมูลทรัพย์สินของระบบเทคโนโลยีสารสนเทศ
2) เพื่อศึกษามาตราฐานการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ
3) เพื่อวิเคราะห์และประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศในปัจุบัน
4) เพื่อออกแบบและพัฒนาระบบ สนับสนุนการบริหารจัดการความเสี่ยง

1.3 ขอบเขตของการจัดทำระบบ

การวิเคราะห์และออกแบบระบบสารสนเทศ เพื่อสนับสนุนการบริหารความเสี่ยง มีขอบเขตในการจัดทำดังต่อไปนี้

1.3.1 ขอบเขตของระบบที่เป็นหน้าที่หลัก

แบ่งเป็น 4 หน้าที่ ได้แก่

1) ระบบสามารถบันทึก ปรับปรุง แก้ไข และออกรายงาน ข้อมูลการประเมินความเสี่ยง (Risk Assessment) เช่น ข้อมูลทรัพย์สิน, ข้อมูลภัยคุกคาม, ข้อมูลจุดอ่อน, การควบคุม, โอกาสความเป็นไปได้ของภัยคุกคามของทรัพย์สินนี้, ผลกระทบทางธุรกิจถ้าทรัพย์สินนี้เสียหาย เป็นต้น

2) ระบบสามารถแสดงคำนวณและแสดงแผนผังการประเมินความเสี่ยง (Risk Matrix Score)

3) ระบบสามารถบันทึก ปรับปรุง แก้ไข และออกรายงาน แผนการบรรเทาความเสี่ยง (Risk Mitigation)

4) ระบบสามารถแสดงและออกรายงานการบริหารจัดการความเสี่ยงในรูปแบบต่างๆ ให้ผู้บริหาร หรือผู้ดูแลระบบ สามารถนำไปใช้งานได้

1.3.2 ขอบเขตของระบบที่ไม่ใช่หน้าที่หลัก

แบ่งเป็น 3 หน้าที่ ได้แก่

1) มีการตรวจสอบสิทธิ์ในการใช้งานระบบ
2) ระบบมีข้อมูลนโยบายการบริหารความเสี่ยงขององค์กร
3) ระบบมีข้อมูลแสดงเกี่ยวกับการบริหารความเสี่ยงตามมาตรฐาน NIST 800-30

1.4 ผลคาดว่าจะได้รับ

จากการนำระบบสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยง มาใช้ในการดำเนินการจะได้รับผล ดังต่อไปนี้

1) มีระบบรวบรวมข้อมูลทรัพย์สินของระบบเทคโนโลยีสารสนเทศ

2) ทราบถึงมาตราฐานการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ

3) ผู้บริหารหรือผู้ดูแลระบบเทคโนโลยีสารสนเทศ สามารถมีข้อมูล เพื่อช่วยในการวิเคราะห์ บริหารจัดการความเสี่ยง และวางแผนสร้างความมั่นคง และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ได้อย่างมีประสิทธิภาพมากขึ้น

4) งานด้านดูแลระบบเทคโนโลยีสารสนเทศมีมาตรฐาน ลดความซ้ำซ้อน สะดวก และรวดเร็วมากยิ่งขึ้น

5) มีต้นแบบ หรือ Prototype ระบบสนับสนุนการบริหารจัดการความเสี่ยง (Risk Management System) เพื่อพัฒนาใช้งานจริงกับองค์กร

บทที่ 2
ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

ความรู้ทางเทคโนโลยีสารสนเทศและเครื่องมือต่างๆ สามารถแบ่งได้ดังนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

1) มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและข้อมูล ISO/IEC 27001
2) มาตรฐานการจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศและข้อมูล NIST SP 800-30
3) SDLC-System development life-cycle
4) การวิเคราะห์และออกแบบระบบเชิงออบเจ็ค
   - แนวความคิดพื้นฐานเชิงออบเจ็ค
   - การสร้างแบบจำลองด้วยยูเอ็มแอล
5) การออกแบบฐานข้อมูลเชิงสัมพันธ์

2.2 เทคโนโลยีที่นำมาใช้

1) เครื่องมือเคส (CASE Tools)
2) ดอตเน็ตเฟรมเวิร์ค (.Net framwork)
3) เอเอสพีดอตเน็ต (ASP.NET)
4) วิชวลสตูดิโอ (Microsoft Visual Studio 2010)
5) เว็บแอพพลิเคชั่น (Web Application)
6) เอสคิวแอลเซิฟเวอร์ (SQL Server)
7) อินเทอร์เน็ต อินฟอร์เมชั่นเซิฟเวอร์ (IIS)
8) คริสตอล รีพอร์ท (Crystal report)

2.1 ทฤษฎีที่เกี่ยวข้องในการออกแบบและพัฒนาระบบ

มาตรฐานสากลต่างๆ ที่ว่าด้วยการบริหารความเสี่ยงเหล่านี้มีอยู่หลายมาตรฐานด้วยกัน บางมาตรฐานก็ไม่เหมาะสำหรับการประเมินความเสี่ยงระบบสารสนเทศ (IT Risk Assessment) ทำให้องค์กรหลายแห่งเกิดปัญหาในการเลือกใช้มาตรฐานต่างๆ ยกตัวอย่าง เช่น

มาตรฐานของ NIST (National Institute of Standards and Technology) ได้แก่ NIST 800-30 "Risk Management Guide for Information Technology Systems",

มาตรฐานของ Australia และ New Zealand ได้แก่ AS/ NZS 4360:2004

มาตรฐานของ Software Engineering Institute (SEI) แห่งมหาวิทยาลัย Carnegie Mellon ได้แก่มาตรฐาน OCTAVE ซึ่งย่อมาจาก Operationally Critical Threat, Asset and Vulnerability Evaluation

เฟรมเวิร์ค (Framework) ต่างๆที่หลายคนคงเคยได้ยินไม่ว่าจะเป็น COSO Framework , CoBit Framework และ ISO/ IEC17799 ซึ่งขณะนี้ได้เปลี่ยนเป็น ISO/IEC 27001 เป็นต้น

ผู้บริหารด้านความปลอดภัยข้อมูลขององค์กรหลายคนเกิดความสับสนและไม่รู้ว่าจะนำมาตรฐานหรือเฟรมเวิร์คใดมาใช้ให้เหมาะสมกับการบริหารความเสี่ยงระบบสารสนเทศในองค์กรของตน

ทำความเข้าใจกับคำว่า "Methodologies" และ "Frameworks"

“Risk Management Methodologies” ได้แก่ ขั้นตอน หรือ วิธีการในการบริหารความเสี่ยงอย่างถูกต้องตามหลักการมาตรฐานสากลที่ทั่วโลกยอมรับและนำมาประยุกต์ใช้กันโดยทั่วไป

"Framework"นั้นหมายถึงขั้นตอนหรือวิธีการที่ช่วยให้องค์กรได้"Compliance"ตามหลักการ มาตรฐานสากล ยกตัวอย่าง เช่น ถ้าพูดถึงการควบคุมภายใน หรือ "Internal Control" ก็จะหมายถึง COSO Framework หรือ Corporate Governance แต่ถ้าพูดถึง "IT Governance" ก็จะหมายถึง CobiT Framework ที่กำหนดขอบเขตแคบลงมาเจาะลึกในส่วนของระบบสารสนเทศ และถ้ากล่าวถึง Information Security Management System หรือ ISMS จะหมายถึง มาตรฐานสากล ISO/IEC27001

จะสังเกตได้ว่าทั้ง COSO, CobiT และ ISO/ IEC 27001 นั้น ได้กล่าวถึงเรื่องของ Risk Assessment และ Risk Management ด้วยกันทั้งสิ้น แต่ยังไม่มีรายละเอียดเจาะลึกในการทำ Risk Management และ Assessment ต่างจากมาตรฐาน NIST 800-30, OCTAVE หรือ AS/ NZS 4360:2004 นั่นคือเราต้องนำมาตรฐานดังกล่าวมาประยุกต์ใช้อีกครั้งหนึ่งเพื่อลงในรายละเอียดเพิ่มมากขึ้น และ ใน CobiT นั้น ได้กล่าวถึงเรื่องของ Risk Management ไว้ใน PO9 (Planning and Organization) ซึ่งก็จะลงรายละเอียดในระดับหนึ่ง แต่ยังไม่ละเอียดเหมือนกับมาตรฐานทั้งสามดังที่ได้กล่าวมาแล้ว

สำหรับมาตรฐาน NIST 800-30 นั้น จะเน้นเรื่อง Threat and Vulnerability Identification, Likelihood determination, Impact Analysis และ Control Recommendations นั่นคือ ต้องกำหนดภัย และ ช่องโหว่ ของระบบให้ได้เสียก่อน จากนั้นจึงดูโอกาสของความเสี่ยงที่อาจจะเกิดขึ้นประกอบกับ ผลกระทบจากความเสี่ยงดังกล่าว ตลอดจนถึงวิธีการแก้ไขปัญหาของความเสี่ยงในรูปแบบต่างๆ โดยมาตรฐาน NIST 800-30 ถือเป็นต้นแบบซึ่งมาตรฐานอื่นๆ นำไปปรับปรุงแก้ไขให้มีรายละเอียดเน้นไปตามวัตถุประสงค์ของมาตรฐานนั้นๆ

สำหรับ ISO/ IEC 17799 และ ISO/ IEC 27001 ถือได้ว่าเป็นมาตรฐานสากล (International Standard) ด้านการบริหารจัดการเรื่องของความปลอดภัยข้อมูล ซึ่งจะครอบคลุมเรื่องสำคัญต่างๆ อาทิ เช่น Security Policy และ Security Incident Management ซึ่งวัตถุประสงค์ก็ไม่ได้ต่างจากวัตถุประสงค์ของการบริหารความเสี่ยงระบบสารสนเทศ ซึ่งก็คือการลดความเสี่ยง (Risk Reduction) ให้อยู่ในจุดที่ยอมรับได้ (Risk Acceptance Level) โดยมีสมมุติฐานเหมือนกันคือ "เราไม่สามารถลดความเสี่ยงให้เท่ากับศูนย์ได้ แต่เราสามารถบริหารจัดการความเสี่ยงให้อยู่ในจุดที่เรายอมรับในความเสียหายที่เกิดขึ้นได้ และ สามารถทำให้องค์กรดำเนินงานได้ต่อเนื่องอย่างไม่ติดขัด"

กล่าวโดยสรุปคือ "การบริหารความเสี่ยงนั้นขึ้นอยู่กับมุมมอง" ถ้าเรามองด้านธุรกิจ การบริหารความเสี่ยงของธุรกิจก็จะขึ้นกับการตัดสินใจของผู้บริหาร เช่น ตัดสินใจว่าจะผลิตสินค้าหรือจะยกเลิกการผลิตสินค้า เป็นต้น แต่ถ้าเรามองในด้านความปลอดภัยข้อมูลสารสนเทศ เรามักจะเจาะลึกถึงขั้นตอนรายละเอียดในการปฏิบัติการ ตลอดจนรายละเอียดทางด้านเทคนิค ซึ่งต้องมีกระบวนการประเมินความเสี่ยงอื่นเสริมเข้ามาช่วยด้วย เช่น การทำ Vulnerability Assessment และ Penetration Testing เพื่อช่วยให้เราเกิดความมั่นใจกับความปลอดภัยของระบบสารสนเทศมากขึ้น (ปริญญา หอมเอนก. 2006 : Online)

2.1.1 มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและข้อมูล ISO/IEC 27001

กระบวนการในการบริหารความเสี่ยงตามมาตรฐาน ISO/IEC 27001 จะประกอบด้วย 2 ส่วนหลักๆ คือ

1. การประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยงที่กล่าวถึงในที่นี้จะหมายถึงความเสี่ยงในรูปแบบต่างๆ ที่อาจก่อให้เกิดผลเสียหายต่อข้อมูลสำคัญและระบบ อุปกรณ์ต่างๆที่สนับสนุนการทำงานให้กับข้อมูลสำคัญนี้อยู่ โดยขั้นตอนนี้จะเป็นขั้นตอนการประเมินระดับของความเสี่ยง (Risk Level) ที่มีทั้งหมดต่อข้อมูลและทรัพย์สินต่างๆ ขององค์กร เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรยอมรับได้ไปดำเนินการควบคุมและแก้ไขความเสี่ยงในขั้นต่อไป

ระดับของความเสี่ยงจะพิจารณาจาก 2 ปัจจัยคือ

1) ความน่าจะเป็น (Probability) ในการที่จะเกิดภัยคุกคามใดๆขึ้น และก่อให้เกิดความเสียหายต่อข้อมูลและทรัพย์สินขององค์กร ซึ่งปกติจะคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคามและช่องโหว่ (Threat/Vulnerability Assessment) ที่มีต่อข้อมูลและทรัพย์สินขององค์กร ร่วมกับการพิจารณาถึงวิธีการควบคุม และการแก้ไขความเสี่ยงที่มีอยู่ในปัจจุบัน

2) ความรุนแรง (Severity) ของความเสียหายที่อาจเกิดขึ้น ซึ่งปกติจะคำนวณค่าโดยการพิจารณาจาก ระดับความสำคัญของข้อมูล หรือทรัพย์สินนั้นๆ ทีมีต่อองค์กร (อรรณพ ขันธิกุล. 2553 : 49)

2. การรักษาความเสี่ยง (Risk Mitigation)

มี 4 วิธีได้แก่

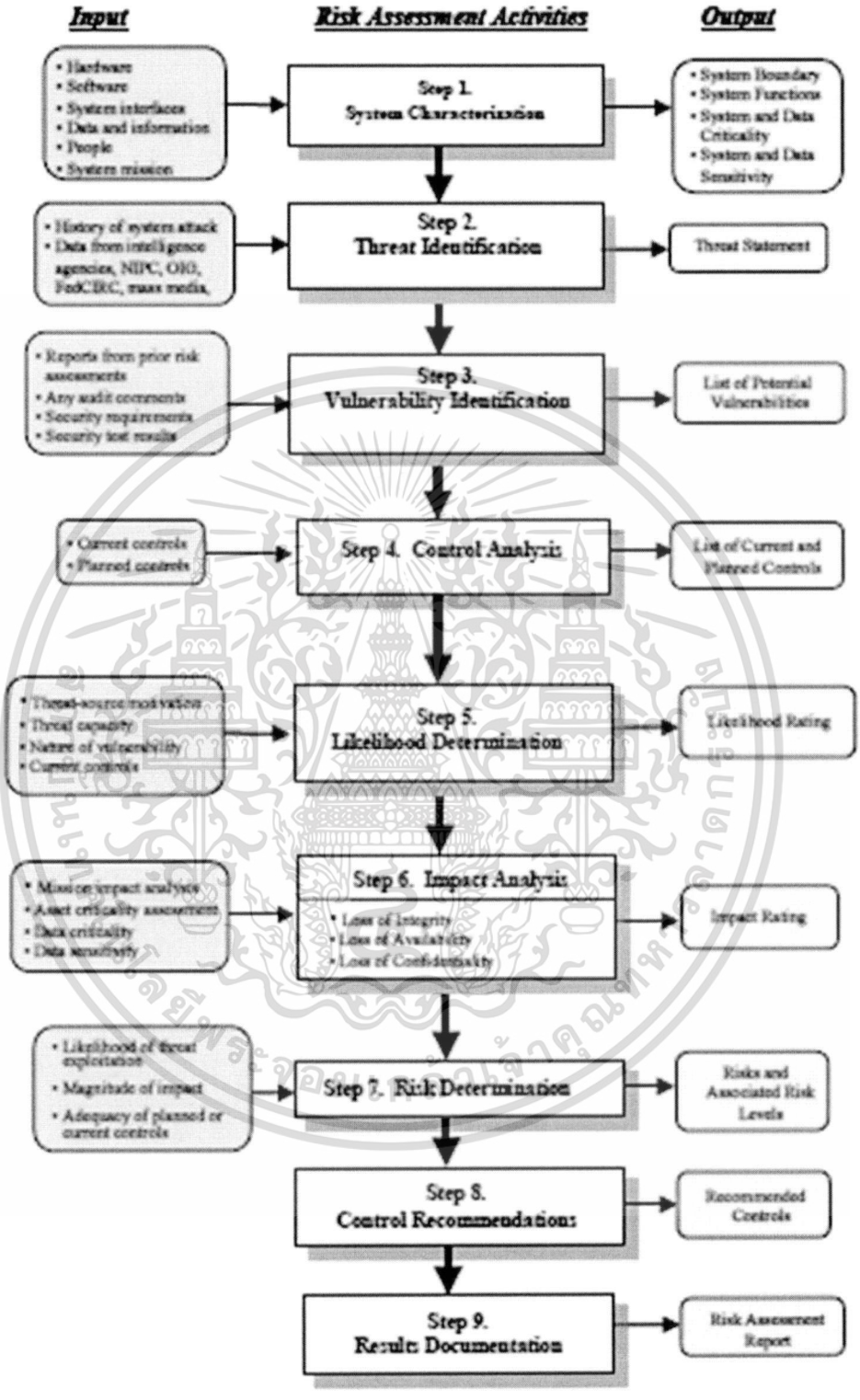
1) การลดความเสี่ยง (Risk Reduction)

2) การยอมรับความเสี่ยง (Risk Acceptance)

3) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

4) การย้ายโอนความเสี่ยง (Risk Transfer)

2.1.2 มาตรฐานการจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศและข้อมูล NIST SP 800-30 มี 9 ขั้นตอนดังรูปที่ 2.1



รูปที่ 2.1 แสดงขั้นตอนกระบวนการในการจัดทำ Risk Assessment

ที่มา (http://csrc.nist.gov/publications/PubsSPs.html)

1. รายละเอียดเกี่ยวกับระบบ (System Characterization)

- กำหนดขอบเขต ที่จะจัดเก็บข้อมูลของระบบ หรืออุปกรณ์ และผู้ดูแลระบบ

- ระบุรายละเอียดของระบบและอุปกรณ์ เช่น เป็นระบบอะไร หรืออุปกรณ์ประเภทไหน ทำงานอย่างไร ใครเป็นผู้ดูแลรับผิดชอบ

- รวบรวมข้อมูล

2. ระบุภัยคุกคาม (Threat Identification)

ระบุภัยคุกคามประเภทต่าง ยกตัวอย่าง ภัยจากธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว พายุ แผ่นดินถล่ม ภัยจากมนุษย์ เช่น Hacker หรือ Cracker ภัยจากสถาพแวดล้อม เช่น ระบบไฟ ระบบความเย็น ของห้องคอมพิวเตอร์ เป็นต้น

3. ระบุช่องโหว่ (Vulnerability Identification)

ความอ่อนแอ ของระบบ หรืออุปกรณ์ ยกตัวอย่างเช่น ไม่มีกำหนดสิทธ์ในการเข้าถึงข้อมูล (Access Control) หรือ ไม่มีการอัพเดทโปรแกรม Anti Virus อย่างสม่ำเสมอ เป็นต้น

4. วิเคราะห์การควบคุม (Control Analysis)

1) เครื่องมือในการควบคุม

- ด้านเทคนิค (Technical Controls) เช่น ติดตั้ง IPS, IDS, Firewall

- ที่ไม่ใช่ด้านเทคนิค (Nontechnical Controls) เช่น ออกกฎระเบียบ ข้อกำหนดนโยบานและกระบวนการต่าง ๆ

2) ประเภทการควบคุม

- การควบคุมแบบป้องกันไม่ให้ความเสี่ยงเกิดขึ้น (Preventive Controls) เช่น ติดตั้ง Firewall หรือ ตรวจสอบประวัติพนักงาน เป็นต้น

- การควบคุมแบบตรวจจับความผิดปกติที่เกิดขึ้น (Detective Controls) เช่น ติดตั้ง IDS หรือ รปภ. กล้องวงจรปิด CCTV เป็นต้น

- การควบคุมแบบการแก้ไขให้กลับคืนสู่สภาพปกติ (Corrective Controls)

5. การระบุโอกาสที่จะเกิดขึ้น (Likelihood Determination)

ขึ้นกับแรงจูงใจของผู้คุกคามและความสามารถของผู้คุกคาม ชนิดของช่องโหว่ โดยแบ่งเป็นระดับของโอกาสที่จะเกิดได้ 3 ระดับ คือ สูง ปานกลาง และต่ำ ตามตารางที่ 2.1

ตารางที่ 2.1 การระบุโอกาสที่จะเกิดขึ้น

โอกาสที่จะเกิด	**คำอธิบาย**
สูงมาก (5)	เกิดขึ้นภายใน 1 ปี
สูง (4)	เกิดขึ้นภายใน 3 ปี
ปานกลาง (3)	เกิดขึ้นภายใน 5 ปี
ต่ำ (2)	เกิดขึ้นภายใน 10 ปี
ไม่มีโอกาส (1)	ไม่น่ามีโอกาสที่จะเกิดขึ้น

6. การวิเคราะห์ผลกระทบ (Impact Analysis)

ผลกระทบที่นำมาวิเคราะห์จะมี 3 ด้านได้แก่

1) ผลกระทบทางด้านการเงินขององค์กร (Financial)

2) ผลกระทบฝ่ายผลิต (Operational)

3) ผลกระทบทางด้านชื่อเสียงของบริษัท (Reputational)

4) ผลกระทบทางด้านกฎหมาย (Regulatory Legal)

ระดับของผลกระทบมี 3 ระดับ คือ สูง ปานกลาง และต่ำ ตามตารางที่ 2.2

ตารางที่ 2.2 การวิเคราะห์ผลกระทบ

ชนิดของผลกระทบ	ระดับของ ผลกระทบ		
	สูง (3)	กลาง (2)	ต่ำ (1)
ด้านการเงิน	- สูญเสีย $ 1,200,000 > หรือ 10% ของรายได้ภายใน 30 วัน - ถูกปรับด้านการเงิน $100,000 ต่อวัน	-สูญเสีย $ 600,000 > หรือ 5% ของรายได้ภายใน 30 วัน - ถูกปรับด้านการเงิน $50,000 ต่อวัน	-สูญเสีย $ 120,000 > หรือ 1% ของรายได้ภายใน 30 วัน - ถูกปรับด้านการเงิน $5,000 ต่อวัน
ฝ่ายผลิต	กระทบฝ่ายการผลิต - Automotive (>7 วัน) - Consumer electronics (>7 วัน) - Netwoking (>7 วัน) -Wireless (>7 วัน)	กระทบฝ่ายการผลิต - Automotive (>3 วัน) - Consumer electronics (>3 วัน) - Netwoking (>3 วัน) -Wireless (>3 วัน)	กระทบฝ่ายการผลิต - Automotive (<3 วัน) - Consumer electronics (<3 วัน) - Netwoking (<3 วัน) -Wireless (<3 วัน)

ตารางที่ 2.2 (ต่อ)

ชื่อเสียง	-เสียหายต่อชื่อเสียงขององค์ในทางลบระดับประเทศ -องค์กรสูญเสียความน่าเชื่อถือ และความเชื่อมั่นจากลูกค้า และผู้ลงทุนหลักโดยทั่วไป	-เสียหายต่อชื่อเสียงขององค์ในทางลบระดับภูมิภาค -องค์กรสูญเสียความน่าเชื่อถือ และความเชื่อมั่นจากลูกค้า และผู้ลงทุนบางกลุ่ม	-เสียหายต่อชื่อเสียงขององค์เล็กน้อย -องค์กรสูญเสียความน่าเชื่อถือ และความเชื่อมั่นจากลูกค้า และผู้ลงทุนเล็ก
กฎระเบียบ/กฎหมาย	ผิดกฎหมายและกระทบกับธุรกิจ	ผิดกฎหมายปรับเล็กน้อยได้รับจดหมายเตือน	ไม่มีผลทางกฎหมาย

7. การกำหนดความเสี่ยง (Risk Determination)

หาจาก โอกาสที่เสี่ยง และ ผลกระทบที่จะเกิด มักใช้ Matrix ในการกำหนด โดยมี โอกาสของภัยคุกคามเป็นแกน Y และ ผลกระทบ เป็นแกน X เริ่มต้นค่าที่ 1 โดยการให้น้ำหนักภัยคุกคามและระดับผลกระทบจะแบ่งเป็น 3 ระดับ คือ สูง ปานกลาง และต่ำ ดังตารางที่ 2.3 และการกำหนดความเสี่ยงจะแบ่งเป็น 3 ระดับ คือ สูง ปานกลาง และต่ำ ดังตารางที่ 2.4

ตารางที่ 2.3 การให้น้ำหนักภัยคุกคามและระดับผลกระทบ

	Impact		
Threat Likelihood	**Low (1)**	**Medium (2)**	**High (3)**
สูงมาก (5)	Low 1x5=5	Medium 2x5=10	High 3x5=15
สูง (4)	Low 1x4=4	Medium 2x4=8	High 3x4=12
ปานกลาง (3)	Low 1x3=3	Medium 2x3=6	Medium 3x3=9
ต่ำ (2)	Low 1x2=2	Low 2x2=4	Medium 3x2=6
ไม่มีโอกาส (1)	Low 1x1=1	Low 2x1=2	Low 3x1=3

หมายเหตุ

- Risk Scale

  High (>10 to 15)

  Medium (>5 to 10)

  Low (1 to 5)

ตารางที่ 2.4 การกำหนดความเสี่ยง

ระดับความเสี่ยง	คำอธิบายและการกระทำที่จำเป็น
สูง	ต้องมีการแก้ไขทันที ระบบอาจสามารถทำงานได้ แต่การแก้ไขยังคงต้องทำ
ปานกลาง	วางแผนที่จะลดความเสี่ยง/แก้ไขว่าทำเมื่อไหร่ โดยเป็นช่วงระยะเวลาที่เหมาะสม
ต่ำ	ระบุว่าจะแก้ไขยังไง และพิจารณาว่าจะแก้ไขหรือยอมรับหรือไม่

8. คำแนะนำสำหรับการควบคุม (Control Recommendations)

แบ่งออกเป็น 3 คำแนะนำ

1) การควบคุมแบบป้องกันไม่ให้ความเสี่ยงเกิดขึ้น (Preventive Controls)
2) การควบคุมแบบตรวจจับความผิดปกติที่เกิดขึ้น (Detective Controls)
3) การควบคุมแบบการแก้ไขให้กลับคืนสู่สภาพปกติ (Corrective Controls)

9. เอกสารสรุป (Results Documentation)

สรุปผลเป็นเอกสารตามรูปแบบ SP800-30

2.1.3 วงจรในการพัฒนาระบบ (System Development Life Cycleหรือ SDLC)

เป็นโครงร่างหรือแนวทางวิธีการ เพื่อใช้ทำความเข้าใจและเพื่อใช้เป็นขั้นตอนการพัฒนาระบบสารสนเทศ หรือซอฟต์แวร์ให้สำเร็จ โดยการให้มาซึ่งซอฟแวร์อาจจะเป็นโดยการซื้อหรือการจ้างทำหรือการพัฒนาเองก็ได้

ระเบียบวิธีการพัฒนาซอฟต์แวร์มีอยู่หลายวิธีการ แต่ละวิธีการมีข้อดีและข้อเสียที่แตกต่างกัน ตัวอย่างระเบียบวิธีการพัฒนาซอฟต์แวร์ที่ได้รับความนิยม เช่น โครงสร้างแบบน้ำตก (Waterfall Model), โครงสร้างแบบก้นหอย (Spiral Model), วิธีการพัฒนาซอฟแวร์แบบคล่องแคล่วว่องไว (Agile Software Development)

ลำดับวงจรชีวิตของการพัฒนาซอฟต์แวร์

1. การวางแผน (Planning) เป็นขั้นตอนการการวางแผนงานโดย กำหนดรูปแบบของซอฟต์แวร์ ประมาณการต้นทุนในการพัฒนาระบบ กำหนดแนวทางของการพัฒนาระบบ กำหนดระยะเวลา เป็นต้น

2. การวิเคราะห์ความต้องการ (Analysis) เป็นขั้นตอนของการค้นหาความต้องการของระบบ และวิเคราะห์ความต้องการนั้น เพื่อให้เข้าใจภาพรวมและหน้าที่การทำงานของระบบ

3. การออกแบบ (Design) เป็นขั้นตอนการออกแบบส่วนประกอบต่างๆของซอฟแวร์ เพื่อให้ตรงกับความต้องการที่ได้วิเคราะห์มาแล้ว

4. การเขียนโปรแกรม (Development) เป็นขั้นตอนการสร้างระบบโดยการเขียนโปรแกรม ตามแนวทางการออกแบบจากขั้นตอนที่ผ่านมา

5. การทดสอบ (Testing) เป็นขั้นตอนการนำระบบที่ทำมาทดสอบการใช้งาน ว่าทำงานถูกต้องตามความต้องการที่ได้หรือไม่ ซึ่งการทดสอบนี้จะรวมถึงการทดสอบการเชื่อมโยงกับระบบซอฟแวร์อื่นๆที่เกี่ยวข้องด้วย

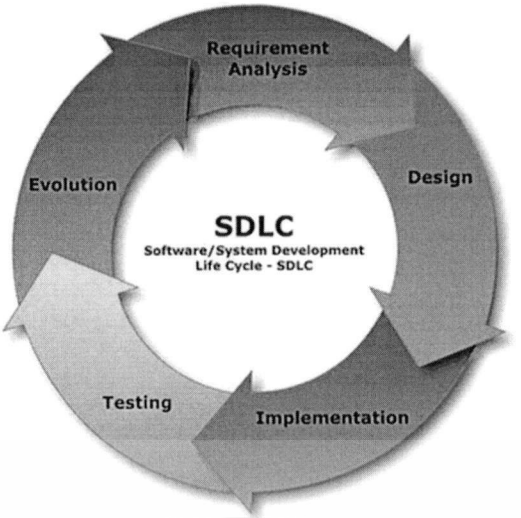
6. การประเมิน เป็นขั้นตอนการประเมินว่าระบบที่ผ่านการทดสอบแล้ว เหมาะสมที่จะนำไปใช้งานได้หรือไม่

7. การโอนย้ายข้อมูล (Data Conversion) เป็นขั้นตอนการนำข้อมูลเก่าเข้าระบบใหม่ก่อนการนำระบบไปใช้จริง

8. การนำไปใช้งานงานจริง (Production) เป็นขั้นตอนที่นำระบบที่พัฒนาสำเร็จและผ่านการทดสอบแล้วไปใช้งาน โดยทำการติดตั้ง และสอนวิธีการใช้งานแก่ผู้ใช้

9. การให้ความช่วยเหลือ (Support) เป็นขั้นตอนของการให้ความช่วยเหลือต่อผู้ใช้ เมื่อพบปัญหา โดยหากปัญหาที่เกิดไม่สามารถแก้ไขได้ จะต้องทำการพัฒนาระบบเพิ่มเติม ก็จะเริ่มวนไปที่ขั้นตอนแรกใหม่

ทั้งนี้วงจรในการพัฒนาระบบสามารถแสดงได้ดังรูปที่ 2.2



รูปที่ 2.2 SDLC (System Development Life Cycle)

ที่มา (http://th.wikipedia.org/wiki/SDLC)

2.1.4 การวิเคราะห์และออกแบบระบบเชิงออบเจ็ค

มีรายละเอียดดังต่อไปนี้

1. แนวความคิดพื้นฐานเชิงออบเจ็ค(Concept of Object-Oriented)

เป็นแนวความคิดในการการพิจารณาสิ่งใดสิ่งหนึ่งในโลกของความเป็นจริงเป็นออบเจ็ค ซึ่งออบเจ็คนี้สามารถจำลองได้ทั้งสิ่งที่จับต้องได้ เช่น บุคคล สิ่งของ และสิ่งที่จับต้องไม่ได้ เช่น รายการสินค้า โดยออบเจ็คหนึ่งๆ จะประกอบไปด้วยคุณสมบัติและพฤติกรรมของออบเจ็คนั้นๆ เมื่อออบเจ็คหลายๆ ออบเจ็คมาทำงานร่วมกัน มีการส่งข้อความหากันเพื่อสื่อสารในการทำงาน จะเกิดเป็นการทำงานของระบบ

โปรแกรมจะสามารถทำงานได้นั้นต้องเกิดจาก การที่ออบเจ็คมีความสัมพันธ์กันและมีการกระทำที่เกิดขึ้นระหว่างออบเจ็คสองตัวขึ้นไปและสามารถสังเกตเห็นได้ เช่น การสร้าง การลบ การเปลี่ยนแปลง เป็นต้น (Oestereich, B. 2002)

2. การสร้างแบบจำลองด้วยยูเอ็มแอล

ยูเอ็มแอล (UML: Unified Modeling Language) เป็นสัญลักษณ์อันเป็นหนึ่งเดียวกันที่ใช้อธิบาย แสดงรายละเอียด จำลองการสร้าง และจัดการกับเอกสารต่างๆ ในระบบการทำงานจริง เพื่อให้การออกแบบซอฟต์แวร์ที่แทนระบบการทำงานจริงนั้นทำได้โดยง่าย และปรับปรุงวิธีการทำงานที่มีอยู่เดิมให้ดียิ่งขึ้น ยูเอ็มแอลมักใช้เป็นการอธิบายและนำเสนอแนวความคิดของการเขียนโปรแกรมเชิงวัตถุ ก่อนนำไปเขียนโปรแกรมจริง (Oestereich, B. 2002)

แต่ละคนจะมีวิวของข้อมูลในฐานข้อมูลที่แตกต่างกันได้ ซึ่งวิวของข้อมูลนี้จะถูกดึงมาจาก Conceptual Schema

3. ระดับภายใน (Internal Level) เป็นระดับของการจัดเก็บฐานข้อมูลในหน่วยเก็บข้อ มูลสำรองจริงๆ เช่นข้อ มูลถูกเก็บอยู่ในตำแหน่งใดในดิสก์ รวมทั้งข้อมูลเกี่ยวกับ Index และ Pointer ก็จะถูกเก็บอยู่ในระดับนี้ทั้งหมด

2.2 เทคโนโลยีที่นำมาใช้ในการออกแบบและพัฒนาระบบ

มีทั้งหมด 8 รายการ ดังรายละเอียดดังนี้

2.2.1 เครื่องมือเคส

เครื่องมือเคส (Computer-Aided Software Engineering Tools หรือ CASE Tools) เป็นเครื่องมือที่ใช้ในการวิเคราะห์และออกแบบระบบ ซึ่งมีความสามารถหลัก ๆ คือ ช่วยนักวิเคราะห์ระบบ (systems analysts: SA) ในการวิเคราะห์และออกแบบระบบข้อมูล ข่าวสารต่าง ๆ โดยการใช้ซอฟต์แวร์ที่ช่วยสร้างแผนภาพ รายงาน โค้ดโปรแกรม ในระหว่างการวิเคราะห์และออกแบบระบบให้เป็นไปโดยอัตโนมัติ ซึ่งเป็นโปรแกรมประยุกต์หรือเป็นซอฟต์แวร์ชนิดหนึ่งของเทคโนโลยีสารสนเทศ ที่ช่วยในการพัฒนาระบบ คอยสนับสนุนการทำงานในแต่ละขั้นตอนของการพัฒนาด้วยการเตรียมฟังก์ชั่นการทำงานต่าง ๆ ที่ทำให้การทำงานแต่ละขั้นตอนมีความรวดเร็วและมีคุณภาพมากขึ้น

2.2.2 ดอตเน็ตเฟรมเวิร์ก

ดอตเน็ตเฟรมเวิร์ก(.NET Framework) คือแพลตฟอร์มสำหรับพัฒนาซอฟต์แวร์สร้างขึ้นโดยไมโครซอฟท์ โดยรองรับภาษาดอตเน็ตมากกว่า 40 ภาษาซึ่งมีไลบรารีเป็นจำนวนมากสำหรับการเขียนโปรแกรม รวมถึงบริหารการดำเนินการของโปรแกรมบนดอตเน็ตเฟรมเวิร์ก โดยไลบรารีนั้นได้รวมถึงส่วนต่อประสานกับผู้ใช้ การเชื่อมต่อฐานข้อมูล วิทยาการเข้ารหัสลับ อัลกอริทึม การเชื่อมต่อเครือข่ายคอมพิวเตอร์ และการพัฒนาเว็บแอปพลิเคชัน

2.2.3 เอเอสพีดอตเน็ต

เอเอสพีดอตเน็ต(ASP.NET) คือเทคโนโลยีสำหรับพัฒนาเว็บไซต์ เว็บแอปพลิเคชัน และเว็บเซอร์วิส ซึ่งเป็นส่วนหนึ่งของดอตเน็ตเฟรมเวิร์ก พัฒนาโดยไมโครซอฟท์

2.2.4 เว็บแอปพลิเคชั่น

โปรแกรมประยุกต์สำหรับเว็บ (Web Application) คือโปรแกรมประยุกต์ที่เข้าถึงด้วยโปรแกรมค้นดูเว็บผ่านเครือข่ายคอมพิวเตอร์อย่างอินเทอร์เน็ตหรืออินทราเน็ต เว็บแอพพลิเคชั่นเป็นที่นิยมเนื่องจากความสามารถในการอัปเดท และดูแล โดยไม่ต้องแจกจ่าย และติดตั้งซอฟต์แวร์บนเครื่องผู้ใช้ ตัวอย่างเว็บแอพพลิเคชั่นได้แก่ เว็บเมล การพาณิชย์อิเล็กทรอนิกส์ การประมูลออนไลน์ กระดานสนทนา บล็อก วิกิ เป็นต้น

2.2.5 ไมโครซอฟท์ วิชวล สตูดิโอ

ไมโครซอฟท์ วิชวลสตูดิโอ คือ Integrated Development Environment พัฒนาขึ้นโดยไมโครซอฟท์ ซึ่งเป็นเครื่องมือที่ช่วยนักพัฒนาซอฟต์แวร์พัฒนาโปรแกรมคอมพิวเตอร์ เว็บไซต์ เว็บแอปพลิเคชัน และ เว็บเซอร์วิส ระบบที่รองรับการทำงานนั้นมีไมโครซอฟท์ วินโดวส์ พ็อคเกตพีซี Smartphone และ เว็บเบราว์เซอร์ ในปัจจุบัน วิชวลสตูดิโอนั้นสามารถใช้ภาษาโปรแกรมที่เป็นภาษาดอตเน็ต ในโปรแกรมเดียวกัน เช่น VB.NET C++ C# J# เป็นต้น

2.2.6 เอสคิวแอลเซิฟเวอร์

SQL Server 2008 คือระบบจัดการฐานข้อมูลพัฒนาโดยไมโครซอฟท์ ซึ่งใช้ภาษา T-SQL ในการดึงเรียกข้อมูล

2.2.7 อินเทอร์เน็ต อินฟอร์เมชั่นเซิฟเวอร์

อินเทอร์เน็ต อินฟอร์เมชั่นเซิฟเวอร์ (Internet Information Service หรือ IIS) คือ เป็นโปรแกรมสำหรับการจำลองเครื่องของเราให้กลายเป็นเครื่องเว็บเซิร์ฟเวอร์ ซึ่งมีไว้ให้บริการด้าน Server ในรูปแบบต่างๆของ Internet เช่น Web server r , FTP Server , SMTP Server ฯลฯ ในระบบปฏิบัติการวินโดวส์ ถูกพัฒนาโดยบริษัทไมโครซอฟท์ ซึ่งในวินโดวส์เซิร์ฟเวอร์ 2003 นั้น เวอร์ชันของ IIS จะเป็นเวอร์ชัน 6.0 (IIS 6.0) ซึ่งทางไมโครซอฟต์ได้ทำการออกแบบโปรแกรมใหม่ทั้งหมด โดยเน้นในเรื่องความปลอดภัยเป็นพิเศษ เนื่องจากในเวอร์ชันก่อนหน้านั้นคือ IIS 5.0 ในวินโดวส์เซิร์ฟเวอร์ 2000 จะมีช่องโหว่ความปลอดภัยค่อนข้างมาก และที่สำคัญคือการมันจะถูกติดตั้งโดยดีฟอลท์พร้อมกับระบบปฏิบัติการ ซึ่งทำให้เกิดปัญหาด้านความปลอดภัยและเป็นช่องทางการระบาดของไวรัสต่างๆ เช่น Code Red และ Nimda ดังนั้น บนวินโดวส์เซิร์ฟเวอร์ 2003 นั้น IIS 6.0 จะไม่ทำการติดตั้งโดยดีฟอลท์พร้อมกับระบบปฏิบัติการแต่ผู้ใช้ต้องทำการติด ตั้งเองเมื่อต้องการใช้งาน และนอกจากนี้ IIS 6.0 ยังได้รับการพัฒนาให้มีประสิทธิภาพการทำงานที่ดีขึ้น ทำให้สามารถรองรับการใช้งานต่างๆ ได้ดียิ่งขึ้น และล่าสุดบริษัทไมโครซอฟท์ ได้ออกเวอร์ชั่นใหม่นั้นคือ IIS 7.0

2.2.8 คริสตอล รีพอร์ท

คริสตอล รีพอร์ท (Crystal Report) คือเครื่องมือที่ใช้ในการออกรายงาน ซึ่งสามารถ ออกรายงานได้หลากหลายรูปแบบ ทั้งแบบ รายงานธรรมดา แบบ Cross Tab และแบบอื่นๆ ซึ่งมีเครื่องไม้เครื่องมือที่ออกแบบมาให้ง่ายต่อการใช้งาน และการติดต่อกับฐานข้อมูลก็สามารถทำได้หลากหลาย เช่น MS SQL Server,Access,Excel,XML,ADO.Net, ตลอดจนสามารถนำข้อมูลจาก Viewer ของเครื่องมาดูก็สามารถทำได้ ซึ่งให้ความสามารถที่หลากหลาย และการ View ก็สามารถ View ได้หลากหลาย เช่น การ View ผ่านตัวโปรแกรมเอง, การ View ผ่านโปรแกรมที่เป็นโปรแกรมประยุกต์ที่ Software House ต่างๆผลิตขึ้นมา หรือแม้กระทั้ง ดูบนเว็บ ซึ่งจากความสามารถที่หลากหลายดังกล่าวจึงเป็นที่นิยมใช้งานในเชิงพาณิชย์กัน

บทที่ 3
การศึกษาและวิเคราะห์ระบบงานปัจจุบัน

ก่อนทำการออกแบบระบบงานใหม่ จะต้องมีการศึกษาและวิเคราะห์ระบบงานเดิมที่ดำเนินการอยู่ในปัจจุบันก่อน เพื่อสร้างความเข้าใจเกี่ยวกับลักษณะทั่วไปของศูนย์บริหารข้อมูลภาครัฐ กระบวนการทำงานระบบงานและปัญหาที่เกิดจากระบบงานเดิม มีการประเมินเหตุการณ์ต่างๆ เพื่อหาทางเลือกที่เหมาะสมมาแก้ปัญหา โดยมีรายละเอียดดังนี้

3.1 ภาพรวมขององค์กร

3.2 การบริหารงานแผนกเทคโนโลยีสารสนเทศ

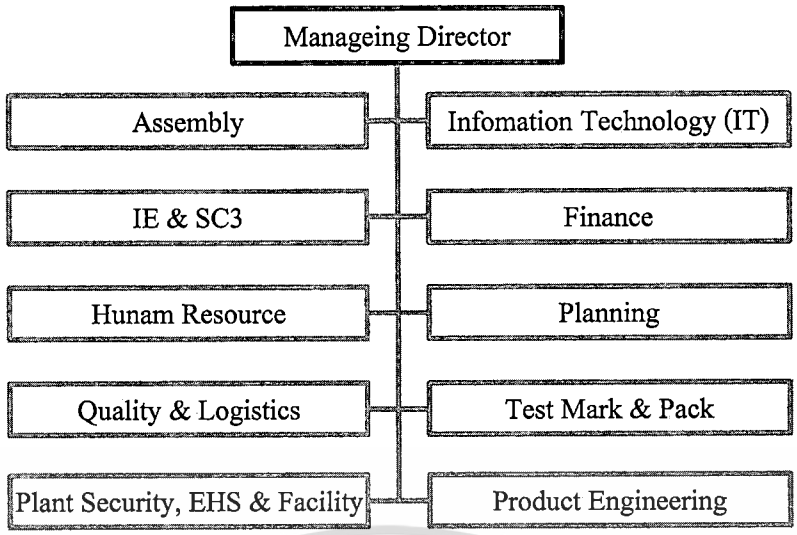
3.3 การดำเนินงานในปัจจุบัน

3.4 ปัญหาของระบบงานปัจุบัน

3.1 ภาพรวมขององค์กร

บริษัท สแปนชั่น (ไทยแลนด์) จำกัดเป็นผู้นำในอุตสาหกรรม NOR หน่วยความจำแฟลช ได้พัฒนาผลิตภัณฑ์เพื่อตอบสนองความต้องการของมนุษย์, สิ่งแวดล้อมและสังคม ในด้านเทคโนโลยี และนวัตกรรมที่ทันสมัยมาเป็นเวลาเกือบสิบปี แสปนชั่น(ไทยแลนด์) ก่อตั้งขึ้นในปี พ.ศ. 2546 และจดทะเบียนในตลาดหลักทรัพย์นิวยอร์กในปี พ.ศ. 2553 ดำเนินธุรกิจภายใต้หลักการที่ว่า "ลูกค้าต้องมาก่อน"

ตั้งอยู่ เลขที่ 229 หมู่ 4 ถนนแจ้งวัฒนะ อ.ปากเกร็ด จ. นนทบุรี บริษัท แสปนชั่น (ไทยแลนด์) เป็นบริษัทที่มี สิ่งอำนวยความสะดวกการผลิตมวลและโรงงานหน่วยความจำเพียง NOR flash ในประเทศไทย บริษัท ปัจจุบันมีพนักงานประมาณ 1000 บุคลากร ในปี พ.ศ. 2555 แผนการผลิตออกมาถึงปริมาณสูงทุกเวลาจาก 9 ล้านหน่วยต่อสัปดาห์ ภาพรวมโครงสร้างขององค์กร ดังรูปที่ 3.1



รูปที่ 3.1 ภาพรวมโครงสร้างขององค์กร
ที่มา บริษัท สแปนชั่น (ไทยแลนด์) จำกัด

3.2 การบริหารงานแผนกเทคโนโลยีสารสนเทศ

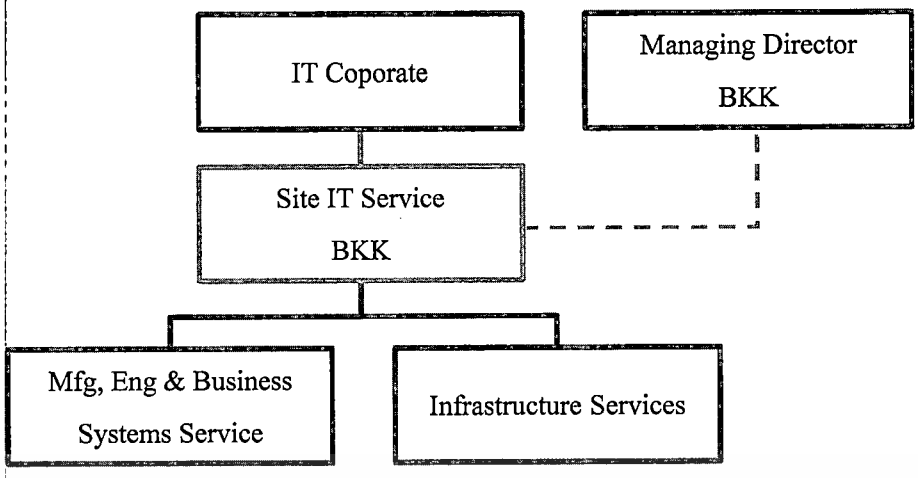
การบริหารจัดการงานแผนกเทคโนโลยีสารสนเทศ ประสานงานโดยตรงกับแผนกเทคโนโลยีของสาขาใหญ่ของบริษัทฯ ที่ประเทศ สหรัฐอเมริกา และอยู่ภายใต้การบริหารจัดการของบริษัท สแปนชั่น (ไทยแลนด์) จำกัด แบ่งสายการปฏิบัติงานเป็น 2 ส่วนใหญ่ๆ คือ

3.2.1 Mfg, Eng & Business Systems Service

ดูแลรับผิดชอบเกี่ยวกับ Application ต่างๆ เพื่อสนับสนุนฝ่ายผลิต และธุรกิจขององค์กร (Manufacting/Business Applications)

3.2.2 Infrastructure Services

ดูแลรับผิดชอบเกี่ยวกับ Networking/Telecom, Server (Windows, Unix). DATABASE, Client, Desktop, VDO Conference ซึ่งสามารถแสดงได้ดังรูปที่ 3.2



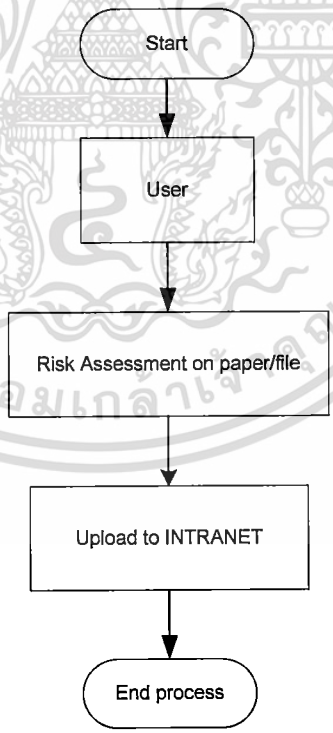
รูปที่ 3.2 การบริหารจัดการแผนกเทคโนโลยีสารสนเทศ
ที่มา บริษัท สแปนชั่น (ไทยแลนด์) จำกัด

3.3 การดำเนินงานในปัจจุบัน

การดำเนินงานในปัจจุบัน ทางองค์กรอ้างอิงจาก Spec ดังต่อไปนี้

3.3.1 708-099.1, Business Continuity Management

เป็นแผนหลัก และมีการประเมินความเสี่ยงในแต่ละแผนกดัง รูปที่ 3.3 และ ตารางที่ 3.1



รูปที่ 3.3 การประเมินความเสี่ยงขององค์กร
ที่มา บริษัท สแปนชั่น (ไทยแลนด์) จำกัด

ตารางที่ 3.1 Spansion Risk Assessment

Hazard Vulnerability Analysis Chart

Location/Facility: Spansion (Thailand)
Date Completed: 17 May 07
Completed by: BCP Team

Type of Hazard	Historical Occurrence	Prob. of Occurrence	Human Impact	Property Impact	Business Impact	Mitigation Activities	Internal Resources	External Resources	Total
Electrical Supply	2	1	1	1	5	3	3	2	1.8
Water Supply System	1	1	1	1	3	3	3	2	0.9
Chillers	1	1	1	1	3	3	3	2	0.9
CDA	1	1	1	1	4	3	3	2	1.1
Air Condition	1	1	1	1	4	3	3	2	1.1
RO/DI System	1	1	1	1	4	3	3	2	1.1
Cold Room Refrigerator	1	1	1	1	4	3	3	3	1.0
Nitrogen Storage Tank	1	2	1	1	3	3	3	3	1.2
Fire Pump not Work	1	1	1	1	1	4	4	3	0.1
Boiler Shut Down	1	1	1	1	3	3	3	3	0.8
Fire	1	2	5	5	5	4	4	2	3.3
Flood	1	1	2	3	3	4	4	1	1.4
Chemical Spill	1	2	2	2	3	3	3	2	1.8
Gas Leak	1	1	1	1	3	4	3	2	0.8
Bomb	1	1	5	5	5	3	3	2	3.1
Key Manufacturing Down	1	1	1	1	3	3	3	1	1.0
Labor Shortage/Strike	1	1	1	1	4	4	4	2	0.9
Material Shortage	2	2	1	1	4	3	2	2	1.9
Subcon Shut Down	1	1	1	1	3	3	3	1	1.0
Transportation Problem	1	1	1	1	3	3	2	2	1.0
IT Disster	1	2	1	1	4	3	3	2	1.8
Outbreak	1	1	4	1	4	3	3	1	1.9
Waste Water Treatment	1	1	1	1	3	3	3	2	0.9
Coup	5	1	1	1	1	1	1	1	1.9
Earthquake	1	2	4	4	4	2	2	2	3.1

Summary: This tool looks at an organization's or a community's vulnerability to the effects of various hazards. Using a scale of 1 to 5, the probability of occurrence and the impact potential are measured against mitigation activities and the resources available to respond to the hazard. The total is based on a formula that weighs risk heavily but provides credit for mitigation and response and recovery resources. The highest score possible is 5.0. The lower the total score, the lower the overall risk from the Hazard.

Instructions:

Score each hazard based on a scale of 0 to 5 with 5 being the highest.

Add or delete hazards as required based on your analysis.

Historical Occurrence: Based on number of occurrence in the last 20 years. Maximum is 5; if a new hazard use 0.

Probability: Score 1 if less than 1%, 2 if less than 5%, 3 if less than 10%, 4 if less than 20%, and 5 if greater than 20%.

Impact: Based on "worst-case scenario" - greatest possible impact should worst-case event occur.

Final Step: Sort the Total Column in descending order once scoring is completed.

Analysis Results:

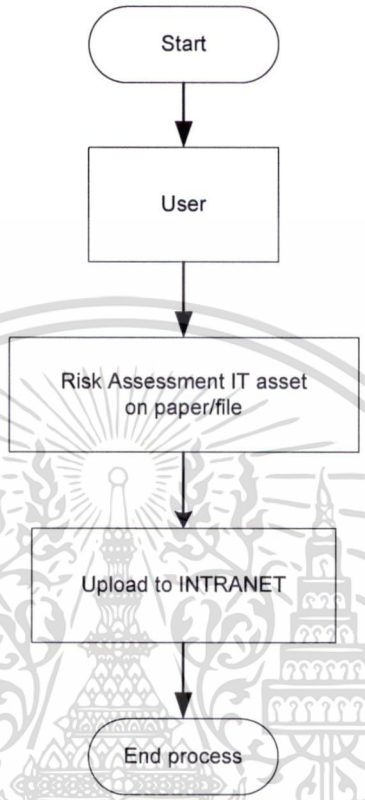
High Risk: Greater than 3.6

Medium Risk: 2.0 to 3.6

Low Risk: Less than 2

3.3.2 708-099.2, Bkk IT Infrastructure Disaster Readiness Plan (DRP)

เป็นแผนกู้คืนระบบ และมีการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ ดังรูปที่ 3.4 และตารางที่ 3.2



รูปที่ 3.4 การประเมินความเสี่ยงของระบบสารสนเทศ

ที่มา บริษัท สแปนชั่น (ไทยแลนด์) จำกัด

ตารางที่ 3.2 Spansion Information System Risk Assessment

Location: Spansion (Thailand)

Data Completed: 30 SEP'08

Completed by: BKK Team

Application and System Analysis Application	Historical Occurrence	Prob.of Occurrence	Human Impact	Property Impact	Business Impact	Mitifation Activites	Internal Resources	External Resources	Total
CAMSTAR(BKK)	0	1	0	0	5	4	4	3	0.3
XSITE (BKK)	1	1	0	0	3	3	4	2	0.3
Wafer map (BKK)	2	1	0	0	3	3	2	2	0.8
SPCA (BKK)	1	1	0	0	2	4	3	2	0.1
HR/Payroll (BKK)	1	1	3	0	1	2	1	2	0.7
Attendance System (BKK)	1	1	0	0	1	3	1	5	0.1
ATEX (US)	1	2	0	0	2	3	1	3	0.8
SAP FICO (US)	1	2	0	0	5	4	1	3	1.1
SAP P2P (US)	1	2	0	0	5	4	1	5	1.1
SAP PD (US)	1	2	0	0	5	4	1	5	1.1
Data Backup System (BKK)	1	1	0	0	4	3	3	2	0.7
Network (LAN/WAN/MPLS/ Internet) (BKK)	1	2	0	0	5	3	3	2	1.3
Network Security	1	1	0	0	4	3	3	2	0.7

3.4 ปัญหาของการทำงาน

ตารางที่ 3.3 สรุปประเด็นปัญหา แนวทางแก้ไขและสิ่งที่ได้ดำเนินการ

ปัญหา	แนวทางแก้ไข	สิ่งที่ได้ดำเนินการ
ข้อมูลถูกบันทึกไว้ในรูปแบบเอกสารกระดาษและระบบไฟล์ ทำให้ 1. ไม่สะดวกในการประเมินความเสี่ยงของระบบสารสนเทศในแต่ละครั้ง 2. เมื่อมีอุปกรณ์มาใหม่ ในแต่ละครั้ง ไม่ได้รับการปรับปรุง รายการของความเสี่ยง ภัยคุกคาม หรือช่องโหว่ ของทรัพย์สิน ให้เป็นปัจจุบัน 3. ไม่สะดวกในการวางแผนบรรเทาความเสี่ยง	ออกแบบและสร้างระบบสารสนเทศเชิงวัตถุเพื่อสนับสนุนการบันทึกข้อมูลในการทำงานในรูปแบบเว็บแอพพลิเคชั่นร่วมกับฐานข้อมูลเชิงสัมพันธ์ ได้แก่ 1. บันทึกข้อมูลการประเมินความเสี่ยง (หัวข้อที่ 4.5.1 หน้าที่ 31) 2. บันทึกข้อมูล ภัยคุกคาม จุดอ่อน หรือช่องโหว่ (หัวข้อที่ 4.5.1 หน้าที่ 33, 35) 3.บันทึกข้อมูล แผนบรรเทาความเสี่ยง (หัวข้อที่ 4.5.1 หน้าที่ 37)	1. การออกแบบและพัฒนาระบบเชิงวัตถุ 2. เว็บแอพพลิเคชั่นบนเทคโนโลยี ASP.NET 4.0 3. การออกแบบฐานข้อมูลเชิงสัมพันธ์
ใช้เวลานาน เมื่อผู้บริหาร ต้องการมีข้อมูล เพื่อช่วยในการ วิเคราะห์บริหารจัดการความเสี่ยง และวางแผนสร้างความมั่นคง และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	ออกแบบและสร้างระบบสารสนเทศเชิงวัตถุเพื่อสนับสนุนการบันทึกข้อมูลในการทำงานในรูปแบบเว็บแอพพลิเคชั่นร่วมกับฐานข้อมูลเชิงสัมพันธ์ ได้แก่ 1. แสดงรายงานการประเมินความเสี่ยง (หัวข้อที่ 4.5.1 หน้าที่ 49)	1. การออกแบบและพัฒนาระบบเชิงวัตถุ 2. เว็บแอพพลิเคชั่นบนเทคโนโลยี ASP.NET 4.0 3. การออกแบบฐานข้อมูลเชิงสัมพันธ์

บทที่ 4
การวิเคราะห์และออกแบบระบบงานใหม่

ระบบบริหารจัดการความเสี่ยง โดยมีรายละเอียดดังต่อไปนี้

4.1 การศึกษาความเป็นไปได้ในการพัฒนาระบบ

4.2 ความต้องการของระบบใหม่

4.3 การออกแบบระบบใหม่

4.4 สถาปัตยกรรมของระบบ

4.5 การออกแบบระบบด้วยยูเอ็มแอล

4.6 การออกแบบฐานข้อมูล

4.1 การศึกษาความเป็นไปได้ในการพัฒนาระบบ

จากการวิเคราะห์การทำงานของระบบปัจจุบัน จึงได้ทำการศึกษาความเป็นไปได้ในการพัฒนาระบบงานใหม่ใน 3 ด้าน คือ

1. ความเป็นไปได้ทางด้านเทคนิค

สามารถดำเนินการได้ในทางเทคนิค ซึ่งใช้เทคโนโลยีที่ มีใช้งานในองค์กร อยู่แล้ว

2. ความเป็นไปได้ทางด้านเศรษฐศาสตร์

สามารถดำเนินการได้ เนื่องจาก เป็นการปรับปรุงการทำงานให้มีประสิทธิภาพมากขึ้น

3. ความเป็นไปได้ทางด้านการดำเนินการขององค์กร

สามารถดำเนินการได้เนื่องจาก ตอบสนองนโยบาย ของทางองค์กร

4.2 ความต้องการของระบบใหม่

การวิเคราะห์และออกแบบระบบบริหารจัดการความเสี่ยง เพื่อเทคโนโนโลยีสารสนเทศ มีขอบเขตในการจัดทำดังต่อไปนี้

4.2.1 ความต้องการเชิงหน้าที่การทำงาน (Functional Requirement)

1) ระบบสามารถบันทึก ปรับปรุง แก้ไข และออกรายงาน ข้อมูลการประเมินความเสี่ยง (Risk Assessment) เช่น ข้อมูลทรัพย์สิน, ข้อมูลภัยคุกคาม, ข้อมูลจุดอ่อน, การควบคุม, โอกาสความเป็นไปได้ของภัยคุกคามของทรัพย์สินนี้, ผลกระทบทางธุรกิจถ้าทรัพย์สินนี้เสียหาย เป็นต้น

2) ระบบสามารถแสดงคำนวณและแสดงแผนผังการประเมินความเสี่ยง (Risk Matrix)

3) ระบบสามารถบันทึก ปรับปรุง แก้ไข และออกรายงาน แผนการบรรเทาความเสี่ยง (Risk Mitigation)

4) ระบบสามารถแสดงและออกรายงานการบริหารจัดการความเสี่ยงในรูปแบบต่างๆ ให้ผู้บริหาร หรือผู้ดูแลระบบ สามารถนำไปใช้งานได้

4.2.2 ความต้องการที่ไม่ใช่เชิงหน้าที่การทำงาน (Non-Functional Requirement)

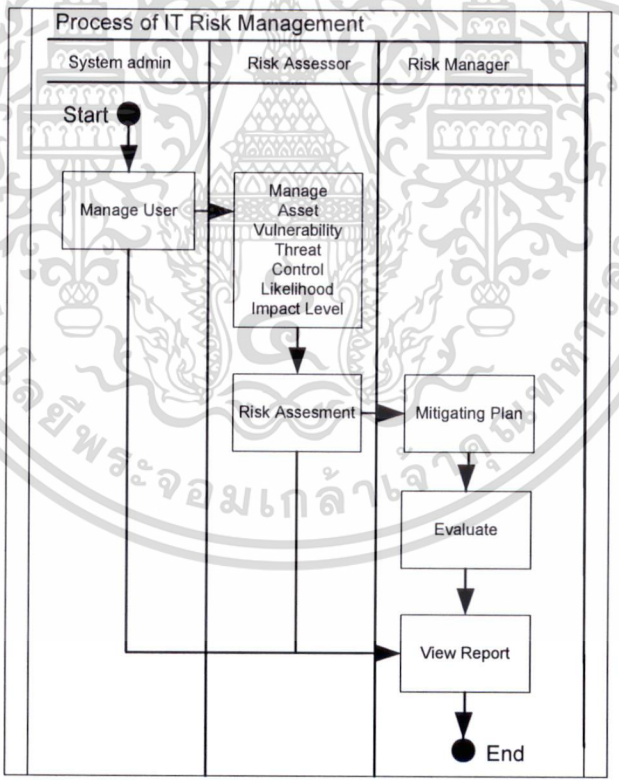
1) มีการตรวจสอบสิทธิ์ในการใช้งานก่อนเข้าสู่ระบบ

2) ระบบมีข้อมูลนโยบายการบริหารความเสี่ยงขององค์กร

3) ระบบมีข้อมูลแสดงเกี่ยวกับการบริหารความเสี่ยงตามมาตราฐาน NIST 800-30

4.3 การออกแบบระบบใหม่

จากการวิเคราะห์ปัญหาและข้อจำกัดของระบบงานในปัจจุบันพบว่า ยังอยู่ในรูปแบบกระดาษ การรูปแบบไฟล์ และ เก็บอยู่ในอินทราเน็ต ขององค์กร ซึ่งไม่สะดวกในการ ปฏิบัติงาน จึงวางแผนปรับขบวนการ ดังรูปที่ 4.1



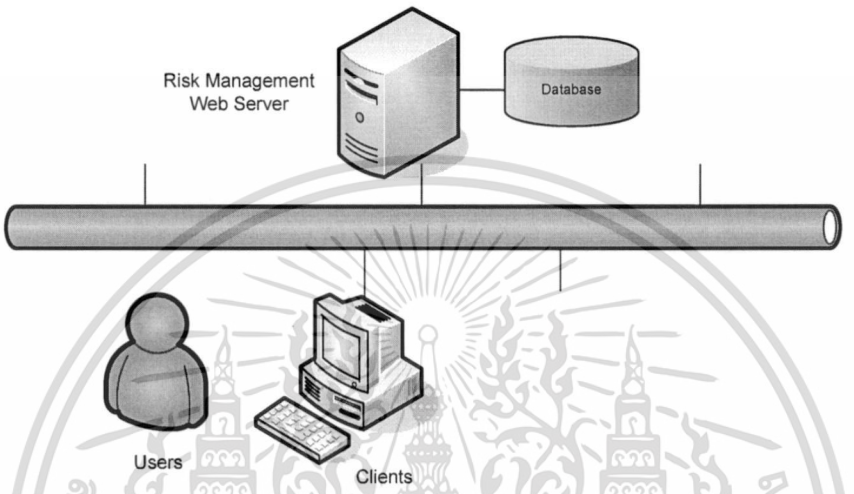
รูปที่ 4.1 Risk Management Process

4.4 สถาปัตยกรรมของระบบ

แบ่งเป็น 2 ส่วน ได้แก่ การเชื่อมต่อเครือข่ายและคุณสมบัติของอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์

4.4.1 การเชื่อมต่อเครือข่าย

การออกแบบและพัฒนาระบบบริหารความเสี่ยง ดังรูปที่ 4.2



รูปที่ 4.2 การเชื่อมต่อระบบเครือข่าย และฐานข้อมูล

4.4.2 คุณสมบัติของอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์

ในการใช้งานระบบบริหารความเสี่ยง อุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ ควรมีคุณสมบัติขั้นต่ำดังต่อไปนี้

คุณสมบัติของฮาร์ดแวร์

- หน่วยประมวลผลกลาง ไม่ต่ำกว่า 2GHz
- หน่วยความจำไม่ต่ำกว่า 1 GB
- พื้นที่ว่างในฮาร์ดดิสก์ 10 GB

คุณสมบัติของซอฟต์แวร์

- ระบบปฏิบัติการ Microsoft Window XP ขึ้นไป
- โปรแกรมเว็บบราวเซอร์

4.5 การออกแบบระบบด้วยยูเอ็มแอล

การสร้างยูสเคสไดอะแกรมของระบบงานใหม่เพื่อแสดงขอบเขตการทำงานของระบบที่ผู้ใช้งานสามารถทำได้ในระบบ

ระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง

4.5.1 Use case Diagram

การสร้างยูสเคสไดอะแกรมของระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง เพื่อแสดงขอบเขตการทำงานของระบบที่ผู้ใช้งานสามารถทำได้ในระบบ ประกอบด้วยแอกเตอร์และยุสเคส ดังนี้

แอกเตอร์ คือ ผู้ที่ใช้งานยูสเคส หรือผู้ที่กระทำกับยูสเคส มีทั้งหมด 3 แอกเตอร์ ดังนี้

1. System Administrator คือ ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการการใช้งานของผู้ใช้งานระบบ

2. Risk Assessor คือ ผู้วิเคราะห์ความเสี่ยง มีหน้าที่ในการบริหารจัดการข้อมูลที่ใช้ในการประเมินความเสี่ยงต่างๆ รวมถึงทำหน้าที่ประเมินความเสี่ยง เช่น ผู้ดูแลระบบเครือข่าย ผู้ดูแลเซอร์เวอร์ ผู้ดูแลแอพพลิเคชั่น เป็นต้น

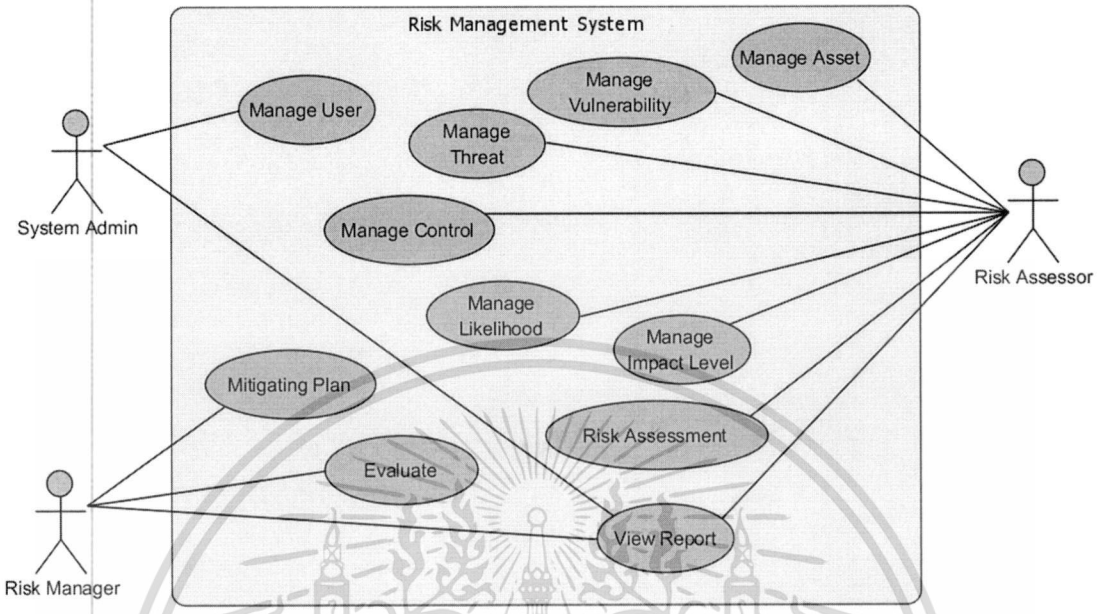
3. Risk Manager คือ ผู้บริหารจัดการความเสี่ยงของหน่วยงาน มีหน้าที่ควบคุมและจัดทำแผนบรรเทาความเสี่ยงภายในองค์กร เช่น IT Manager

ยูสเคส คือ ฟังก์ชันที่ระบบจะต้องสามารถทำงานได้ ซึ่งในระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง

ประกอบด้วย 11 ยูสเคสดังต่อไปนี้

1. Manage User เป็นสร้างและปรับปรุงข้อมูลผู้ใช้งานระบบ
2. Manage Asset เป็นสร้างและปรับปรุงข้อมูลสินทรัพย์ที่มีอยู่
3. Manage Vulnerability เป็นการสร้างและแก้ไขข้อมูลจุดอ่อน
4. Manage Threat เป็นการสร้างและแก้ไขข้อมูลภัยคุกคาม
5. Manage Control เป็นการสร้างและแก้ไขตัวควมคุมหรือมาตรฐานที่ใช้
6. Manage Likelihood เป็นการสร้างและแก้ไขข้อมูลความน่าจะเป็น
7. Manage Impact Level เป็นการสร้างและแก้ไขข้อมูลระดับผลกระทบด้านต่างๆ
8. Risk Assignment เป็นการนำข้อมูลที่มีอยู่ในระบบมาวิเคราะห์ความเสี่ยง
9. Mitigating Plan เป็นการจัดทำและปรับปรุงแผนบรรเทาความเสี่ยงที่จะเกิดขึ้น
10. Evaluate เป็นการศึกษาข้อมูลความเสี่ยงต่างๆ ของผู้จัดการบริหารความเสี่ยง
11. View Report เป็นการดูรายงานทั้งหมดภายในระบบ

จากแอกเตอร์และยูสเคสที่มีอยู่ในระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง สามารถแสดงเป็นยูสเคสไดอะแกรมได้ดังรูปที่ 4.3

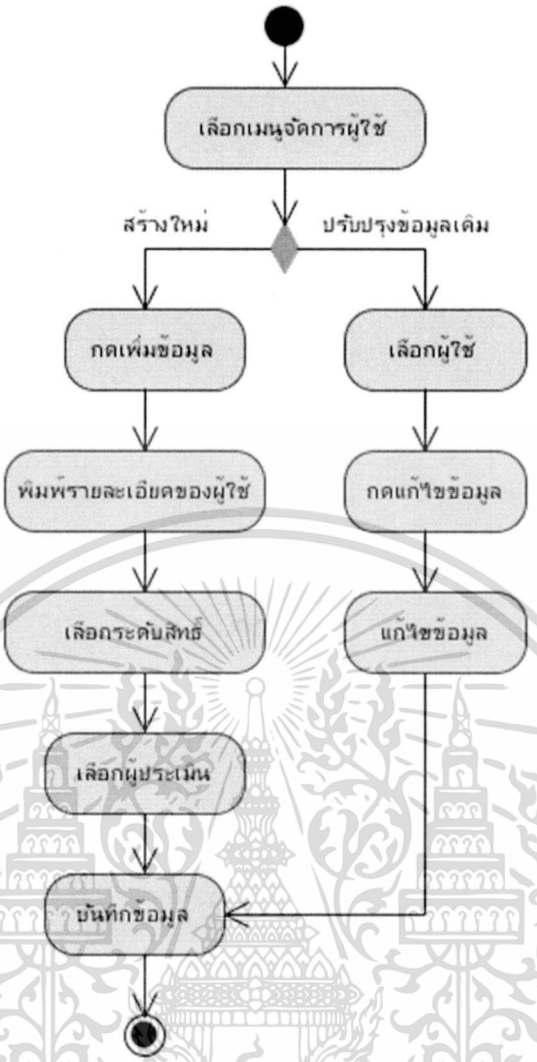


รูปที่ 4.3 ยูสเคสไดอะแกรมระบบบริหารความเสี่ยง

จากรูปยูสเคสไดอะแกรมสามารถเขียนอธิบายรายละเอียดแต่ละยูสเคส ได้ดังตารางที่ 4.1 ถึง 4.13 และจากเขียนเป็นแอกทิวิตีไดอะแกรม เพื่ออธิบายรายละเอียดแต่ละยูสเคส ได้ดังรูปที่ 4.4 ถึง 4.14 ตามลำดับ

ตารางที่ 4.1 รายละเอียดยูสเคส Manage User

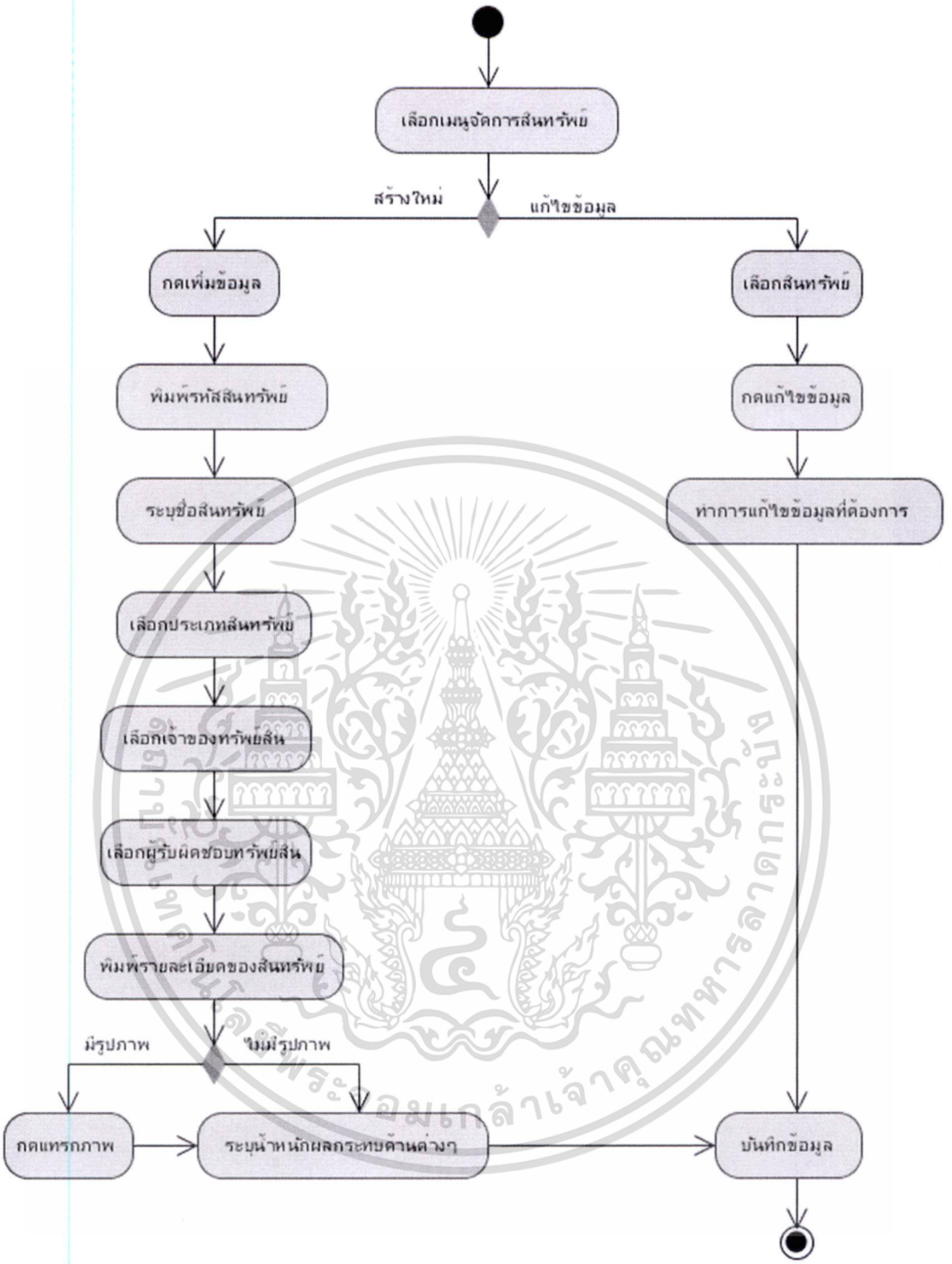
ชื่อยูสเคส	Manage User
รายละเอียดโดยสังเขป	ผู้ดูแลระบบสร้างข้อมูลของผู้ใช้และปรับปรุงข้อมูลอยู่เสมอ
แอกเตอร์	ผู้ดูแลระบบ
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูจัดการผู้ใช้ 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 พิมพ์รายละเอียดเกี่ยวกับผู้ใช้งานระบบ 2a.3 เลือกระดับสิทธิ์ เลือกผู้ประเมิน 2b.1 เลือกผู้ใช้งาน 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูลของผู้ใช้งาน
เงื่อนไขภายหลัง	-



รูปที่ 4.4 แอ็กทิวิตี้ไดอะแกรมอธิบายยูสเคส Manage User

ตารางที่ 4.2 รายละเอียดยูสเคส Manage Asset

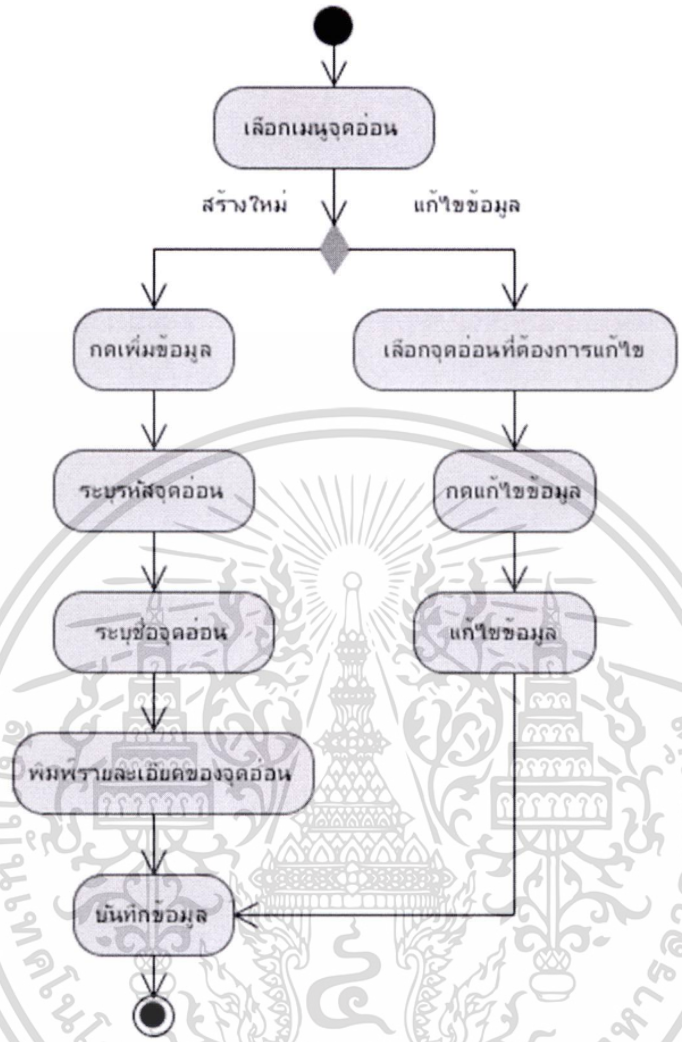
ชื่อยูสเคส	Manage Asset
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยงบันทึกข้อมูลสินทรัพย์ภายในองค์กร พร้อมระบุน้ำหนักผลกระทบด้านต่างๆ และปรับปรุงข้อมูลให้ถูกต้อง
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูจัดการสินทรัพย์ 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 พิมพ์รายละเอียดเกี่ยวกับสินทรัพย์ 2a.3 เลือกประเภทเจ้าของ 2a.4 ผู้รับผิดชอบของสินทรัพย์ 2a.5 หากมีภาพให้ทำการแทรกรูปภาพของสินทรัพย์ 2a.6 ระบุน้ำหนักผลกระทบด้านต่างๆ 2b.1 เลือกสินทรัพย์ที่ต้องการ 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.5 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Manage Asset

ตารางที่ 4.3 รายละเอียดยูสเคส Manage Vulnerability

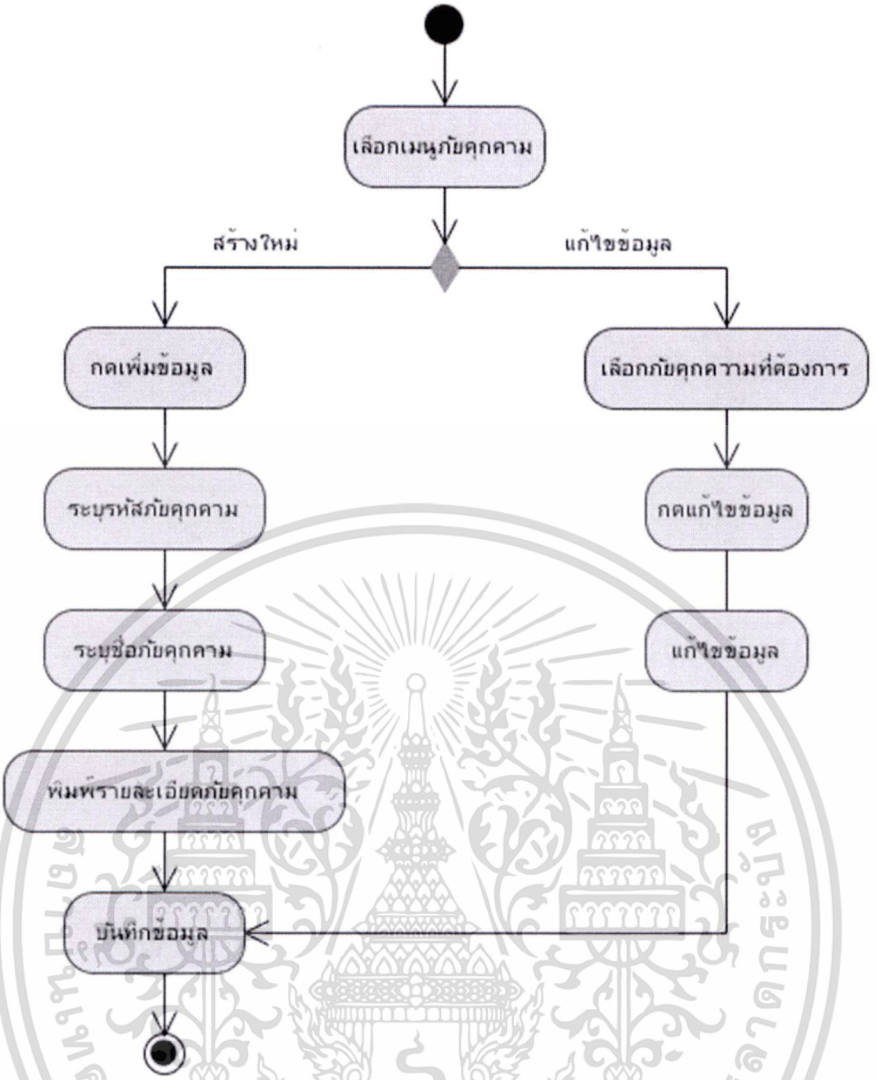
ชื่อยูสเคส	Manage Vulnerability
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยง สร้างข้อมูลเกี่ยวกับจุดอ่อนและปรับปรุงข้อมูลของจุดอ่อน
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูจุดอ่อน 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 ระบุรหัสและชื่อของจุดอ่อน 2a.3 พิมพ์รายละเอียดของจุดอ่อน 2b.1 เลือกจุดอ่อนที่ต้องการ 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.6 แอ็กทิวิตี้ไดอะแกรมอธิบายยูสเคส Manage Vulnerability

ตารางที่ 4.4 รายละเอียดยูสเคส Manage Threat

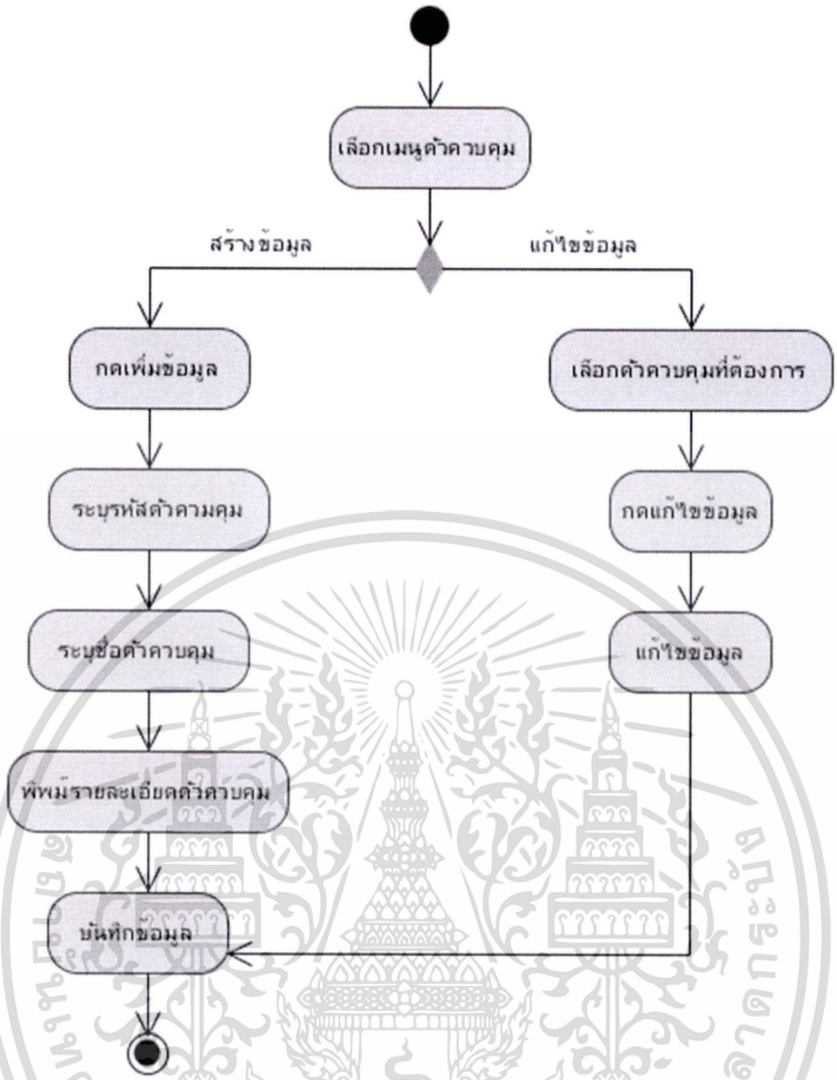
ชื่อยูสเคส	Manage Threat
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยง สร้างข้อมูลภัยคุกคามลงในระบบ และปรับปรุงข้อมูล
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูภัยคุกคาม 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 ระบุรหัสและชื่อของภัยคุกคาม 2a.3 พิมพ์รายละเอียดของภัยคุกคาม 2b.1 เลือกภัยคุกคามที่ต้องการ 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.7 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Manage Threat

ตารางที่ 4.5 รายละเอียดยูสเคส Manage Control

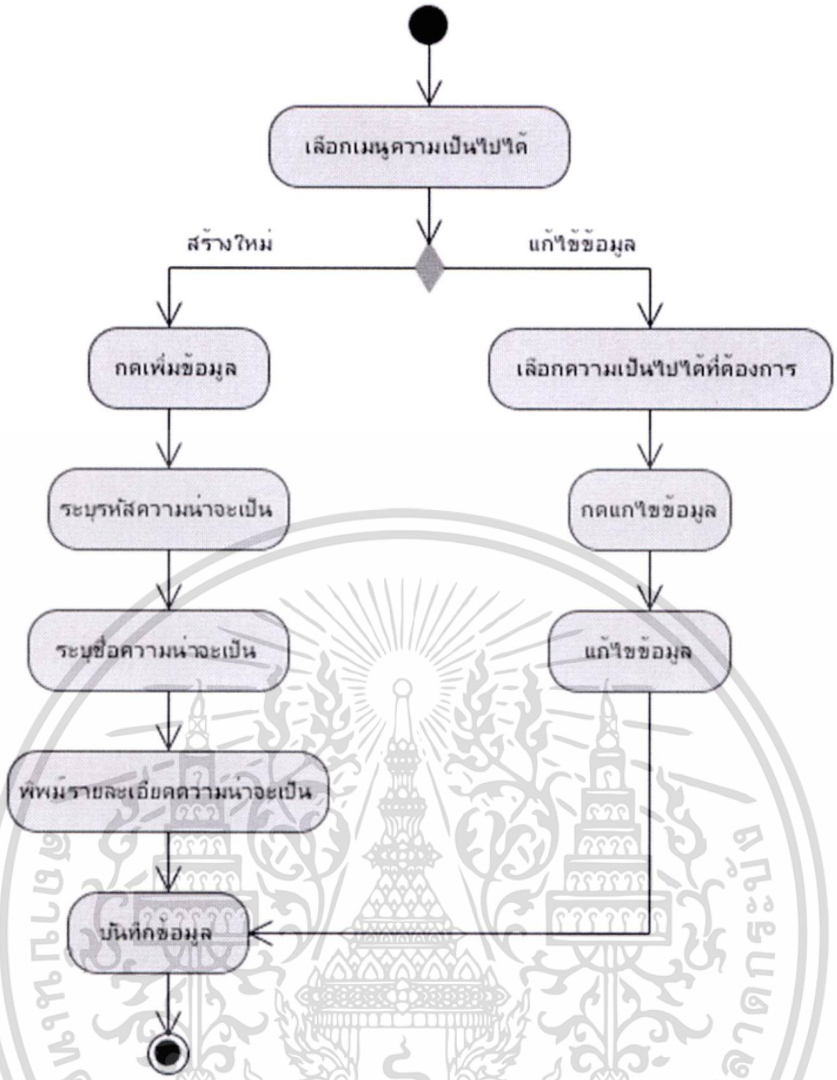
ชื่อยูสเคส	Manage Control
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยง สร้างข้อมูลตัวควบคุมลงในระบบ และปรับปรุงข้อมูลให้ถูกต้อง
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูตัวควบคุม 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 ระบุรหัสและชื่อของตัวควบคุม 2a.3 พิมพ์รายละเอียดของตัวควบคุม 2b.1 เลือกตัวควบคุมที่ต้องการ 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.8 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Manage Control

ตารางที่ 4.6 รายละเอียดยูสเคส Manage Likelihood

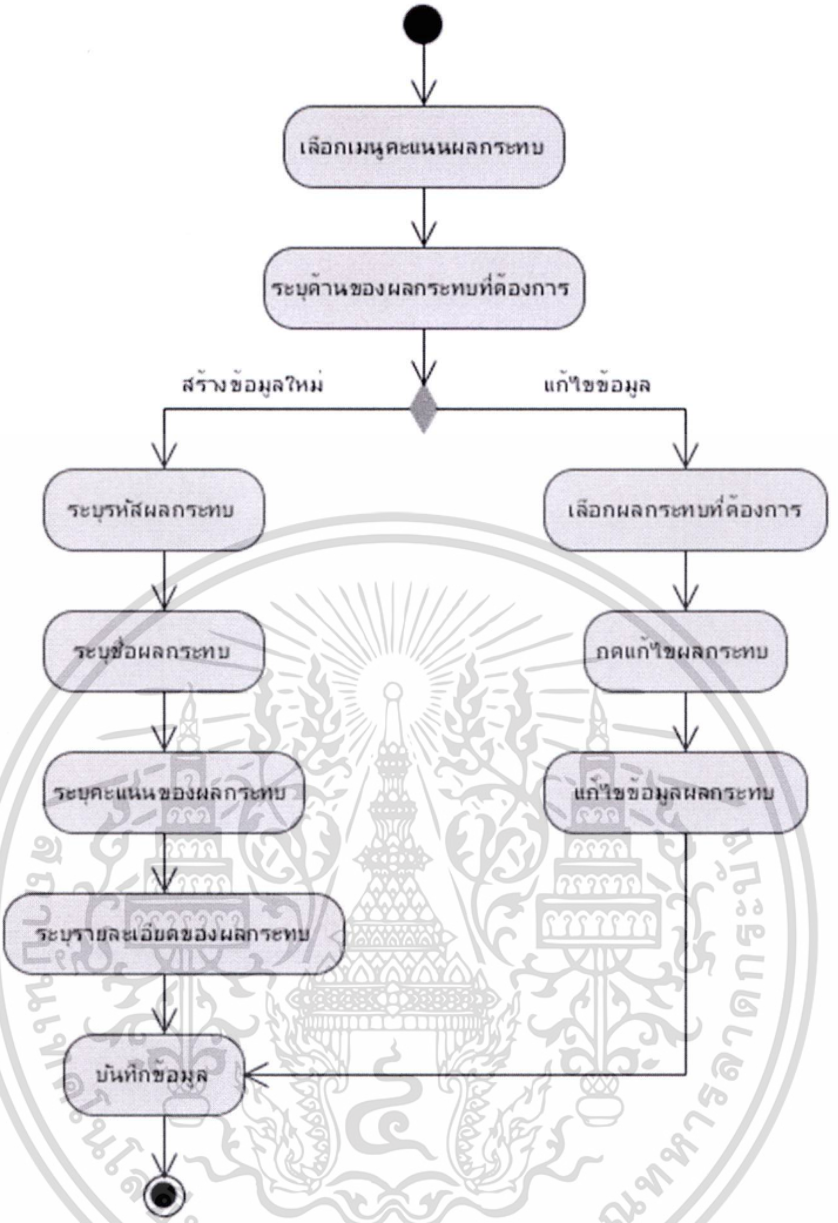
ชื่อยูสเคส	Manage Likelihood
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยง สร้างข้อมูลความเป็นไปได้ลงในระบบ และปรับปรุงข้อมูลให้ถูกต้อง
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูความเป็นไปได้ 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 ระบุรหัสและชื่อของความน่าจะเป็น 2a.3 พิมพ์รายละเอียดของความน่าจะเป็น 2b.1 เลือกความน่าจะเป็นที่ต้องการ 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.9 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Manage Likelihood

ตารางที่ 4.7 รายละเอียดยูสเคส Manage Impact Level

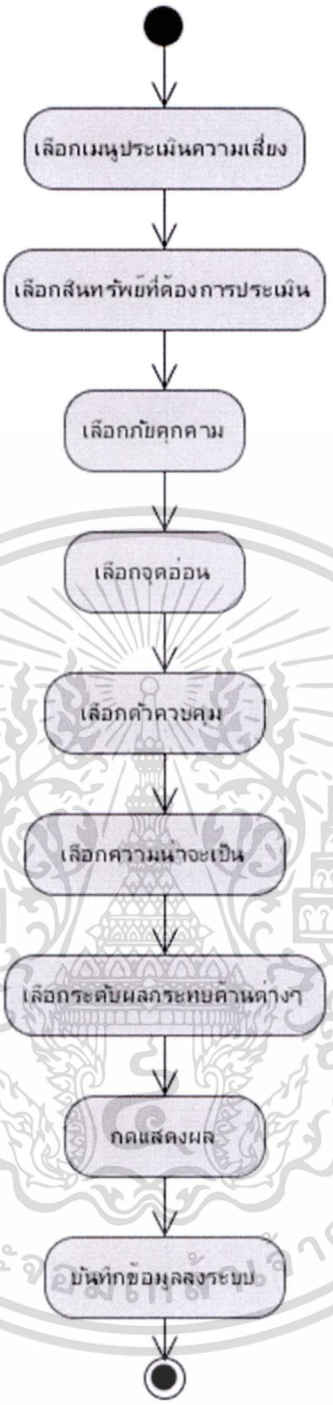
ชื่อยูสเคส	Manage Impact Level
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยง สร้างข้อมูลคะแนนผลกระทบลงในระบบ และปรับปรุงข้อมูลให้ถูกต้อง
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูคะแนนผลกระทบ 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 ระบุรหัสและชื่อของคะแนนผลกระทบ 2a.3 ระบุคะแนนของผลกระทบ 2a.4 พิมพ์รายละเอียดของคะแนนผลกระทบ 2b.1 เลือกคะแนนผลกระทบที่ต้องการ 2b.2 กดแก้ไขข้อมูล 2b.3 ดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.10 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Manage Impact Level

ตารางที่ 4.8 รายละเอียดยูสเคส Risk Assignment

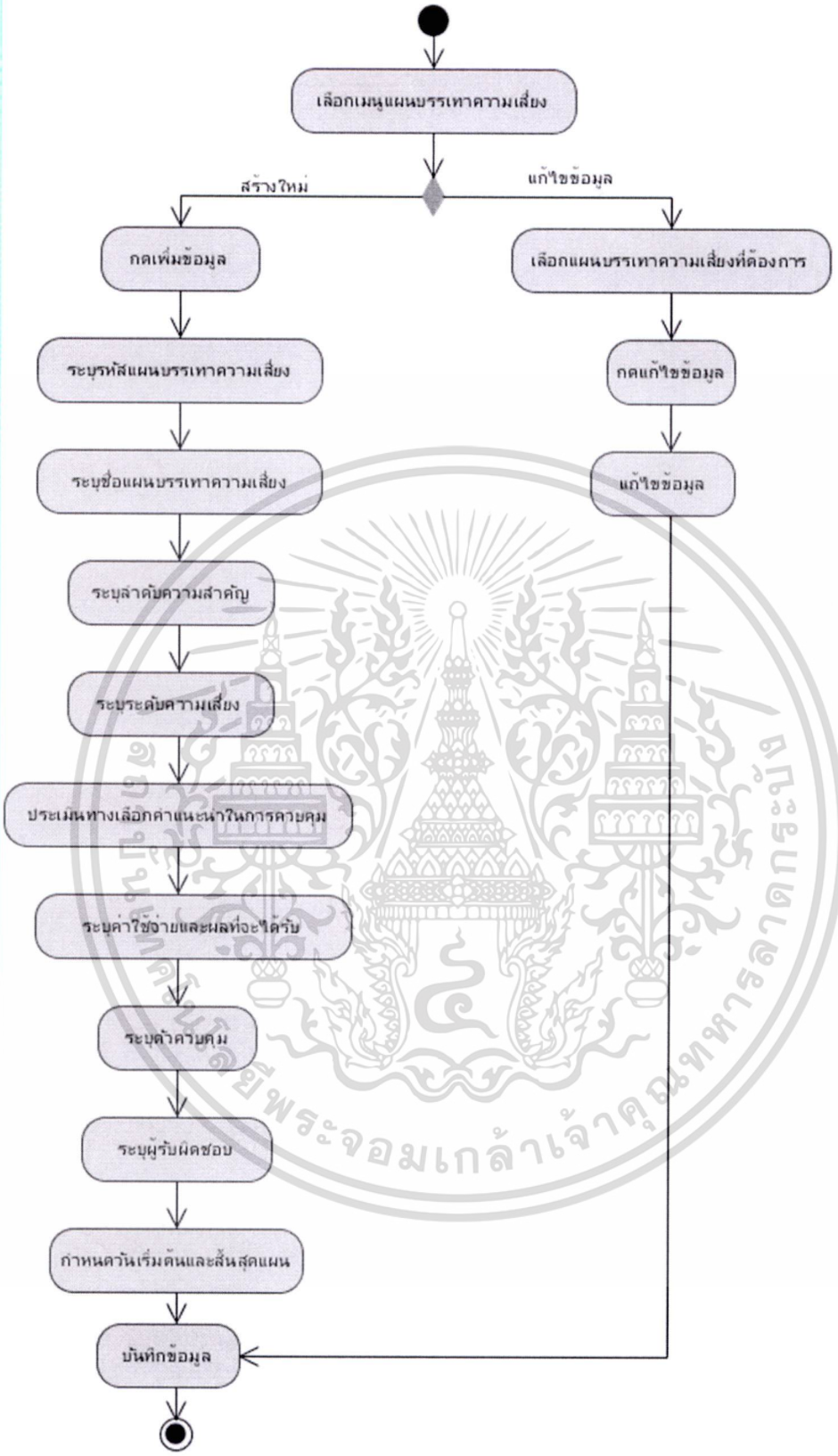
ชื่อยูสเคส	Risk Assignment
รายละเอียดโดยสังเขป	ผู้วิเคราะห์ความเสี่ยงทำการเลือกพารามิเตอร์ต่างๆ เพื่อใช้ในการวิเคราะห์ความเสี่ยง
แอกเตอร์	ผู้วิเคราะห์ความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูประเมินความเสี่ยง 2. เลือกสินทรัพย์ที่ต้องการประเมิน 3. เลือกภัยคุกคาม 4. เลือกจุดอ่อน 5. เลือกตัวควบคุม 6. เลือกความน่าจะเป็น 7. เลือกระดับผลกระทบด้านต่างๆ 8. กดแสดงผล 9. บันทึกข้อมูลลงระบบ
ขั้นตอนการทำงานทางเลือก	
เงื่อนไขภายหลัง	



รูปที่ 4.11 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Risk Assignment

ตารางที่ 4.9 รายละเอียดยูสเคส Mitigating Plan

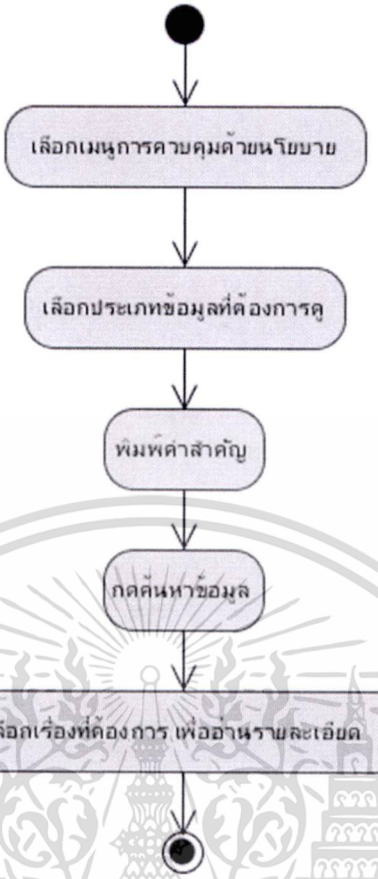
ชื่อยูสเคส	Mitigating Plan
รายละเอียดโดยสังเขป	ผู้บริหารจัดการความเสี่ยงสร้างแผนบรรเทาความเสี่ยงโดยเลือกข้อมูลที่ได้ผู้วิเคราะห์ความเสี่ยงได้ทำการบันทึกไว้ในระบบ
แอกเตอร์	ผู้บริหารจัดการความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูแผนบรรเทาความเสี่ยง 2. เลือกประเภทการจัดการว่าเป็นการสร้างข้อมูลใหม่หรือแก้ไขข้อมูลเดิม 3. บันทึกข้อมูล
ขั้นตอนการทำงานทางเลือก	2a.1 กดเพิ่มข้อมูล 2a.2 ระบุรหัสและชื่อแผนบรรเทาความเสี่ยง 2a.3 ระบุลำดับความสำคัญ 2a.4 ระบุระดับความเสี่ยง 2a.5 ประเมินทางเลือกคำแนะนำในการควบคุม 2a.6 ระบุค่าใช้จ่ายและผลที่จะได้รับ 2a.7 ระบุตัวควบคุม 2a.8 ระบุผู้รับผิดชอบ 2a.9 กำหนดวันเริ่มต้นและสิ้นสุดแผน 2b.1 เลือกแผนบรรเทาความเสี่ยงที่ต้องการ 2b.2 กดแก้ไขและดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.12 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Mitigating Plan

ตารางที่ 4.10 รายละเอียดยูสเคส Evaluate

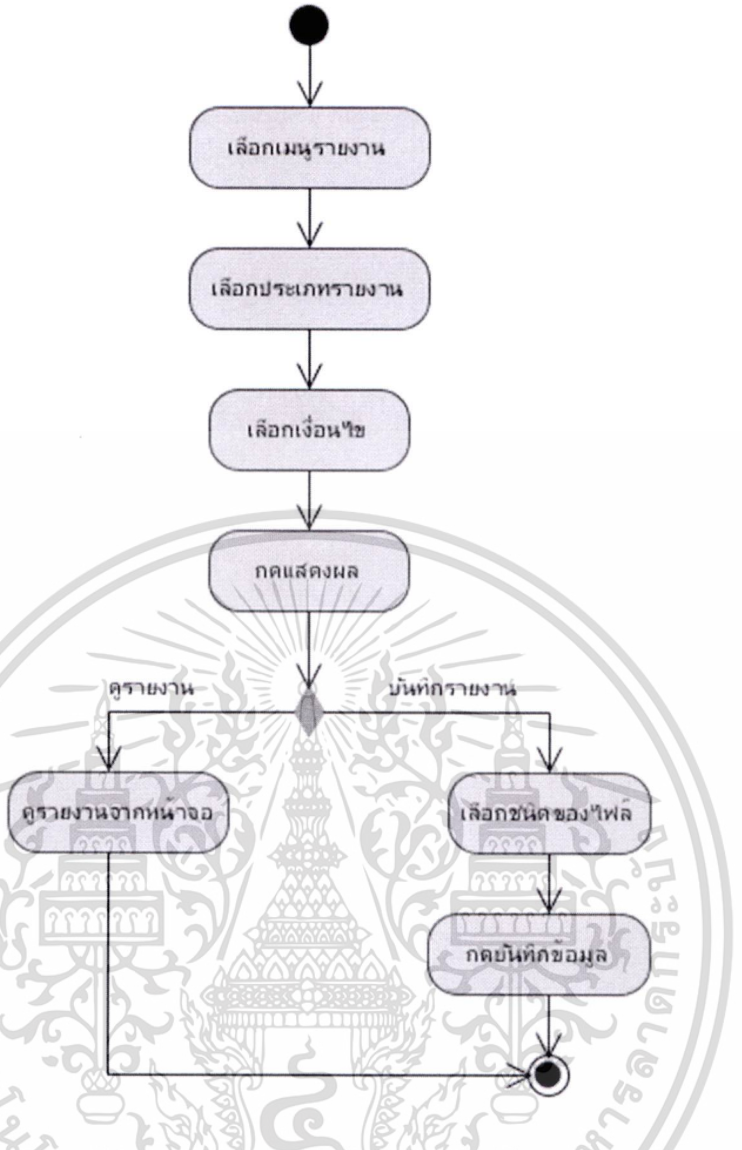
ชื่อยูสเคส	Evaluate
รายละเอียดโดยสังเขป	ผู้บริหารจัดการความเสี่ยง ทำการเลือกประเภทข้อมูลที่ต้องการเพื่อศึกษาข้อมูลสำหรับการตัดสินใจ
แอกเตอร์	ผู้บริหารจัดการความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูการควบคุมด้วยนโยบาย 2. เลือกประเภทข้อมูลที่ต้องการ 3. พิมพ์คำสำคัญ 4. กดค้นหาข้อมูล 5. เลือกเรื่องที่ต้องการเพื่ออ่านรายละเอียด
ขั้นตอนการทำงานทางเลือก	2a. กดเพิ่มข้อมูล ระบุรหัสและชื่อของภัยคุกคาม พิมพ์รายละเอียดของภัยคุกคาม 2b. เลือกจุดอ่อนที่ต้องการแก้ไขข้อมูล กดแก้ไขและดำเนินการแก้ไขข้อมูล
เงื่อนไขภายหลัง	



รูปที่ 4.13 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส Evaluate

ตารางที่ 4.11 รายละเอียดยูสเคส View Report

ชื่อยูสเคส	View Report
รายละเอียดโดยสังเขป	ผู้ใช้งานระบบเลือกประเภทรายงาน กำหนดเงื่อนไขต่างๆ เพื่อดูรายงานและเลือกชนิดของไฟล์เพื่อบันทึกรายงาน
แอกเตอร์	ผู้ดูแลระบบ, ผู้วิเคราะห์ความเสี่ยง และผู้บริหารจัดการความเสี่ยง
ผู้มีส่วนได้เสีย	
เงื่อนไขก่อนหน้า	
ขั้นตอนการทำงานหลัก	1. เลือกเมนูรายงาน 2. เลือกประเภทรายงาน 3. เลือกเงื่อนไข 4. กดแสดงผล 5. กดบันทึกผล
ขั้นตอนการทำงานทางเลือก	2a. ดูรายงานจากหน้าจอแสดงผล 2b. เลือกชนิดของไฟล์เพื่อบันทึกข้อมูลรายงาน
เงื่อนไขภายหลัง	

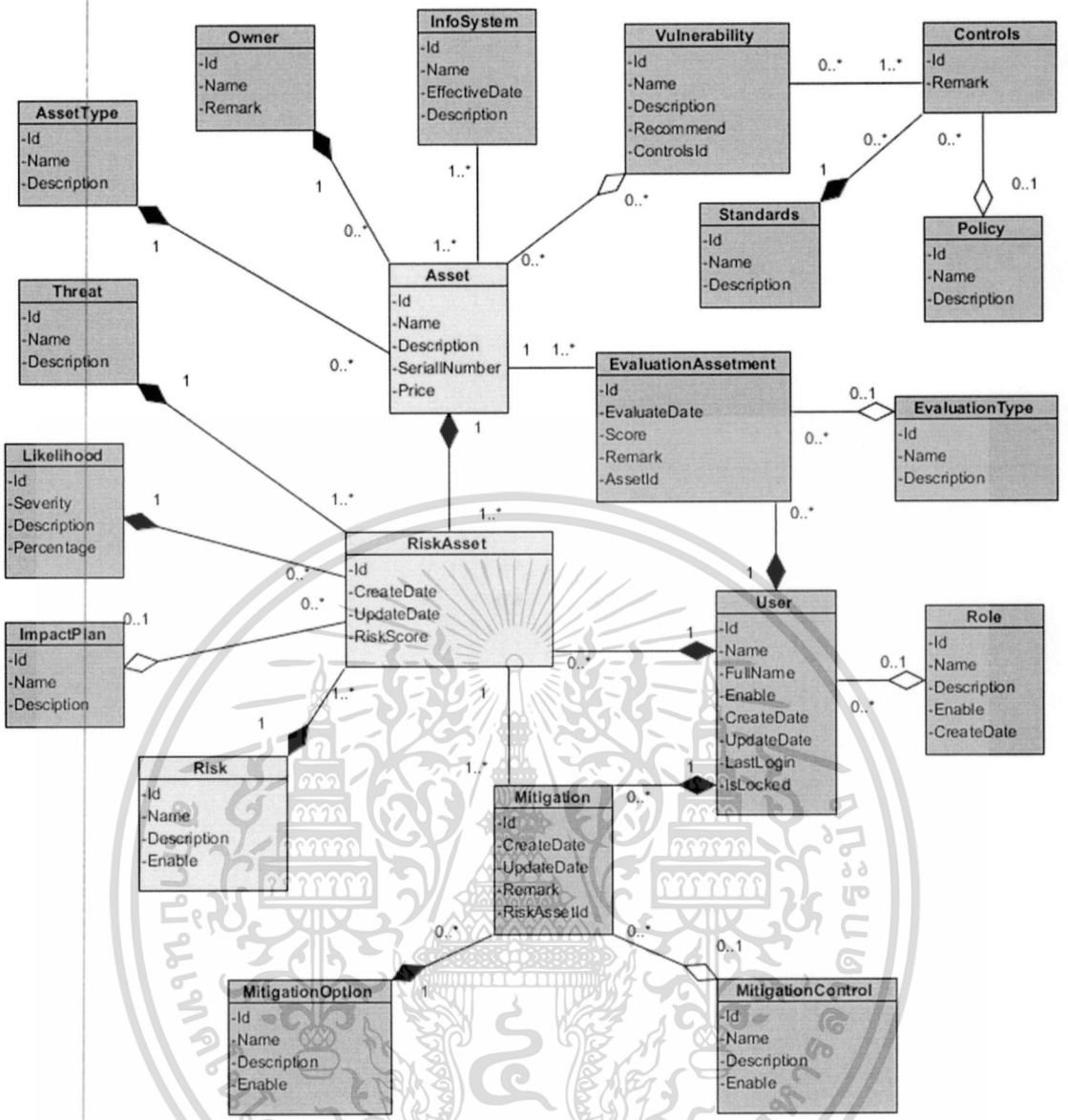


รูปที่ 4.14 แอ็กทิวิตีไดอะแกรมอธิบายยูสเคส View Report

4.5.2 Class Diagram

จากการวิเคราะห์และออกแบบโครงสร้างของระบบบริหารความเสี่ยง สามารถสร้างคลาสไดอะแกรมได้ โดยคลาสต่างๆ จะแสดงโครงสร้างความสัมพันธ์ระหว่างคลาสที่จำเป็นในระบบ แสดงได้ดังรูปที่ 4.15 ซึ่งประกอบไปด้วย 20 คลาส ดังต่อไปนี้

1. Asset เป็นคลาสของทรัพย์สิน
2. AssetType เป็นคลาสของชนิดของทรัพย์สิน
3. Controls เป็นคลาสของการควบคุมความเสี่ยง
4. EvaluationAssetment เป็นคลาสของการวัดผลและประเมินความเสี่ยง
5. EvaluationType เป็นคลาสของชนิดของการวัดผล
6. ImpactPlan เป็นคลาสของการวางแผนผลกระทบ
7. InfoSystem เป็นคลาสของรายละเอียดของระบบ
8. Likelihood เป็นคลาสของโอกาสความน่าจะเป็นของภัยคุกคาม
9. Mitigation เป็นคลาสของการบรรเทาความเสี่ยง
10. MitigationControl เป็นคลาสของแนวทางสำหรับใช้การควบคุมความเสี่ยง
11. MitigationOption เป็นคลาสของทางเลือกในการบรรเทาความเสี่ยง
12. Owner เป็นคลาสของเจ้าของทรัพย์สิน
13. Policy เป็นคลาสของนโยบายความเสี่ยงขององค์กร
14. Risk เป็นคลาสของความเสี่ยง
15. RiskAsset เป็นคลาสของการประเมินความเสี่ยง
16. Role เป็นคลาสของบทบาทของผู้ที่เกี่ยวข้อง
17. Standards เป็นคลาสของมาตรฐานที่เกี่ยวข้องกับการบริหารความเสี่ยง
18. Threat เป็นคลาสของการระบุภัยคุกคาม
19. User เป็นคลาสของ ผู้ที่เกี่ยวข้องในการบริหารความเสี่ยง
20. Vulnerability เป็นคลาสของจุดอ่อนหรือช่องใหว่ของระบบสารสนเทศ

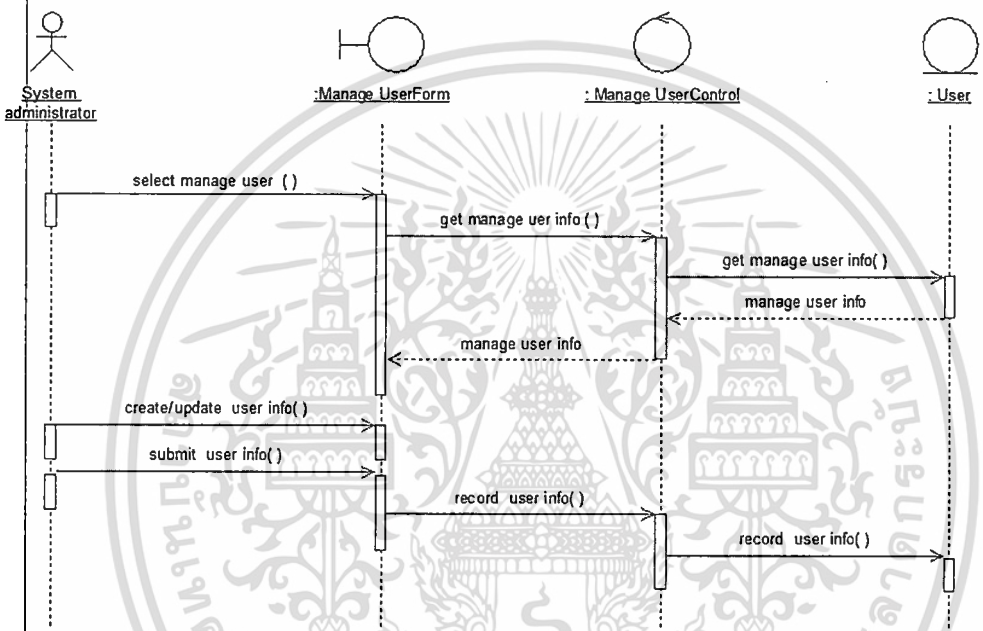


รูปที่ 4.15 คลาสไดอะแกรมระบบสนับสนุนการการบริหารความเสี่ยง

4.5.3 ซีเควนซ์ไดอะแกรม

ระบบสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยง ซึ่งมีทั้งหมด 11 ซีเควนซ์ไดอะแกรม ได้แก่

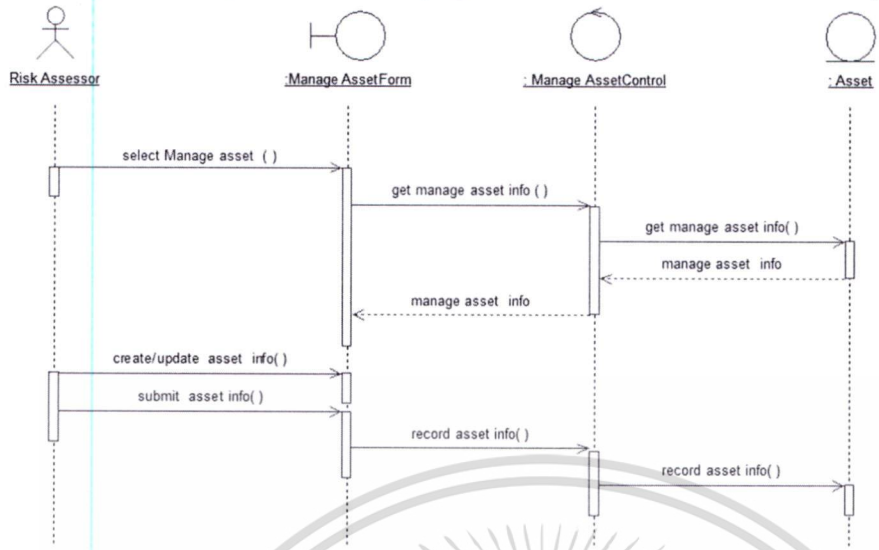
1.จากยูสเคสการบันทึกผู้ใช้งาน (Manage User) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ดูแลระบบ เลือก Manage User ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล User เมื่อระบบพบข้อมูลในคลาส User ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage UserForm ผู้ดูแลระบบสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.16



รูปที่ 4.16 ซีเควนซ์ไดอะแกรมของยูสเคส Manage User

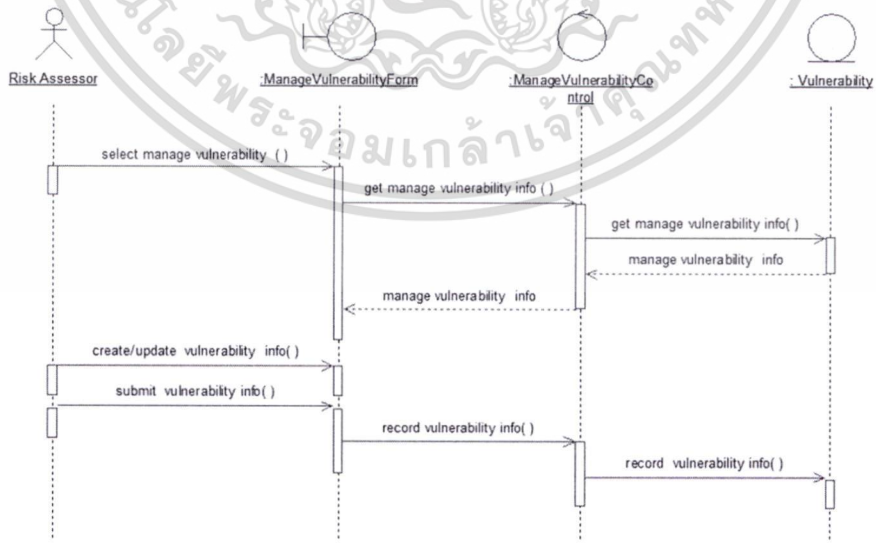
2. จากยูสเคสการจัดการสินทรัพย์ (Manage Asset) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Manage Asset ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Asset เมื่อระบบพบข้อมูลในคลาส Asset ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage AssetForm ผู้ประเมินความ

เสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.17



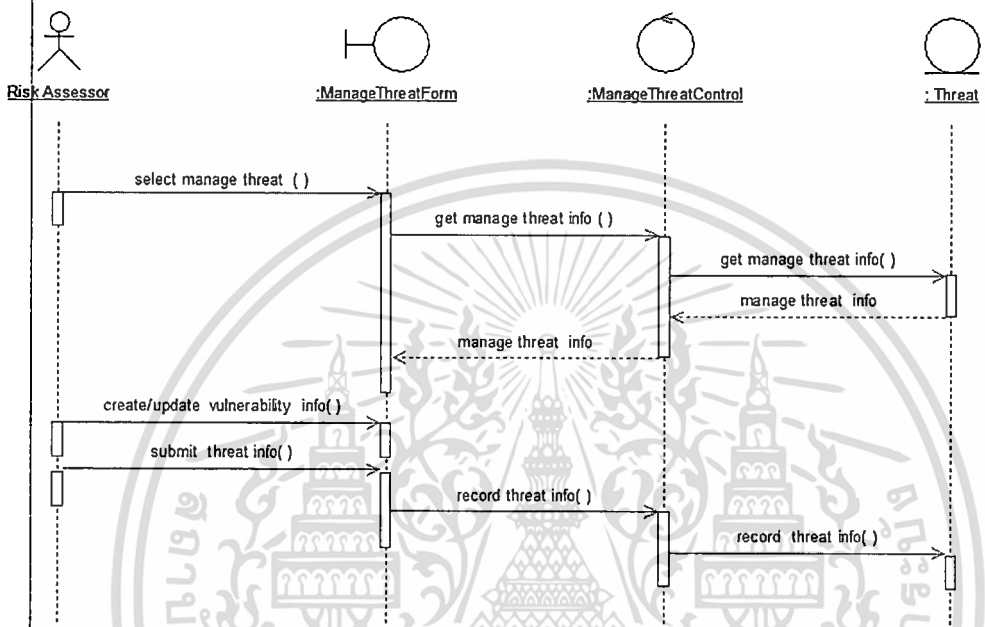
รูปที่ 4.17 ซีเควนซ์ไดอะแกรมของยูสเคส Manage Asset

3. จากยูสเคสการจัดการข้อมูลจุดอ่อน (Manage Vulnerability) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Manage Vulnerability ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Vulnerability เมื่อระบบพบข้อมูลในคลาส Vulnerability ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage VulnerabilityForm ผู้ประเมินความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.18



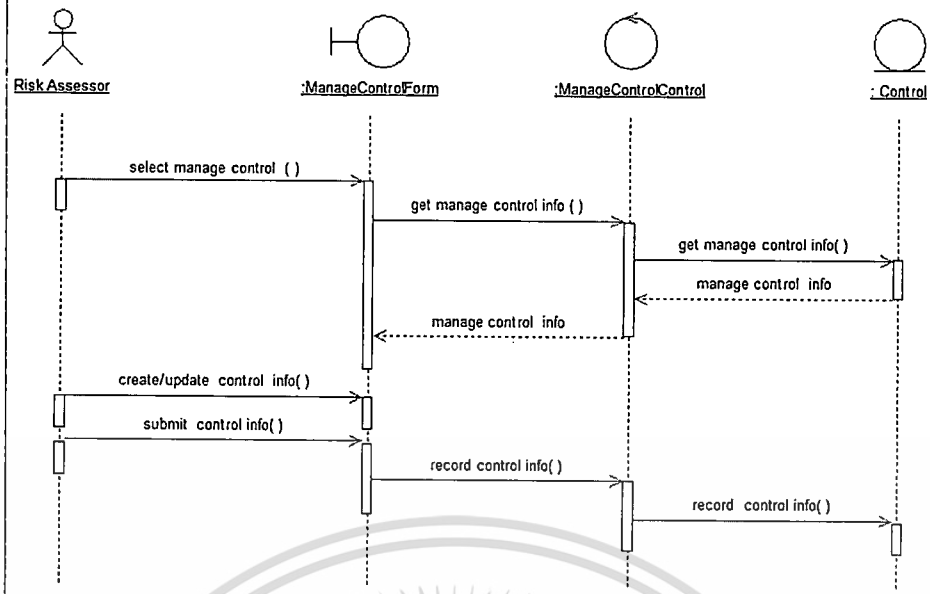
รูปที่ 4.18 ซีเควนซ์ไดอะแกรมของยูสเคส Manage Vulnerability

4. จากยูสเคสการจัดการข้อมูลภัยคุกคาม (Manage Threat) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Manage Threat ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Threat เมื่อระบบพบข้อมูลในคลาส Threat ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage ThreatForm ผู้ประเมินความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.19



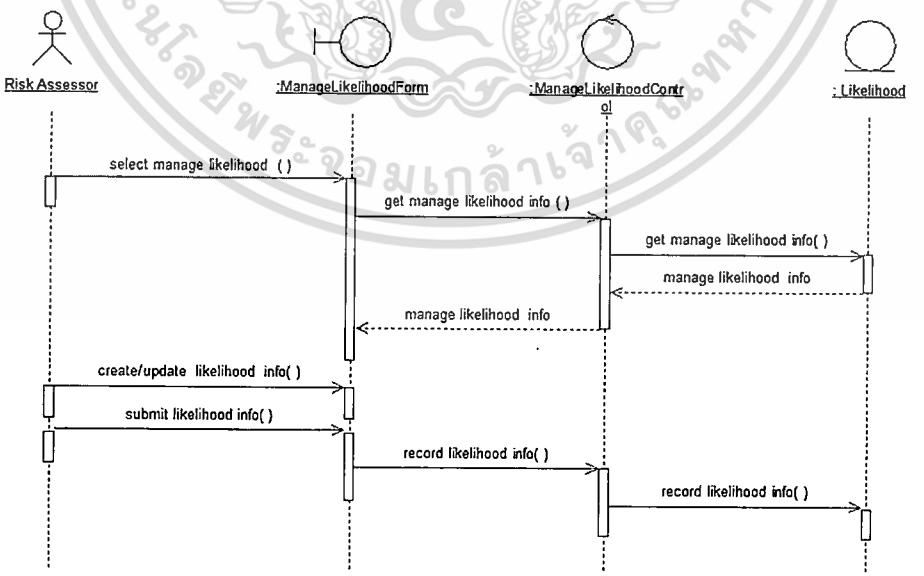
รูปที่ 4.19 ซีเควนซ์ไดอะแกรมของยูสเคส Manage Threat

5. จากยูสเคสการควบคุม (Manage Control) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Manage Control ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Control เมื่อระบบพบข้อมูลในคลาส Control ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage ControlForm ผู้ประเมินความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.20



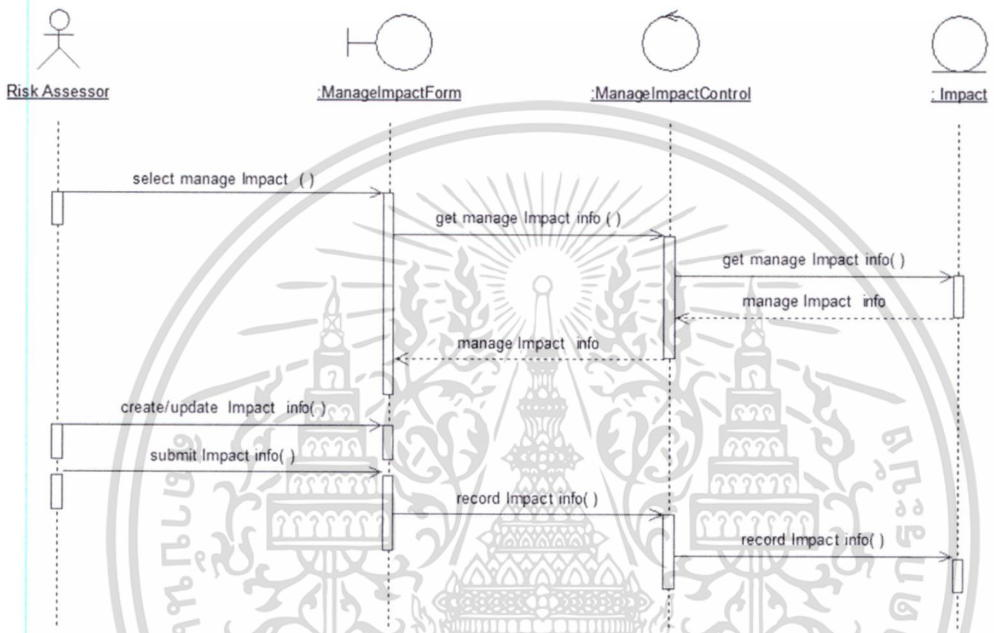
รูปที่ 4.20 ซีเควนซ์ไดอะแกรมของยูสเคส Manage Control

6. จากยูสเคสการจัดการความเป็นไปได้ (Manage likelihood) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Manage likelihood ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล likelihood เมื่อระบบพบข้อมูลในคลาส likelihood ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage likelihood Form ผู้ประเมินความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.21



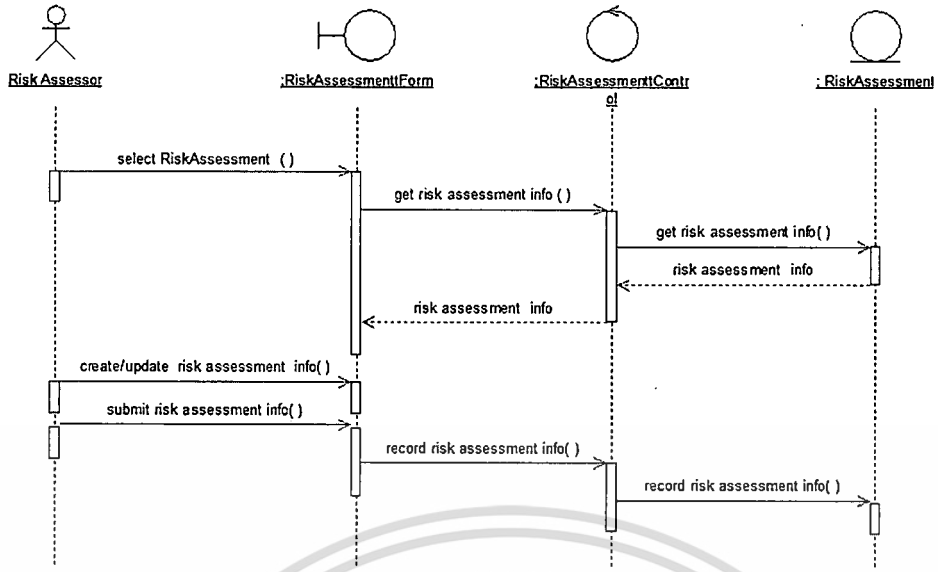
รูปที่ 4.21 ซีเควนซ์ไดอะแกรมของยูสเคส Manage likelihood

7. จากยูสเคสการจัดการผลกระทบ (Manage Impact) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Manage Impact ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Impact เมื่อระบบพบข้อมูลในคลาส Impact ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Manage ImpactForm ผู้ประเมินความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.22



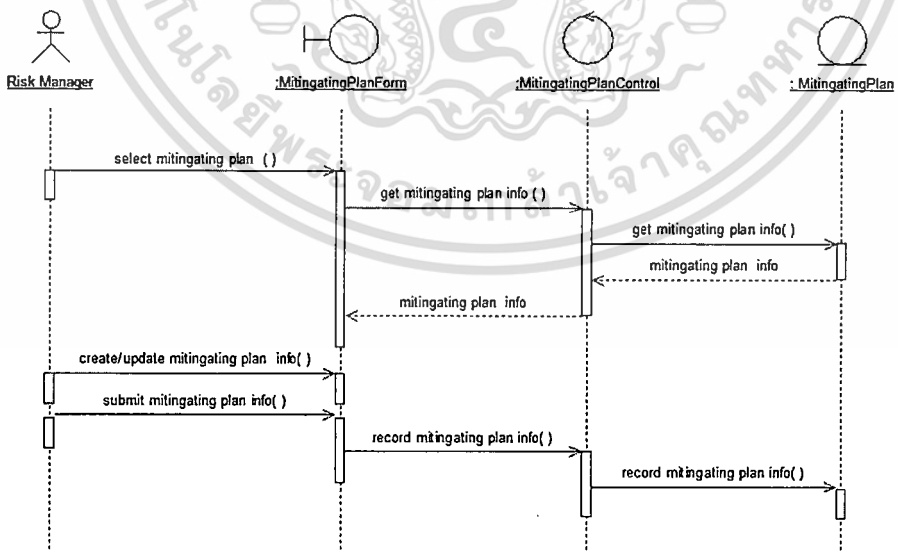
รูปที่ 4.22 ซีเควนซ์ไดอะแกรมของยูสเคส Manage Impact

8. จากยูสเคสการประเมินความเสี่ยง (Risk Assessment) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ประเมินความเสี่ยง เลือก Risk Assessment ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Risk Assessment เมื่อระบบพบข้อมูลในคลาส Risk Assessment ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Risk AssessmentForm ผู้ประเมินความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.23



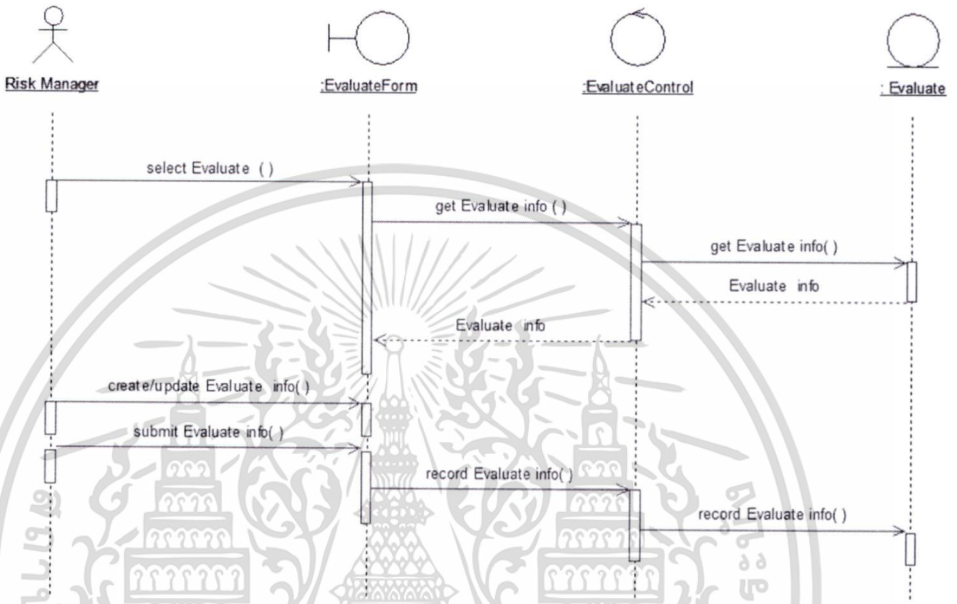
รูปที่ 4.23 ซีเควนซ์ไดอะแกรมของยูสเคส Risk Assessment

9. จากยูสเคสการสร้างแผนบรรเทา (Mitigating Plan) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้จัดการความเสี่ยง เลือก Mitigating Plan ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Mitigating Plan เมื่อระบบพบข้อมูลในคลาส Mitigating Plan ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ Mitigating PlanForm ผู้จัดการความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.24



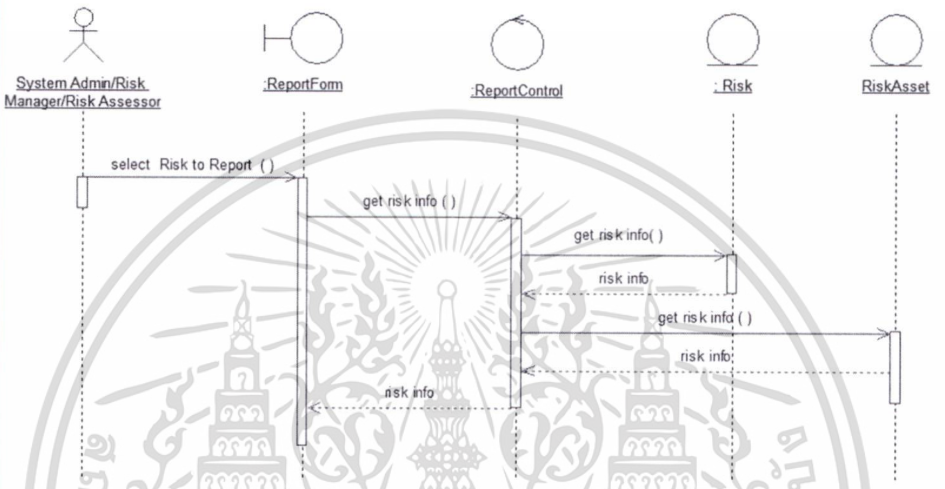
รูปที่ 4.24 ซีเควนซ์ไดอะแกรมของยูสเคส Mitigating Plan

10. จากยูสเคสการประเมินผล (Evaluate) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้จัดการความเสี่ยง เลือก Evaluate ระบบจะทำการค้นหาเพื่อทำการสร้างข้อมูลหรือปรับปรุงข้อมูล Evaluate เมื่อระบบพบข้อมูลในคลาส Evaluate ก็จะแสดงข้อมูลผู้ใช้งานระบบผ่านทางหน้าจอ EvaluateForm ผู้จัดการความเสี่ยงสามารถปรับปรุงหรือบันทึกข้อมูลผู้ใช้งานลงในระบบได้ ดังแสดงตามรูปที่ 4.25



รูปที่ 4.25 ซีเควนซ์ไดอะแกรมของยูสเคส Evaluate

11. จากยูสเคสแสดงรายงาน (View Report) สามารถนำมาเขียน ซีเควนซ์ไดอะแกรม เพื่ออธิบายรายละเอียดการทำงานของยูสเคสได้ คือ ผู้ดูแลระบบ ผู้ประเมินความเสี่ยง ผู้จัดการความเสี่ยง เรียกใช้รายงานโดยเรียกจากรหัสความเสี่ยง เพื่อเรียกรายงานข้อมูลความเสี่ยง เมื่อระบบพบข้อมูลในคลาส Risk คลาส Risk Asset ก็จะแสดงรายงานผ่านทางหน้าจอ ReportForm ผู้ดูแลระบบ ผู้ประเมินความเสี่ยง ผู้จัดการความเสี่ยง เข้าสู่หน้าจอการเรียกดูรายงานของโครงการต่างๆ ดังแสดงตามรูปที่ 4.26



รูปที่ 4.26 ซีเควนซ์ไดอะแกรมของยูสเคส View Report

4.6 การออกแบบฐานข้อมูล

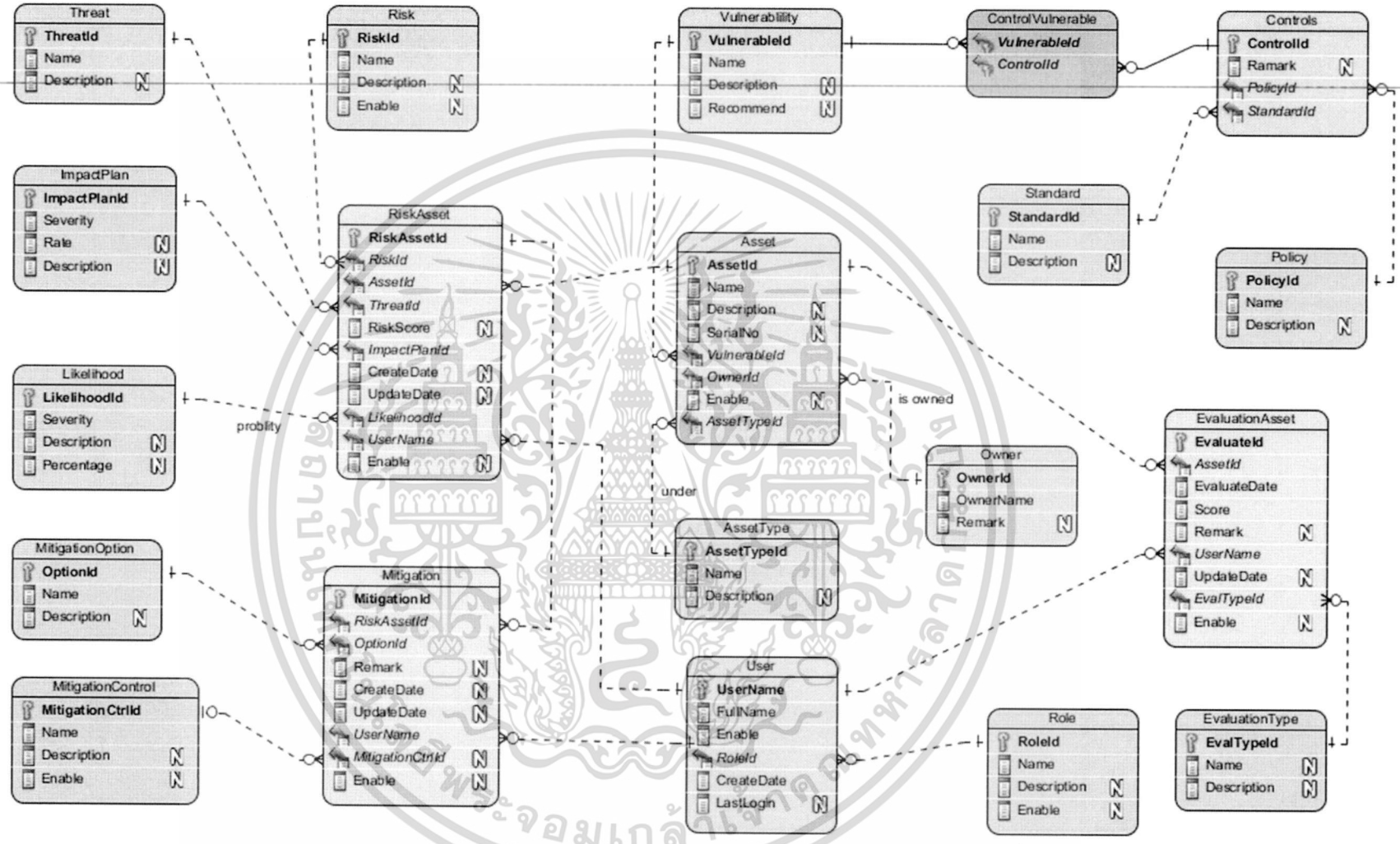
แบ่งออกเป็น 2 ส่วน ได้แก่ แผนภาพเชิงสัมพันธ์ระหว่างเอนทิตี และพจนานุกรมข้อมูล

4.6.1 แผนภาพเชิงสัมพันธ์ระหว่างเอนทิตี

จากการวิเคราะห์และออกแบบโครงสร้างของระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง สามารถออกแบบฐานข้อมูลเชิงสัมพันธ์ โดยเขียนเป็นแผนภาพเชิงสัมพันธ์ระหว่างเอนทิตีหรืออีอาร์ไดอะแกรม ได้ดังรูปที่ 4.27 โดยประกอบไปด้วยตารางต่างๆ จำนวน 20 เอนทิตี สำหรับใช้จัดเก็บข้อมูลดังนี้

1. Asset หมายถึง ทรัพย์สิน
2. AssetType หมายถึง ชนิดของทรัพย์สิน
3. Controls หมายถึง การควบคุมความเสี่ยง
4. ControlVulnerable หมายถึง การวัดผลและประเมินความเสี่ยง

5. EvaluationAsset หมายถึง ชนิดของการวัดผล
6. EvaluationType หมายถึง การวางแผนผลกระทบ
7. ImpactPlan หมายถึง รายละเอียดของระบบ
8. Likelihood หมายถึง โอกาสความน่าจะเป็นของภัยคุกคาม
9. Mitigation หมายถึง การบรรเทาความเสี่ยง
10. MitigationControl หมายถึง แนวทางสำหรับใช้การควบคุมความเสี่ยง
11. MitigationOption หมายถึง ทางเลือกในการบรรเทาความเสี่ยง
12. Owner หมายถึง เจ้าของทรัพย์สิน
13. Policy หมายถึง นโยบายความเสี่ยงขององค์กร
14. Risk หมายถึง ความเสี่ยง
15. RiskAsset หมายถึง การประเมินความเสี่ยง
16. Role หมายถึง บทบาทของผู้ที่เกี่ยวข้อง
17. Standard หมายถึง มาตรฐานที่เกี่ยวข้องกับการบริหารความเสี่ยง
18. Threat หมายถึง การระบุภัยคุกคาม
19. User หมายถึง ผู้ที่เกี่ยวข้องในการบริหารความเสี่ยง
20. Vulnerablility หมายถึง จุดอ่อนหรือช่องโหว่ของระบบสารสนเทศ



รูปที่ 4.27 แผนภาพเชิงสัมพันธ์ระหว่างเอนทิตีของระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง

4.6.2 พจนานุกรมข้อมูล

พจนานุกรมของระบบบริหารความเสี่ยง มีทั้งหมด 21 ตาราง แสดงได้ดังตารางที่ 4.14 ถึง 4.34

ตารางที่ 4.12 พจนานุกรมข้อมูลตาราง Asset

ตาราง Asset จัดเก็บข้อมูลทรัพย์สิน					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
AssetId	รหัสทรัพย์สิน	Integer	10	PK	
Name	ชื่อทรัพย์สิน	Varchar	250		
Description	รายละเอียดของทรัพย์สิน	Varchar	500		
SerialNo	หมายเลขของทรัพย์สิน	Varchar	40		
VulnerableId	รหัสของจุดอ่อน	Integer	10	FK	Vulnerablility
OwnerId	รหัสเจ้าของทรัพย์สิน	Integer	10	FK	Owner
Enable	สถานะของทรัพย์สิน	Bit			
AssetTypeId	รหัสชนิดของทรัพย์สิน	Integer	10	FK	AssetType

ตารางที่ 4.13 พจนานุกรมข้อมูลตาราง AssetType

ตาราง AssetType จัดเก็บข้อมูลชนิดของทรัพย์สิน					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
AssetTypeId	รหัสชนิดของทรัพย์สิน	Integer	10	PK	
Name	ชื่อของชนิดของทรัพย์สิน	Varchar	250		
Description	รายละเอียดชนิดของทรัพย์สิน	Varchar	500		

ตารางที่ 4.14 พจนานุกรมข้อมูลตาราง Controls

ตาราง Controls จัดเก็บข้อมูลการควบคุมความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
ControlId	รหัสควบคุม	Integer	10	PK	
Remark	รายละเอียดเพิ่มเติม	Varchar	250		
PolicyId	รหัสนโยบาย	Integer	10	FK	Policy
StandardId	รหัสมาตรฐาน	Integer	10	FK	Standard

ตารางที่ 4.15 พจนานุกรมข้อมูลตาราง ControlVulnerable

ตาราง ControlVulnerable จัดเก็บข้อมูลการวัดผลและประเมินความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
VulnerableId	รหัสจุดอ่อน	Integer	10	PK/FK	Vulnerablility
ControlId	รหัสควบคุมจุดอ่อน	Integer	10	PK/FK	Controls

ตารางที่ 4.16 พจนานุกรมข้อมูลตาราง EvaluationAsset

ตาราง EvaluationAsset จัดเก็บข้อมูลชนิดของการวัดผล					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
EvaluateId	รหัสการประเมิน	Integer	10	PK	
AssetId	รหัสทรัพย์สิน	Integer	10	FK	Asset
EvaluateDate	วันที่ประเมิน	Date			
Score	ระดับความเสี่ยง	Integer	10		
Remark	รายละเอียดเพิ่มเติม	Varchar	250		
UserName	ชื่อผู้ประเมิน	Varchar		FK	User
UpdateDate	วันที่ Update การประเมิน	Date	50		
EvalTypeId	รหัสชนิดของการประเมิน	Integer		FK	EvaluationType
Enable	สถานะการประเมิน	Bit	10		

ตารางที่ 4.17 พจนานุกรมข้อมูลตาราง EvaluationType

ตาราง EvaluationType จัดเก็บข้อมูลการวางแผนผลกระทบ					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
EvalTypeId	รหัสชนิดของการประเมิน	Integer	10	PK	
Name	ชื่อของการ	Varchar	100		
Description	รายละเอียดของการประเมิน	Varchar	300		

ตารางที่ 4.18 พจนานุกรมข้อมูลตาราง ImpactPlan

ตาราง ImpactPlan จัดเก็บข้อมูลรายละเอียดของระบบ					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
ImpactPlanId	รหัสผลกะทบ	Integer	10	PK	
Severity	ความรุนแรง	Varchar	50		
Rate	อัตราความรุนแรง	Decimal	5		
Description	รายละเอียดผลกระทบ	Varchar	250		

ตารางที่ 4.19 พจนานุกรมข้อมูลตาราง Likelihood

ตาราง Likelihood จัดเก็บข้อมูลโอกาสความน่าจะเป็นของภัยคุกคาม					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
LikelihoodId	รหัสโอกาสที่จะเกิด	Integer	10	PK	
Severity	ความรุนแรง	Varchar	50		
Description	รายละเอียดของโอกาส	Varchar	250		
Percentage	เปอร์เซนต์ของโอกาส	Decimal	5		

ตารางที่ 4.20 พจนานุกรมข้อมูลตาราง Mitigation

ตาราง Mitigation จัดเก็บข้อมูลการบรรเทาความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
MitigationId	รหัสการบรรเทาความเสี่ยง	Integer	10	PK	
RiskAssetId	รหัสการประเมินความเสี่ยง	Integer	10	FK	RiskAsset
OptionId	รหัสทางเลือการบรรเทาความเสี่ยง	Integer	10	FK	MitigationOption
Remark	รายละเอียดการบรรเทา	Varchar	255		
CreateDate	วันที่สร้างการบรรเทาความเสี่ยง	Date			
UpdateDate	วันที่ปรับปรุงการบรรเทาความเสี่ยง	Date			
UserName	ชื่อผู้ใช้งาน	Varchar	50	FK	User
MitigationCtrlId	รหัสการบรรเทาความเสี่ยง	Integer	10	FK	MitigationControl
Enable	สถานะของการบรรเทาความเสี่ยง	Bit			

ตารางที่ 4.21 พจนานุกรมข้อมูลตาราง MitigationControl

ตาราง MitigationControl จัดเก็บข้อมูลแนวทางสำหรับใช้การควบคุมความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
MitigationCtrlId	รหัสการควบคุมบรรเทาความเสี่ยง	Integer	10	PK	
Name	ชื่อการควบคุมการบรรเทาความเสี่ยง	Varchar	100		
Description	รายละเอียดการควบคุมการบรรเทาความเสี่ยง	Varchar	255		
Enable	สถานะการควบคุมการบรรเทาความเสี่ยง	Bit			

ตารางที่ 4.22 พจนานุกรมข้อมูลตาราง MitigationOption

ตาราง MitigationOption จัดเก็บข้อมูล ทางเลือกในการบรรเทาความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
OptionId	รหัสของทางเลือก	Integer	10	PK	
Name	ชื่อของทางเลือก	Varchar	50		
Description	รายละเอียดของทางเลือก	Varchar	300		

ตารางที่ 4.23 พจนานุกรมข้อมูลตาราง Owner

ตาราง Owner จัดเก็บข้อมูลเจ้าของทรัพย์สิน					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
OwnerId	รหัสเจ้าของทรัพย์สิน	Integer	10	PK	
OwnerName	ชื่อเจ้าของทรัพย์สิน	Varchar	250		
Remark	รายละเอียดเจ้าของทรัพย์สิน	Varchar	300		

ตารางที่ 4.24 พจนานุกรมข้อมูลตาราง Policy

ตาราง Policy จัดเก็บข้อมูลนโยบายความเสี่ยงขององค์กร					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
PolicyId	รหัสของนโยบาย	Integer	10	PK	
Name	ชื่อของนโยบาย	Varchar	250		
Description	รายละเอียดของนโยบาย	Varchar	500		

ตารางที่ 4.25 พจนานุกรมข้อมูลตาราง Risk

ตาราง Risk จัดเก็บข้อมูลความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
RiskId	รหัสความเสี่ยง	Integer	10	PK	
Name	ชื่อความเสี่ยง	Varchar	200		
Description	รายละเอียดความเสี่ยง	Varchar	300		
Enable	สถานะของความเสี่ยง	Bit			

ตารางที่ 4.26 พจนานุกรมข้อมูลตาราง RiskAsset

ตาราง RiskAsset จัดเก็บข้อมูลการประเมินความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
RiskAssetId	รหัสการประเมินความเสี่ยง	Integer	10	PK	
RiskId	รหัสความเสี่ยง	Integer	10	FK	Risk.
AssetId	รหัสทรัพย์สิน	Integer	10	FK	Asset
ThreatId	รหัสภัยคุกคาม	Integer	10	FK	Threat
RiskScore	คะแนนความเสี่ยง	decimal	10		
ImpactPlanId	รหัสแผนผลกระทบ	Integer	10	FK	ImpactPlan
CreateDate	วันที่ประเมินความเสี่ยง	Date			
UpdateDate	วันที่ปรับปรุงการประเมินความเสี่ยง	Date			
LikelihoodId	รหัสโอกาส	Integer	10	FK	Likelihood
UserName	ชื่อผู้ใช้งาน	Varchar	50	FK	User
Enable	สถานะของการประเมินความเสี่ยง	Bit			

ตารางที่ 4.27 พจนานุกรมข้อมูลตาราง Role

ตาราง Role จัดเก็บข้อมูลบทบาทของผู้ที่เกี่ยวข้อง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
RoleId	รหัสบทบาท	Integer	10	PK	
Name	ชื่อบทบาท	Varchar	100		
Description	รายละเอียดของบทบาท	Varchar	255		
Enable	สถานะของบทบาท	Bit			

ตารางที่ 4.28 พจนานุกรมข้อมูลตาราง Standard

ตาราง Standard จัดเก็บข้อมูลมาตรฐานที่เกี่ยวข้องกับการบริหารความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
StandardId	รหัสมาตรฐาน	Integer	10	PK	
Name	ชื่อมาตรฐาน	Varchar	250		
Description	รายละเอียดของมาตรฐาน	Varchar	250		

ตารางที่ 4.29 พจนานุกรมข้อมูลตาราง Threat

ตาราง Threat จัดเก็บข้อมูลการระบุภัยคุกคาม					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
ThreatId	รหัสภัยคุกคาม	Integer	10	PK	
Name	ชื่อภัยคุกคาม	Varchar	250		
Description	รายละเอียดของภัยคุกคาม	Varchar	250		

ตารางที่ 4.30 พจนานุกรมข้อมูลตาราง User

ตาราง User จัดเก็บข้อมูลผู้ที่เกี่ยวข้องในการบริหารความเสี่ยง					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
UserName	ชื่อผู้ใช้	Varchar	50	PK	
FullName	ชื่อเต็มผู้ใช้	Varchar	255		
Enable	เปลี่ยนสถานะพนักงาน	But			
RoleId	รหัสบทบาท	Integer	10	FK	Role
CreateDate	วันที่สร้าง	Date			
LastLogin	ข้อมูลสุดท้ายการเข้าระบบ	Date			

ตารางที่ 4.31 พจนานุกรมข้อมูลตาราง Vulnerability

ตาราง Vulnerablility จัดเก็บข้อมูลจุดอ่อนหรือช่องโหว่ของระบบสารสนเทศ					
แอตทริบิวต์	**ความหมาย**	**ชนิดของข้อมูล**	**ความยาว**	**คีย์**	**ตารางอ้างอิง**
VulnerableId	รหัสความอ่อนแอ	Integer	10	PK	
Name	ชื่อความอ่อนแอ	Varchar	250		
Description	รายละเอียดความอ่อนแอ	Varchar	250		
Recommend	คำแนะนำ	Varchar	250		

บทที่ 5
การออกแบบส่วนต่อประสานกับผู้ใช้

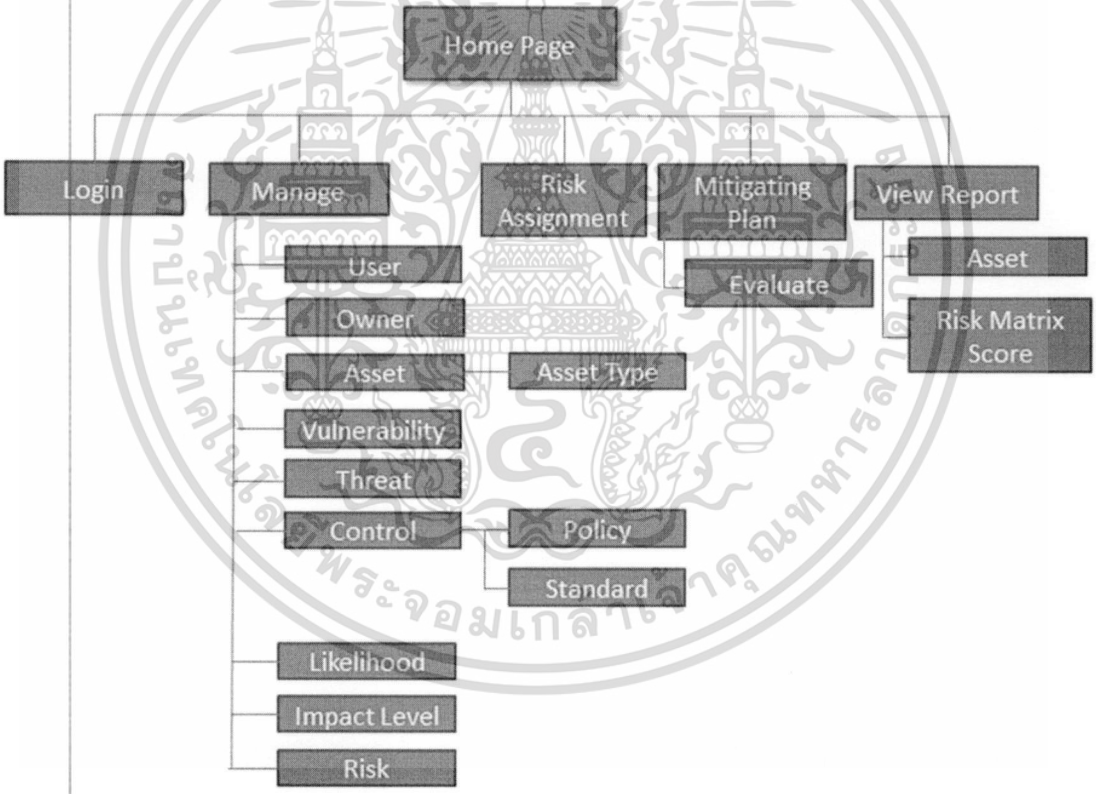
จากการวิเคราะห์และออกแบบระบบการบริหารความเสี่ยง ซึ่งการออกแบบส่วนต่อประส่านกับผู้ใช้ แบ่งเป็น 2 ส่วน ได้แก่

5.1 โครงสร้างของระบบ

5.2 หน้าจอและการทำงานของโปรแกรม

5.1 โครงสร้างของระบบ

โครงสร้างของระบบการบริหารความเสี่ยง ได้ดังรูปที่ 5.1

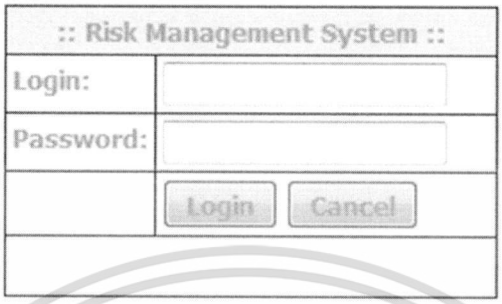


รูปที่ 5.1 แผนภาพเชิงสัมพันธ์ระหว่างเอนทิตีของระบบสารสนเทศเพื่อการสนับสนุนการบริหารความเสี่ยง

หน้าจอและการทำงานของโปรแกรม

5.2.1 หน้าจอเข้าสู่ระบบ

เป็นหน้าจอที่ใช้ในการตรวจสอบสิทธิ์การเข้าใช้งานระบบ แสดงได้ดังรูปที่ 5.2



รูปที่ 5.2 หน้าจอเข้าสู่ระบบ

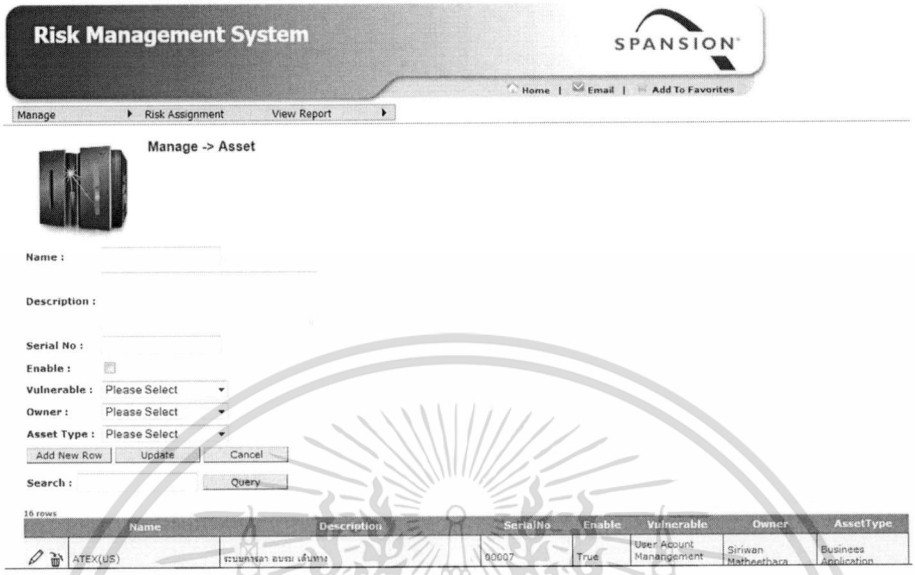
5.2.2 หน้าจอการจัดการข้อมูลผู้ใช้งานระบบ

เป็นหน้าจอที่ใช้ในการสร้างและปรับปรุงข้อมูลผู้ใช้งานระบบ แสดงได้ดังรูปที่ 5.3

รูปที่ 5.3 หน้าจอการจัดการผู้ใช้

5.2.3 หน้าจอการจัดการสินทรัพย์

เป็นหน้าจอที่ใช้ในการบันทึกและปรับปรุงข้อมูลสินทรัพย์ที่มีอยู่ภายในบริษัท แสดงได้ดังรูปที่ 5.4



รูปที่ 5.4 หน้าจอการจัดการสินทรัพย์

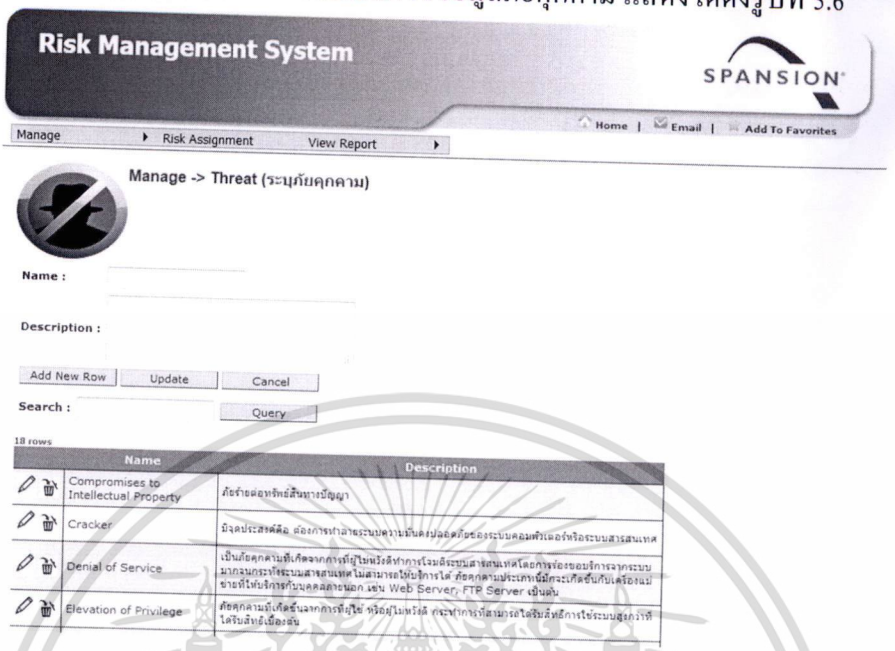
5.2.4 หน้าจอการจัดการจุดอ่อน

เป็นหน้าจอที่ใช้ในการการสร้างและแก้ไขข้อมูลจุดอ่อน แสดงได้ดังรูปที่ 5.5

รูปที่ 5.5 หน้าจอการจัดการจุดอ่อน

5.2.5 หน้าจอการจัดการภัยคุกคาม

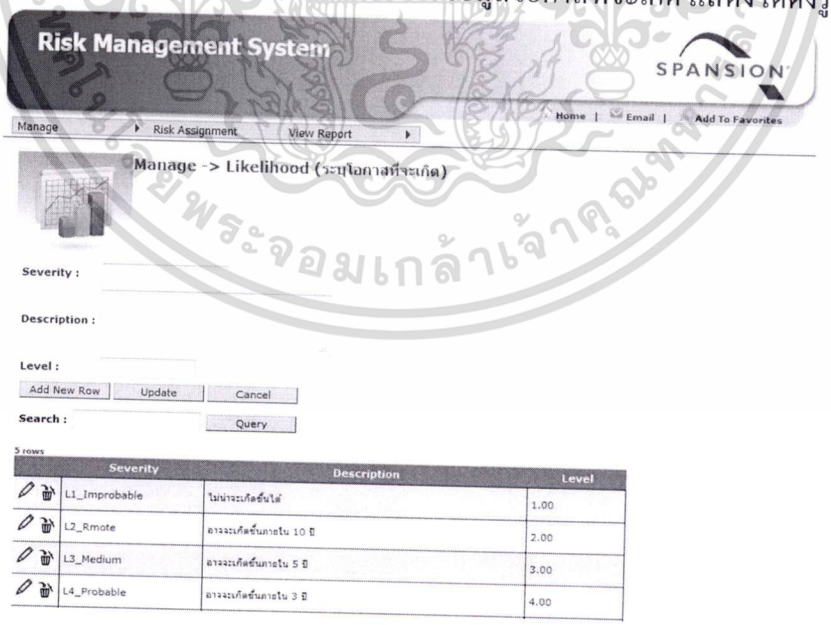
เป็นหน้าจอที่ใช้ในการสร้างและแก้ไขข้อมูลภัยคุกคาม แสดงได้ดังรูปที่ 5.6



รูปที่ 5.6 หน้าจอการจัดการภัยคุกคาม

5.2.7 หน้าจอการจัดการโอกาสที่จะเกิด

เป็นหน้าจอที่ใช้ในการการสร้างและแก้ไขข้อมูลโอกาสที่จะเกิด แสดงได้ดังรูปที่ 5.7



รูปที่ 5.7 หน้าจอการระบุโอกาสที่จะเกิด

บรรณานุกรม

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

อรรณพ ขันธิกุล 2553 **Master in Security** 2nd Edition กรุงเทพ อินโฟเพรส

Coronel, C. Morris, S. and Rob, P. 2011. **Database Principles: Fundamentals of Design, Implementation, and Management.** 9th ed. China: China Translation & Printing Services Limited.

Hughes, B and Cotterll, M. 2002. **Software Project Management.**3rd ed. Berkshire: McGraw-Hill Education (UK).

NIST SP800-30. 2001. **Risk management Guide for Information Technology Systems.** [Online]
Avaliable: http://csrc.nist.gov/publications/PubsSPs.html.

Oestereich, B.2002.**Developing Software with UML Object-Oriented Analysis and Design in Practice.** 2nd ed. Great Britain: Biddles.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายมนตรี ทองมา
วัน เดือน ปีเกิด	14 ธันวาคม 2512 ที่ กรุงเทพมหานคร
ที่อยู่	40/34 หมู่ 8 หมู่บ้าน กิตติญา 3 ต. บางพูด อ. ปากเกร็ด
	จ. นนทบุรี 11120 โทร. 0-2963-1631
ประวัติการศึกษาปริญาตรี	เทคโนโลยีไฟฟ้าอุตสาหกรรม
	สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ความชำนาญเฉพาะด้าน	1) ระบบเครือข่ายคอมพิวเตอร์ Network LAN/WAN
	2) ระบบ Cisco Unified Communications
	3) Data Center Profresional Certified
	4) Network Secrity
ประสบการณ์การทำงาน	
พ.ศ. 2533	ช่างเทคนิค บริษัท ซิกเนติค (ไทยแลนด์) จำกัด
พ.ศ. 2534-ปัจจุบัน	วิศวกรเครือข่ายคอมพิวเตอร์
	MTS (Member Technical Staff)
	บริษัท สแปนชั่น (ไทยแลนด์) จำกัด