ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐาน ไอเอสโอ/ไออีซี 27002

นางสาวเนตยา พิกุลแกม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2552

A SYSTEM TO SUPPORT SECURE SOFTWARE DEVELOPMENT PROCESS BASED ON ISO/IEC 27002

Miss. Nattaya Pikunkam

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2009

หัวข้อวิทยานิพนธ์	ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐาน ไอเอสโอ/ไออีซี 27002
โดย	นางสาวเนตยา พิกุลแกม
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.ญาใจ ลิ่มปิยะกรณ์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศาสตราจารย์ ดร.บุญเสริม กิจศิริกุล)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ญาใจ ลิ่มปิยะกรณ์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.วิษณุ โคตรจรัส)

..... กรรมการภายนอกมหาวิทยาลัย
(อาจารย์ ดร.ภาสกร อภิรักษ์วรพินิต)

เนตยา พิกุลแกม : ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐาน ไอเอสโอ/ไออีซี 27002. (A SYSTEM TO SUPPORT SECURE SOFTWARE DEVELOPMENT PROCESS BASED ON ISO/IEC 27002) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ.ดร.ญาใจ ลิ่มปิยะกรณ์, 123 หน้า.

การมีมาตรการรักษาความปลอดภัยระหว่างกระบวนการพัฒนาซอฟต์แวร์จะทำให้มั่นใจได้ว่า ซอฟต์แวร์ที่ได้พัฒนาขึ้นนั้นได้ผ่านการตรวจสอบ ติดตาม และประเมินผลตามนโยบาย หรือข้อบังคับต่างๆ ขององค์กรที่ได้กำหนดไว้ ทั้งยังช่วยป้องกันความผิดพลาดที่อาจเกิดขึ้นในระบบสารสนเทศ ได้แก่ การสูญหายของข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และต้องสามารถรักษาความลับของข้อมูล สามารถยืนยันตัวตนของผู้ส่งและผู้รับข้อมูลได้ งานวิจัยนี้จึงได้ออกแบบและพัฒนาระบบอำนวยความสะดวกให้องค์กรสามารถพัฒนาซอฟต์แวร์ได้อย่างปลอดภัย น่าเชื่อถือ โดยคำนึงถึงการรักษาความปลอดภัยในด้านต่างๆที่เกี่ยวข้องซึ่งอ้างอิงจากมาตรฐาน ไอเอสโอ/ไออีซี 27002

ภาควิชา : วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต เนตยา พิกุลแกม

สาขาวิชา : วิทยาศาสตร์คอมพิวเตอร์ ลายมือ อ.ที่ปรึกษาวิทยานิพนธ์หลัก

ปีการศึกษา : 2552

5071427421 : MAJOR COMPUTER SCIENCE

KEYWORDS : SECURITY / SOFTWARE DEVELOPMENT PROCESS /ISO/IEC 27002

NATTAYA PIKUNKAM : A SYSTEM TO SUPPORT SECURE SOFTWARE DEVELOPMENT PROCESS BASED ON ISO/IEC 27002. THESIS ADVISOR : ASST. PROF. YACHAI LIMPIYAKORN, Ph.D.,123pp.

The secure software development process would ensure that the software product has been inspected, monitored, and evaluated by the established policies or regulations of an organization. Additionally, it would prevent various faults such as data loss, and unauthorized access. IT systems are also expected to secure their data, or capable of authenticating data receivers and senders. This research work has designed and implemented a system to provide an organization of safe and reliable software development with the considerations of various security aspects described in ISO/IEC 27002 standard.

Department : Computer Engineering Student's Signature นัฐยา พิกุลแก้ม

Field of Study : Computer Science Advisor's Signature Y. Limpiyakorn

Academic Year : 2009

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความอนุเคราะห์อย่างดียิ่งของท่านผู้ช่วยศาสตราจารย์ ดร.ญาใจ ลิ่มปิยะกรณ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาให้ความรู้ ให้คำปรึกษา ตรวจสอบ ให้คำแนะนำแนวทางการวิจัย และสนับสนุนเป็นอย่างดี จนทำให้การวิจัยในครั้งนี้สำเร็จออกมาด้วยดี

ขอขอบพระคุณ ศาสตราจารย์ ดร.บุญเสริม กิจศิริกุล ผู้ช่วยศาสตราจารย์ ดร. วิษณุ โคตรจรัส และอาจารย์ ดร.ภาสกร อภิรักษ์วรพินิต กรรมการสอบวิทยานิพนธ์ ที่กรุณาเสียสละเวลา ให้คำแนะนำ ตรวจสอบ และแก้ไขวิทยานิพนธ์ฉบับนี้

ขอกราบขอบพระคุณ คุณพ่อ-คุณแม่ ที่ให้การสนับสนุนและเป็นกำลังใจที่ดีให้เสมอมา

ขอขอบคุณพี่ๆ ศูนย์คอมพิวเตอร์ มหาวิทยาลัยกรุงเทพ ที่ให้โอกาส ให้คำปรึกษา และให้การสนับสนุนเป็นอย่างดี

ท้ายที่สุด ผู้วิจัยขอขอบพระคุณเพื่อนๆ ทุกๆคน ที่คอยติดตามและให้กำลังใจ รวมถึงท่านอื่นๆ ที่มิได้กล่าวชื่อไว้ ณ ที่นี้ที่มีส่วนทำให้วิทยานิพนธ์สำเร็จได้ด้วยดี

สารบัญ

หน้า

สารบัญภาพ

หน้า

สารบัญตาราง

หน้า

หน้า

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน องค์กรต่างๆใช้ระบบสารสนเทศในการดำเนินงานทางธุรกิจกันมากขึ้น ซึ่งระบบสารสนเทศที่ใช้อาจได้จากการซื้อซอฟต์แวร์สำเร็จมาใช้ หรือว่าจ้างบริษัทที่ปรึกษาจัดทำระบบให้ หรือไม่ก็พัฒนาระบบสารสนเทศขึ้นมาเอง โดยอาศัยบุคลากรภายในองค์กรเป็นผู้พัฒนาระบบ หรืออาจผสมผสานกันในการที่จะได้มาซึ่งซอฟต์แวร์เพื่อนำมาใช้งาน แล้วแต่ความต้องการความเหมาะสมและงบประมาณขององค์กร

การพัฒนาระบบสารสนเทศขึ้นมาเพื่อใช้งานในองค์กรหรือเพื่อจำหน่ายให้กับองค์กรที่ว่าจ้างนั้น ปัจจัยหนึ่งที่ไม่ควรมองข้าม คือความปลอดภัยในกระบวนการพัฒนาซอฟต์แวร์ เนื่องจากเป็นปัจจัยสำคัญที่ก่อให้เกิดความเสียหายให้กับองค์กรได้ ไม่ว่าจะเป็นข้อมูลที่ใช้ในการประมวลผลระหว่างพัฒนา ซอร์สโค้ดที่พัฒนา ล้วนเป็นสินทรัพย์ที่มีค่าขององค์กรที่ใช้ในการพัฒนาซอฟต์แวร์ทั้งสิ้น หากมีผู้ไม่ประสงค์ดีได้ข้อมูลที่สำคัญต่างๆนี้ไป ล้วนไม่ส่งผลดีต่อองค์กรอย่างแน่นอน กระทบทั้งความน่าเชื่อถือ ทำให้คู่แข่งรู้จุดอ่อนขององค์กร ส่งผลให้ลูกค้าหมดความไว้วางใจในการให้พัฒนาซอฟต์แวร์และกระทบต่อความมั่นคงขององค์กร

วัฏจักรการพัฒนาซอฟต์แวร์ คือ กระบวนการในการพัฒนาระบบสารสนเทศ เพื่อตอบสนองความต้องการของผู้ใช้ รวมถึงช่วยแก้ปัญหาทางธุรกิจขององค์กรที่ใช้ระบบสารสนเทศนั้น โดยวัฏจักรการพัฒนาซอฟต์แวร์มีหลายรูปแบบ เช่น Waterfall Spiral Incremental เป็นต้น ซึ่งภายในกระบวนการประกอบด้วยหลายขั้นตอนเพื่อให้ได้มาซึ่งระบบซอฟต์แวร์ แบ่งออกเป็น Phase หลักๆ ได้แก่ การวางแผน (Planning) การวิเคราะห์ (Analysis) การออกแบบ (Design) การสร้าง (Construction) เป็นต้น

แม้ว่าในปัจจุบันจะมีระบบรักษาความปลอดภัยติดตั้งอยู่บนระบบเครือข่ายอยู่แล้ว เช่น ระบบ Firewall ระบบตรวจจับไวรัส เป็นต้น แต่ไม่ได้หมายความว่าระบบรักษาความปลอดภัยเหล่านั้นจะสามารถป้องกันและดูแลรักษาการทำงานที่เกิดขึ้นในระบบเครือข่ายได้ทั้งหมด อุปกรณ์ต่างๆ เหล่านั้นทำหน้าที่ในการป้องกันให้กับผู้ใช้งานเพื่อให้มั่นใจได้ว่าอย่างน้อยระบบยังมีความน่าเชื่อถือ และมีความปลอดภัยอยู่บ้าง แต่ในเรื่องของการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์นั้นมีอยู่หลายด้าน ที่ถือได้ว่ามีความสำคัญไม่แพ้กัน เช่น มาตรการรักษาความปลอดภัยที่เกี่ยวกับการพัฒนาซอฟต์แวร์ เป็นต้น เพื่อให้มั่นใจได้ว่า ซอฟต์แวร์ที่ได้พัฒนาขึ้นมานั้นมีความปลอดภัย ได้ผ่านการตรวจสอบ ติดตาม และประเมินผลมาตามนโยบาย หรือข้อบังคับ

ต่างๆ ขององค์กรที่ได้มีการกำหนดไว้ อีกทั้งยังช่วยป้องกันความผิดพลาดที่อาจจะเกิดขึ้นในระบบสารสนเทศ การสูญหายของข้อมูล หรือ เกิดการเปลี่ยนแปลงข้อมูลโดยที่ไม่ได้รับอนุญาต และต้องสามารถรักษาความลับของข้อมูล สามารถยืนยันตัวตนของผู้ส่งและผู้รับข้อมูลได้ ซึ่งสิ่งต่างๆ เหล่านี้เป็นสิ่งสำคัญและอาจส่งผลต่อองค์กรได้

ไอเอสโอ/ไออีซี 27002 เป็นมาตรฐานความมั่นคงปลอดภัย ซึ่งเดิมเป็นที่รู้จักกันในชื่อ ไอเอสโอ/ไออีซี 17799 Part 1 เป็นมาตรฐานและหลักการทั่วไปสำหรับการเริ่ม การสร้าง การบำรุงรักษา และการปรับปรุงการจัดการความปลอดภัยสารสนเทศในองค์กร วัตถุประสงค์ของการควบคุมและมาตรฐานสำหรับการควบคุมนี้ตั้งใจช่วยให้สามารถทำได้ตรงกับความต้องการที่กำหนดไว้ตามหลักการประเมินความเสี่ยง และมาตรฐานนี้จะเป็นแนวทางสำหรับการพัฒนามาตรฐานระบบรักษาความปลอดภัยให้กับองค์กร และช่วยในการบริหารระบบรักษาความปลอดภัยให้มีประสิทธิภาพ อีกทั้งยังช่วยสร้างการรักษาความลับของข้อมูลของกิจกรรมต่างๆ จึงเหมาะสมกับการควบคุมความปลอดภัยในกระบวนพัฒนาซอฟต์แวร์ ช่วยเพิ่มความมั่นใจให้กับองค์กรว่ากระบวนการดังกล่าวจะไม่ก่อให้เกิดหรือเพิ่มความเสี่ยงให้กับองค์กร [1]

งานวิจัยนี้จะเป็นการศึกษากระบวนการพัฒนาซอฟต์แวร์ รวมถึงความสัมพันธ์กับมาตรฐาน ไอเอสโอ/ไออีซี 27002 เพื่อพัฒนาระบบอำนวยความสะดวกให้องค์กรสามารถพัฒนาซอฟต์แวร์ได้อย่างปลอดภัย น่าเชื่อถือ โดยคำนึงถึงการรักษาความปลอดภัยในด้านต่างๆ ที่เกี่ยวข้องอ้างอิงมาตรฐาน ไอเอสโอ/ไออีซี 27002

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีจุดประสงค์เพื่อทำการพัฒนาระบบอำนวยความสะดวกให้กับองค์กรที่พัฒนาซอฟต์แวร์ เพื่อใช้สำหรับการควบคุมความปลอดภัยในกระบวนการพัฒนาซอฟต์แวร์ อ้างอิงตามมาตรฐาน ไอเอสโอ/ไออีซี 27002 พร้อมทั้งช่วยจัดการงานเอกสารต่างๆ ให้สะดวกรวดเร็ว ง่ายต่อการค้นคืน และเป็นกลไกหนึ่งในการควบคุมความปลอดภัยระหว่างกระบวนการพัฒนาซอฟต์แวร์

1.3 ขอบเขตของการวิจัย

1. ออกแบบกระแสงานของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย โดยระเบียบวิธีการควบคุมกระบวนการพัฒนาซอฟต์แวร์ที่ใช้ในระบบนี้จะอ้างอิงจากมาตรฐาน ไอเอสโอ/ไออีซี 27002 ในส่วนที่เกี่ยวข้องกับกระบวนการพัฒนาซอฟต์แวร์เท่านั้น โดย Phase ของกระบวนการพัฒนาซอฟต์แวร์จะถูกแบบออกเป็น 7 Phase เนื่องจากเพื่อให้เข้าใจถึงกระบวนการของการพัฒนาซอฟต์แวร์ได้ชัดเจนและละเอียดมากยิ่งขึ้น
2. ระบบที่พัฒนาขึ้นนี้จะมีความสามารถต่อไปนี้เป็นอย่างน้อย

- สามารถจัดการกับเอกสารที่เกิดขึ้นในกระบวนการพัฒนาซอฟต์แวร์ได้ (เช่น สามารถเรียกดู เพิ่ม แก้ไขและลบข้อมูลดังกล่าวได้)
- สามารถทำการจัดการและควบคุมสิทธิ์การเข้าถึงระบบและการใช้งานเอกสารต่างๆ ได้
- มีการควบคุมการทำงานโดยมีการสร้างรายการตรวจสอบและกระบวนการอนุมัติ เพื่อช่วยควบคุมกระบวนการของระบบสนับสนุนนี้
- สามารถเรียกดูประวัติการพัฒนาซอฟต์แวร์ต่างๆ ได้
- สามารถทำการติดตามการแก้ไขข้อบกพร่องที่ตรวจพบได้

3. ระบบที่พัฒนาขึ้นนี้จะถูกทดสอบโดยการนำไปใช้จริง แล้วนำผลที่ได้มาทำการประเมินเพื่อค้นหาข้อบกพร่องของระบบ และทำการปรับปรุงให้ดีขึ้น หรือนำเสนอเป็นข้อเสนอแนะ

1.4 ขั้นตอนและวิธีดำเนินการวิจัย

1. ศึกษาและทำความเข้าใจกระบวนการพัฒนาซอฟต์แวร์และแนวทางปฏิบัติตามมาตรฐานไอเอสโอ/ไออีซี 27002
2. ศึกษาและทำความเข้าใจมาตรฐานไอเอสโอ 27002 และงานวิจัยที่เกี่ยวข้อง
3. นำมาตรฐาน ไอเอสโอ/ไออีซี 27002 และงานวิจัยที่เกี่ยวข้อง มาประยุกต์ใช้เพื่อออกแบบขั้นตอนของกระบวนการพัฒนาซอฟต์แวร์โดยอิงตามมาตรฐาน ไอเอสโอ/ไออีซี 27002
4. พัฒนาระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์โดยอิงตามมาตรฐาน ไอเอสโอ/ไออีซี 27002
5. ทดสอบและประเมินผลระบบสนับสนุนกระบวนการที่นำเสนอ
6. สรุปผลการวิจัยและข้อเสนอแนะ
7. จัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ได้ระบบงานต้นแบบสำหรับกระบวนการพัฒนาซอฟต์แวร์อย่างปลอดภัยให้กับองค์กรที่พัฒนาซอฟต์แวร์ โดยระบบจะช่วยอำนวยความสะดวกแก่ผู้ที่เกี่ยวข้องในการจัดเก็บรวบรวมข้อมูลที่เกิดขึ้นในกระบวนการพัฒนาซอฟต์แวร์ภายใต้กลไกควบคุมความมั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ ไออีซี 27002

1.6 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์

วิทยานิพนธ์นี้แบ่งเนื้อหาออกเป็น 6 บทดังต่อไปนี้ บทที่ 1 เป็นบทนำซึ่งกล่าวถึง ความเป็นมาและความสำคัญของปัญหา รวมถึงวัตถุประสงค์ของการวิจัย บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้องในงานวิจัยนี้ บทที่ 3 กล่าวถึงการออกแบบขั้นตอนดำเนินงาน บทที่ 4 กล่าวถึงการพัฒนาระบบสนับสนุน บทที่ 5 กล่าวถึงการทดสอบระบบสนับสนุน บทที่ 6 กล่าวถึงการสรุปผลการวิจัยและข้อเสนอแนะ

1.7 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความวิจัยในหัวข้อเรื่อง “ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002” โดย เนตยา พิกุลแกม และ ญาใจ ลิ่มปิยะกรณ์ ในวารสารเทคโนโลยีและสื่อสารการศึกษา(ECT Journal) ฉบับที่ 5 ซึ่งตีพิมพ์โดยมหาวิทยาลัยสุโขทัยธรรมมาธิราช

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 วัฏจักรการพัฒนาซอฟต์แวร์ (Software Development Life Cycle : SDLC) - [6]

SDLC คือ โครงร่างสำหรับการพัฒนาซอฟต์แวร์ให้สำเร็จ ซึ่งได้ถูกสร้างจากวิธีการต่างๆ ที่พัฒนาขึ้นมา โดยขั้นตอนพื้นฐานที่มี ดังนี้

1. การเริ่มต้นโครงการและกำหนดความต้องการด้านหน้าที่ (Project initiation and functional requirements definition)

เป็นระยะเริ่มต้นของโครงการ ความต้องการทางด้านธุรกิจจะถูกกำหนดโดยเป็นไปตามจุดประสงค์ การระบุจุดประสงค์จะต้องเป็นไปตามกลยุทธ์ทางด้านธุรกิจหรือเรียกว่า กลยุทธ์ของสารสนเทศ และกลยุทธ์ด้านความปลอดภัย

2. ข้อกำหนดการออกแบบระบบ (System design specifications)

เป็นระยะที่รวมทุกกิจกรรมที่เกี่ยวข้องกับการออกแบบระบบ เช่น สถาปัตยกรรมระบบ ผลลัพธ์ของระบบ และส่วนต่อประสานของระบบที่ถูกออกแบบ ขณะที่ข้อมูลนำเข้า การไหลของข้อมูล และความต้องการผลลัพธ์จะถูกสร้างขึ้น

3. สร้าง/พัฒนา และ การทำเอกสาร (Build (develop) and documentation)

เป็นระยะที่ซอร์สโค้ดถูกพัฒนาขึ้น เหตุการณ์ทดสอบ กรณีทดสอบ ถูกพัฒนาขึ้น รวมถึงการทดสอบระบบย่อยและระบบรวมจะถูกสร้างขึ้น โปรแกรมและระบบจะถูกบันทึกเพื่อบำรุงรักษาและเพื่อกลับไปแก้ไขเพื่อการทดสอบการยอมรับระบบและผลลัพธ์

4. การยอมรับระบบที่พัฒนา (Acceptance)

ในระยะการยอมรับระบบนี้ นักพัฒนาจะทำการทดสอบข้อมูลและทดสอบโค้ดอย่างเป็นอิสระต่อกัน เพื่อให้มั่นใจว่ามันจะสามารถทำหน้าที่ได้ตามสภาพแวดล้อมขององค์กรและทำงานได้ตรงตามหน้าที่ที่ต้องการ ผู้จัดการจะต้องมั่นใจว่าความต้องการและเกณฑ์สำหรับยอมรับระบบของแอพพลิเคชันใหม่นี้ได้ถูกกำหนดไว้อย่างชัดเจน เป็นไปตามที่ตกลง และมีการบันทึกและทดสอบ

5. นำไปใช้จริง (Transition to production (installation))

ระยะนี้ระบบได้ถูกจัดส่งมาจากระยะการยอมรับระบบที่พัฒนาเพื่อนำระบบไปสู่สภาพแวดล้อมการใช้งานจริง กิจกรรมต่างๆในระยะนี้จะมีการอบรมผู้ใช้งานใหม่ ซึ่งต้องเป็นไปตามตารางการอบรมที่สร้างขึ้น รวมถึงการติดตั้งระบบ การแปลงข้อมูล

6. บำรุงรักษา (Operations and maintenance support (Post installation))

ระยะนี้ระบบจะถูกใช้งานจากองค์กร กิจกรรมที่เกี่ยวข้องกับระยะนี้ก็คือการเฝ้าระวังติดตามประสิทธิภาพของระบบและต้องมั่นใจได้ว่าการดำเนินงานจะเป็นไปได้อย่างต่อเนื่อง รวมถึงการป้องกันข้อเสียหายหรือจุดอ่อน การจัดการและป้องกันปัญหาของระบบ การกู้คืนระบบจากปัญหาของระบบ และการสร้างการเปลี่ยนแปลงของระบบ

7. จัดการแทนที่ระบบ (System Replacement (disposal))

เป็นระยะสุดท้ายใน SDLC จะเป็นการจัดเตรียมสำหรับการแทนที่ระบบ โดยเมื่อระบบสารสนเทศกำลังหมดสภาพการใช้งานไป หรือไม่ได้ใช้เป็นระยะเวลานาน จะต้องมั่นใจได้ว่าทรัพยากรและทรัพย์สินขององค์กรนี้จะถูกป้องกัน โดยเจ้าของแอพพลิเคชันจะเก็บข้อมูลที่สำคัญไว้ และลบทิ้งสื่อที่บันทึกข้อมูลนั้น แล้วจึงทำลายฮาร์ดแวร์/ซอฟต์แวร์นั้น

2.1.2 **มาตรฐานความมั่นคงปลอดภัย ไอเอสโอ/ไออีซี** 27002

มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย โดยแบ่งเนื้อหาออกเป็น 11 โดเมน ซึ่งแต่ละโดเมนประกอบไปด้วยวัตถุประสงค์จำนวนแตกต่างกัน รวมแล้วจำนวน 39 วัตถุประสงค์การควบคุม (Control Objective) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความมั่นคงปลอดภัยแตกต่างกัน รวมแล้วจำนวน 133 การควบคุม (Controls) ซึ่งสามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กรได้ [2]

โดยมาตรฐานนี้จะเน้นที่วิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ไอเอสโอ/ไออีซี 27001 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบ โดยแบ่งเป็นหัวข้อหลักที่เกี่ยวข้องกับระบบ และให้แนวทางว่าผู้จัดทำควรปฏิบัติอย่างไร ซึ่งผู้ใช้สามารถเพิ่มเติมมาตรการหรือใช้วิธีการที่มีความมั่นคงปลอดภัยเพียงพอ หรือเหมาะสมตามที่องค์กรได้ประเมินไว้ [2]

รายละเอียดของโดเมนหลักในมาตรฐาน ไอเอสโอ/ไออีซี 27002 มีดังนี้ [5]

1) นโยบายความมั่นคงปลอดภัย (Security policy)

ประกอบด้วยวัตถุประสงค์การควบคุม 1 ข้อย่อย ดังนี้

- นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

2) การจัดระเบียบความมั่นคงปลอดภัยสารสนเทศ (Organization of information security)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 2 ข้อย่อย ดังนี้

- การจัดระเบียบภายใน (Internal organization)
- หน่วยงานภายนอก (External parties)

3) การบริหารจัดการสินทรัพย์ (Asset management)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 2 ข้อย่อย ดังนี้

- หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for assets)
- การจำแนกประเภทสารสนเทศ (Information classification)

4) ความมั่นคงปลอดภัยทรัพยากรบุคคล (Human resources security)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 3 ข้อย่อย ดังนี้

- ก่อนการจ้างงาน (Prior to employment)
- ระหว่างการจ้างงาน (During employment)
- การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination or change of employment)

5) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 2 ข้อย่อย ดังนี้

- บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)
- ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and operations management)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 10 ข้อย่อย ดังนี้

- ขั้นตอนการดำเนินงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)
- การบริหารจัดการการส่งมอบงานบริการของหน่วยงานภายนอก (Third party service delivery management)
- การวางแผนและการตรวจรับระบบ (System planning and acceptance)

- การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)
- การสำรองข้อมูล (Back-up)
- การบริหารจัดการความมั่นคงปลอดภัยเครือข่าย (Network security management)
- การจัดกระทำสื่อที่ใช้บันทึกข้อมูล (Media handling)
- การแลกเปลี่ยนสารสนเทศ (Exchange of information)
- บริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)
- การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

7) <u>การควบคุมการเข้าถึง</u> (Access Control)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 7 ข้อย่อย ดังนี้

- ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)
- การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)
- หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)
- การควบคุมการเข้าถึงเครือข่าย (Network access control)
- การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)
- การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)
- การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

8) <u>การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ</u> (Information systems acquisition, development and maintenance)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 6 ข้อย่อย ดังนี้

- ความต้องการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Security requirements of information systems)
- การทำกระบวนการที่ถูกต้องในแอพพลิเคชัน (Correct processing in applications)
- การควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)
- ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of systems files)

- ความมั่นคงปลอดภัยในการพัฒนาและกระบวนการสนับสนุน (Security in development and support processes)
- การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Information security incident management)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 2 ข้อย่อย ดังนี้

- การรายงานเหตุการณ์และจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events and weaknesses)
- การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

10) การจัดการลักษณะความมั่นคงปลอดภัยสารสนเทศของการบริหารความต่อเนื่องของธุรกิจ (Information security aspects of business continuity management)

ประกอบด้วยวัตถุประสงค์การควบคุม 1 ข้อย่อย ดังนี้

- หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร

11) การปฏิบัติตามข้อกำหนด (Compliance)

ประกอบด้วยวัตถุประสงค์การควบคุมทั้งหมด 3 ข้อย่อย ดังนี้

- การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)
- การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)
- การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 Guidelines for Secure Software Development [4]

งานวิจัยนี้เป็นการเสนอข้อแนะนำในการออกแบบและพัฒนาซอฟต์แวร์โดยกำหนดกลุ่มของข้อแนะนำสำหรับการพัฒนาซอฟต์แวร์อย่างปลอดภัย โดยข้อเสนอแนะนี้ได้สร้างบนพื้นฐานของมาตรฐานต่างๆ ที่ได้รับการยอมรับ และข้อปฏิบัติที่ดีที่สุด และกลุ่มของกระบวนการถูกพัฒนาโดยผู้เกี่ยวข้องหลัก ซึ่งงานวิจัยชิ้นนี้ได้แบ่งพื้นที่สำหรับการแนะนำออกเป็นออกเป็น 3 พื้นที่หลัก ดังนี้

(1) จัดการกระบวนการพัฒนาซอฟต์แวร์ (Managing the software development process)

โดยแบ่งเป็นหัวข้อย่อย 4 หัวข้อ ดังนี้

- Integrate Security into the SDLC
- Define Security Roles
- Provide Security Education and Training
- Perform Risk Management

(2) ส่วนประกอบต่างๆในกระบวนการพัฒนาซอฟต์แวร์ (Elements in the software development process)

โดยแบ่งเป็นหัวข้อย่อย 1 หัวข้อ ดังนี้

- Define Security Requirements

(3) ฟังก์ชันความมั่นคงปลอดภัยที่ถูกสร้างในแอพพลิเคชัน (Security function to be built into applications)

2.2.2 Integrating ISO 17799 into your Software Development Lifecycle [6]

บทความนี้เป็นการนำเสนอการเชื่อมโยงในส่วนความมั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 17799:2005 ที่ควรคำนึงถึงใน SDLC เช่น ในกระบวนการพัฒนาซอฟต์แวร์ Phase การสร้าง/พัฒนา และ การทำเอกสาร กิจกรรมด้านความมั่นคงปลอดภัยที่ควรปฏิบัติไปพร้อมกับการพัฒนาซอฟต์แวร์ เช่น การพัฒนาซอร์สโค้ดต้องปลอดภัยจากการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต รวมถึงต้องมีการรักษาความลับของข้อมูล เช่น การเข้ารหัสข้อมูล เป็นต้น ซึ่งในมาตรฐาน 17799 หัวข้อที่เกี่ยวข้องกับเรื่องดังกล่าว คือ หัวข้อ ที่ 12.3 และ 12.4 ในเรื่องการสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ และเรื่องมาตรการการเข้ารหัสข้อมูล เป็นต้น ดังนั้นจึงเกิดการเชื่อมโยงดังกล่าวขึ้น ดังตารางที่ 1 โดยผู้วิจัยได้นำการเชื่อมโยงกิจกรรมความปลอดภัยดังกล่าวมาเป็นข้อมูลเพื่อการวิเคราะห์กิจกรรมและเอกสารที่ควรเกิดขึ้นในกระบวนการพัฒนาซอฟต์อย่างปลอดภัย

ตารางที่ 1 การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 17799:2005 กับ SDLC

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
Project Initiation and Functional Requirements Definition	Identify business needs Identify areas affected and Responsibilities Develop functional requirements Propose technical solution Evaluate alternatives Document project's objectives, scope, strategies, costs and schedule Select / approve approach Prepare project plan Prepare preliminary test plan Select acquisition strategy Establish formal functional baseline	Determine security requirement Classification and criticality of information /applications Identify legal, statutory and contractual requirements Initial Risk Analysis Cost / benefit analysis Preliminary contingency planning Prepare a security evaluation plan Include security requirements in the security base-line as well as in request for proposal and contracts Determine SLAs Document security framework	5.1.1 – Security Policy 7.x – Asset management and information classification 6.1.1, 6.1.2, 6.1.3 – Organization of Information Security 12.1 – Security requirements of information systems 6.2.3 – Addressing security in third party agreements 15.1 – Compliance with legal requirements 14.1.3 – Business Continuity Management

ตารางที่ 1 การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 17799:2005 กับ SDLC

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
System Design Specifications	Develop detailed design (system architecture, system outputs and system inter-faces). Detail the solution's interactions with external systems. Update testing goals and plans. Establish data input, data flow and output requirements. Establish formal baseline/ quality controls and requirements	Identification of Risks related to external parties. Define access control strategy Define security specifications (program, database, hardware, firmware and network) Develop security test procedure Include security area in formal baseline documentation and quality assurances	11.1 – Business requirement for access Control 6.2.1 – Identification of risks related to external parties 10.8.1 – Information ex-change policies and procedure 10.3.1 – Capacity management

ตารางที่ 1 (ต่อ) การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 17799:2005 กับ SDLC

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
Build/Development and Documentation	Contract source code from detailed design specifications. Perform and evaluate unit tests. Implement detailed design into final system	Write or procure and install security-related code. Control access to code. Evaluate security-related code. Ensure approved security components in formal baseline are included.	12.2.x – Correct processing in Applications 12.3.x – Cryptographic controls 12.4.x – Security of System Files
Acceptance	Test system components Validate system performance. Install system. Prepare project manuals. Perform acceptance test. Accept system	Sanitize test data. Independent security tests. Install security code with necessary modifications. Document security controls.	10.3.2 – System acceptance 12.6.1 – Technical vulnerability management 10.1.4 – Separation of development, test and operational facilities.

ตารางที่ 1 (ต่อ) การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 17799:2005 กับ SDLC

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
Transition to Production (implementation)	Train new users according to implementation Implement the system (installation, data conversion…).	Control data conversion and data entry. Reconcile and validate data integrity. Enforce segregation of duties and segregation of environments.	12.5.1 – Change control procedures 10.1.3 – Segregation of duties 10.1.4 – Separation of development, test and operational facilities.
Operations and Maintenance Support (post-installation)	Monitoring performance. Ensuring continuity of operations. Detect weakness or defects. Manage and prevent system problems. Recover from system problems. Implement system changes.	Periodic risk analysis. Change management. Verify compliance with applicable SLAs and security baselines. Maintain release integrity with secure and controlled environments.	10.10.x – Monitoring 12.5.2 - Technical review of applications after operating system changes 10.6.x – Network security management 11.x – Access control 15.2.2 – Technical

ตารางที่ 1 (ต่อ) การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 17799:2005 กับ SDLC

SDLC Phases	Project Activities	Parallel Security Activities	ISO 17799:2005 mapping
			compliance checking 15.3.x – Information systems audit considerations 10.1.1 – documented operating procedures 12.4.1 – Control of operational software 10.4.x – Protection against malicious and mobile code
System Replacement Disposal	Hardware and Software disposal	Information preservation. Media sanitization.	9.2.6 – Secure disposal or reuse of equipment 9.2.7 – Removal of property

บทที่ 3

การออกแบบขั้นตอนการดำเนินงาน

งานวิจัยนี้มีแนวคิดที่จะนำเสนอขั้นตอนของกระบวนการพัฒนาซอฟต์แวร์อย่างปลอดภัย รวมถึงออกแบบและพัฒนาระบบสนับสนุนการรักษาความปลอดภัยในกระบวนการพัฒนาซอฟต์แวร์โดยอ้างอิงตามมาตรฐาน ไอเอสโอ/ไออีซี 27002 เฉพาะในส่วนที่เกี่ยวข้องกับกระบวนการพัฒนาซอฟต์แวร์โดยตรงเท่านั้น ซึ่งระบบที่พัฒนาขึ้นจะมีฟังก์ชันการทำงานดังต่อไปนี้

3.1 การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย

ระบบจะมีการควบคุมกระบวนการพัฒนาซอฟต์แวร์ในแต่ละขั้นตอนของกระบวนการ โดยระบุสิ่งที่จำเป็นต้องจัดขึ้น ผู้เกี่ยวข้อง สิ่งที่ต้องควบคุม และเอกสารที่ต้องมีเพื่อเป็นหลักฐานด้านความปลอดภัย

ผู้วิจัยจะแบ่งผู้ที่เกี่ยวข้องกับกระบวนการพัฒนาซอฟต์แวร์ตามบทบาทต่าง ๆ ดังนี้ [5]

- ผู้บริหารองค์กร คือ พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์กร
- ผู้บริหารสารสนเทศ คือ พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการและมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในองค์กร
- ผู้ดูแลระบบ คือ พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น
- ผู้พัฒนาระบบ คือ พนักงานที่ได้รับมอบหมายให้มีหน้าที่พัฒนาซอร์สโค้ด
- หัวหน้างานสารสนเทศ คือ พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์กร และรายงานต่อผู้บริหารสารสนเทศ

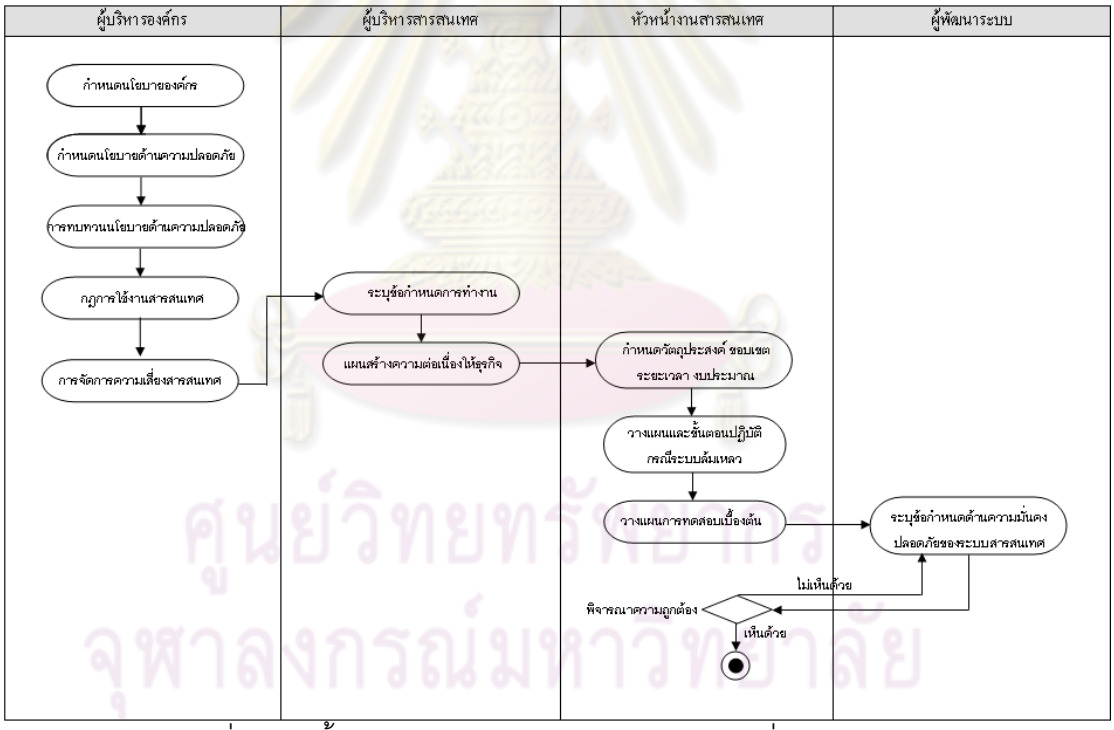
หลังจากนั้น ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์อย่างปลอดภัยจะถูกพัฒนาขึ้นตามขั้นตอนการดำเนินงานที่ได้ออกแบบไว้ ยกตัวอย่างขั้นตอนการดำเนินงานที่สำคัญ ดังนี้

ในเฟสของการเริ่มต้นโครงการ กิจกรรมที่ควรเกิดขึ้นและควบคุมเพื่อความมั่นคงปลอดภัยของกระบวนการนี้ตามมาตรฐานไอเอสโอ/ไออีซี 27002 จะประกอบไปด้วย

1. กำหนดนโยบายองค์กร

2. กำหนดนโยบายด้านความปลอดภัย
3. การทบทวนนโยบายด้านความปลอดภัย
4. กำหนดกฎการใช้งานสารสนเทศ
5. การจัดการความเสี่ยงสารสนเทศ
6. ระบุข้อกำหนดการทำงาน
7. กำหนด แผนสร้างความต่อเนื่องทางธุรกิจ
8. กำหนดวัตถุประสงค์ ขอบเขต ระยะเวลา งบประมาณ
9. วางแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว
10. วางแผนการทดสอบเบื้องต้น
11. ระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ซึ่งจากการรวบรวมกิจกรรมที่ต้องเกิดขึ้นในเฟสนี้ทั้งหมดแล้วนั้น งานวิจัยนี้ได้ออกแบบขั้นตอนของกระบวนการที่เหมาะสมได้ดังรูปนี้



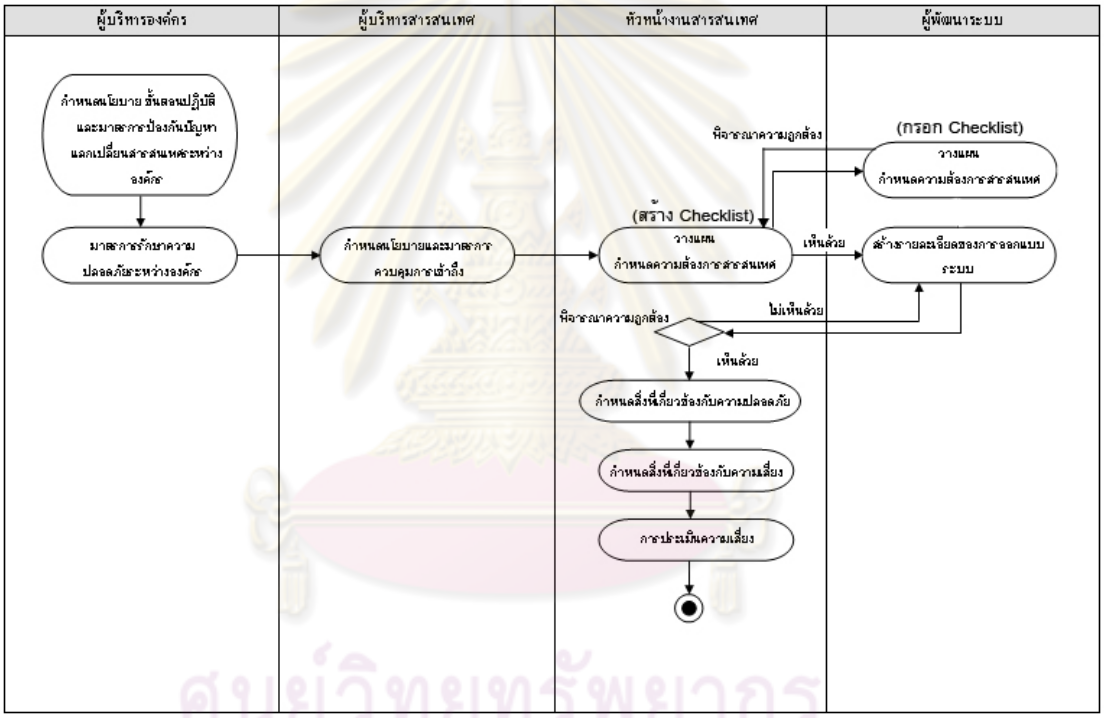
รูปที่ 1 ภาพขั้นตอนการทำงานของ SDLC เฟสการเริ่มต้นโครงการ

ในเฟสของการออกแบบระบบ กิจกรรมที่ควรเกิดขึ้นและต้องควบคุมเพื่อความมั่นคงปลอดภัยของกระบวนการนี้ ตามมาตรฐานไอเอสโอ/ไออีซี 27002 นั้น จะประกอบไปด้วย

1. กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร

2. กำหนดมาตรการรักษาความปลอดภัยระหว่างองค์กร
3. กำหนดนโยบายและมาตรการควบคุมการเข้าถึง
4. วางแผนกำหนดความต้องการสารสนเทศ
5. สร้างรายละเอียดของการออกแบบระบบ
6. กำหนดสิ่งที่เกี่ยวข้องกลับความปลอดภัย
7. กำหนดสิ่งที่เกี่ยวข้องกับความเสี่ยง
8. การประเมินความเสี่ยง

ซึ่งจากการรวบรวมกิจกรรมที่ต้องเกิดขึ้นในเฟสนี้ทั้งหมดแล้วนั้น งานวิจัยนี้ได้ออกแบบขั้นตอนของกระบวนการที่เหมาะสมได้ดังรูปนี้



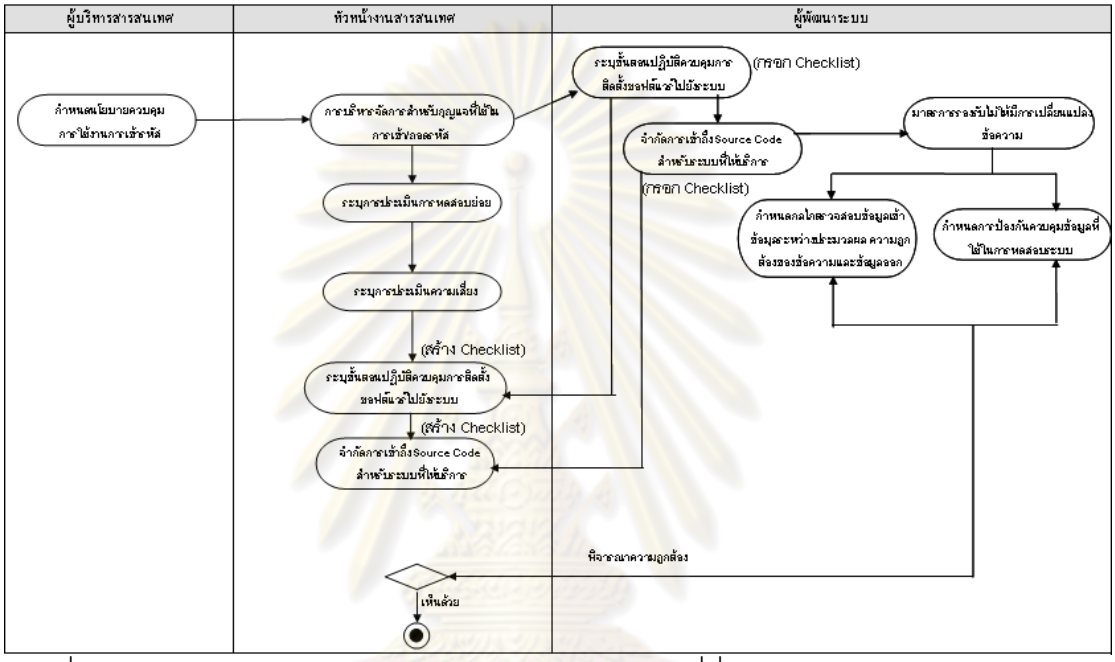
รูปที่ 2 แผนภาพกิจกรรมของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย ระยะออกแบบระบบ

สิ่งที่ถูกตรวจสอบหลักในกระบวนการที่ 3 (สร้าง/พัฒนา และการทำเอกสาร)

1. กำหนดนโยบายควบคุมการใช้งานงานเข้ารหัส
2. การบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส
3. ระบุการประเมินการทดสอบย่อย
4. ระบุการประเมินความเสี่ยง
5. ระบุขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ
6. กำหนดมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ

7. กำหนดกลไกตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก
8. กำหนดการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ

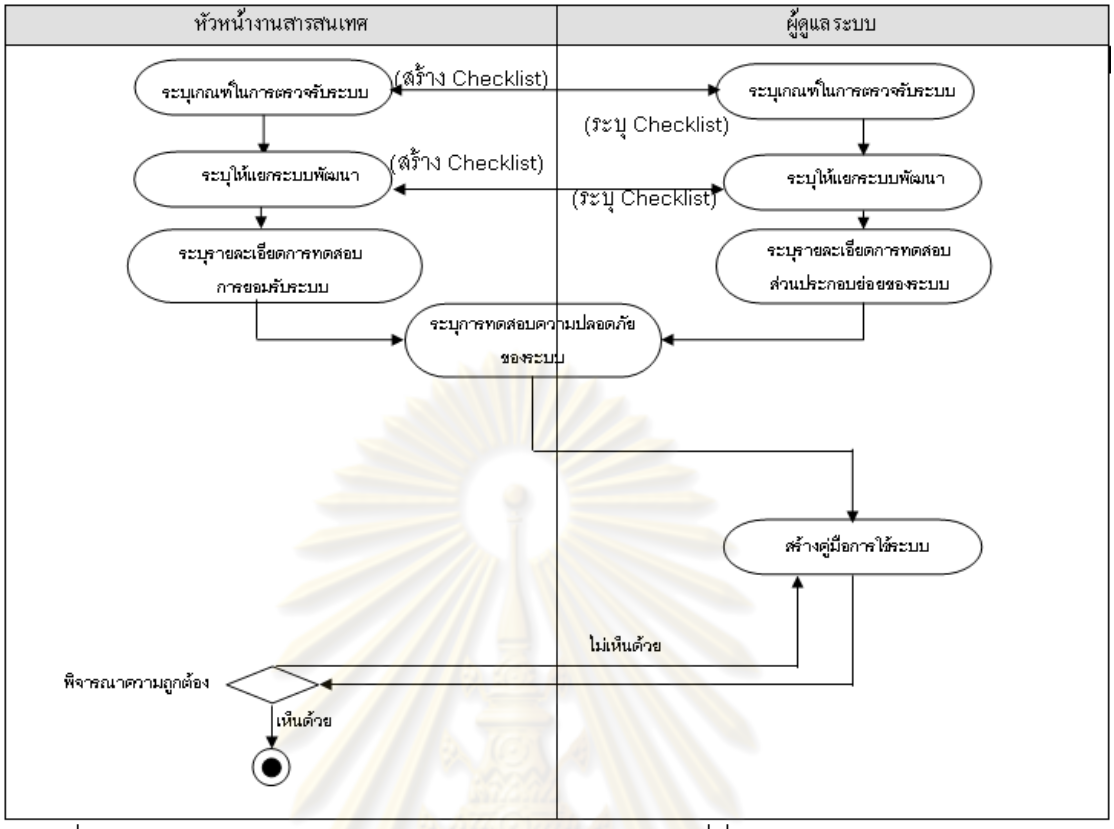
ซึ่งจากการรวบรวมกิจกรรมที่ต้องเกิดขึ้นในเฟสนี้ทั้งหมดแล้วนั้น งานวิจัยนี้ได้ออกแบบขั้นตอนของกระบวนการที่เหมาะสมได้ดังรูปนี้



รูปที่ 3 แผนภาพกิจกรรมของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย ระยะพัฒนาระบบ

สิ่งที่ถูกตรวจสอบหลักในกระบวนการที่ 4 (การยอมรับระบบที่พัฒนา)

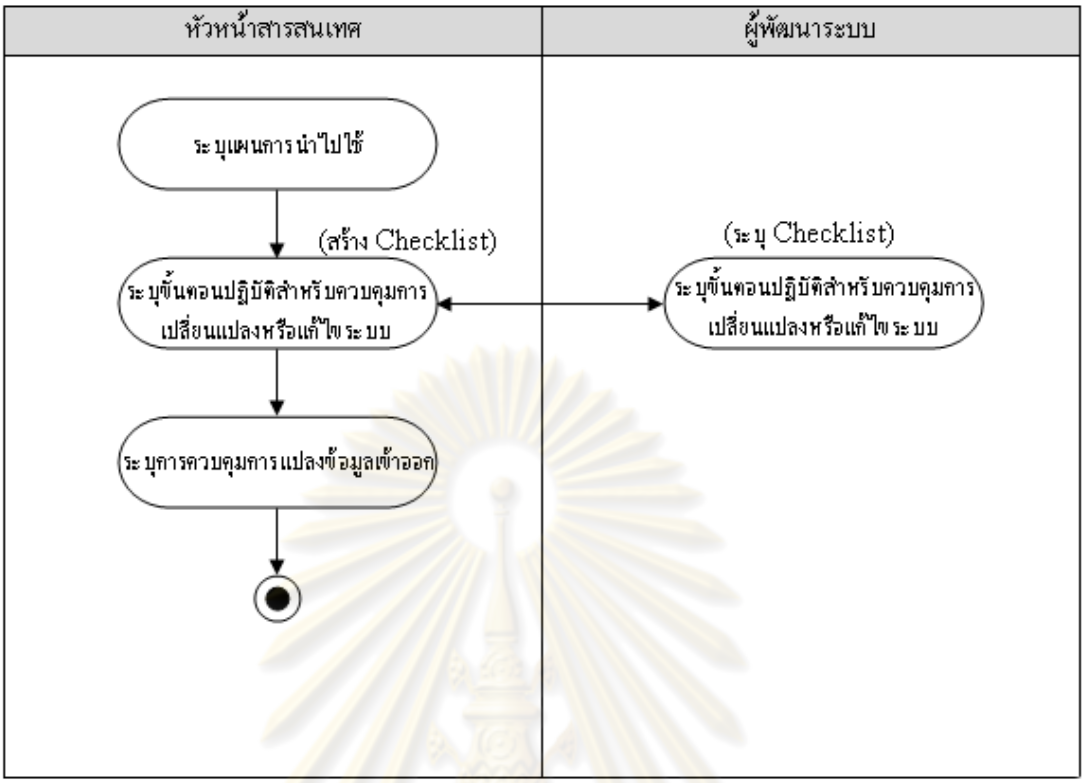
1. กำหนดมาตรการรองรับความเสี่ยง
2. ระบุเกณฑ์ในการตรวจรับระบบ
3. ระบุรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ
4. ระบุการทดสอบความปลอดภัยของระบบ
5. สร้างคู่มือการใช้ระบบ



รูปที่ 4 แผนภาพกิจกรรมของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย ระยะการยอมรับระบบ

สิ่งที่ถูกตรวจสอบหลักในกระบวนการที่ 5 (นำไปใช้จริง)

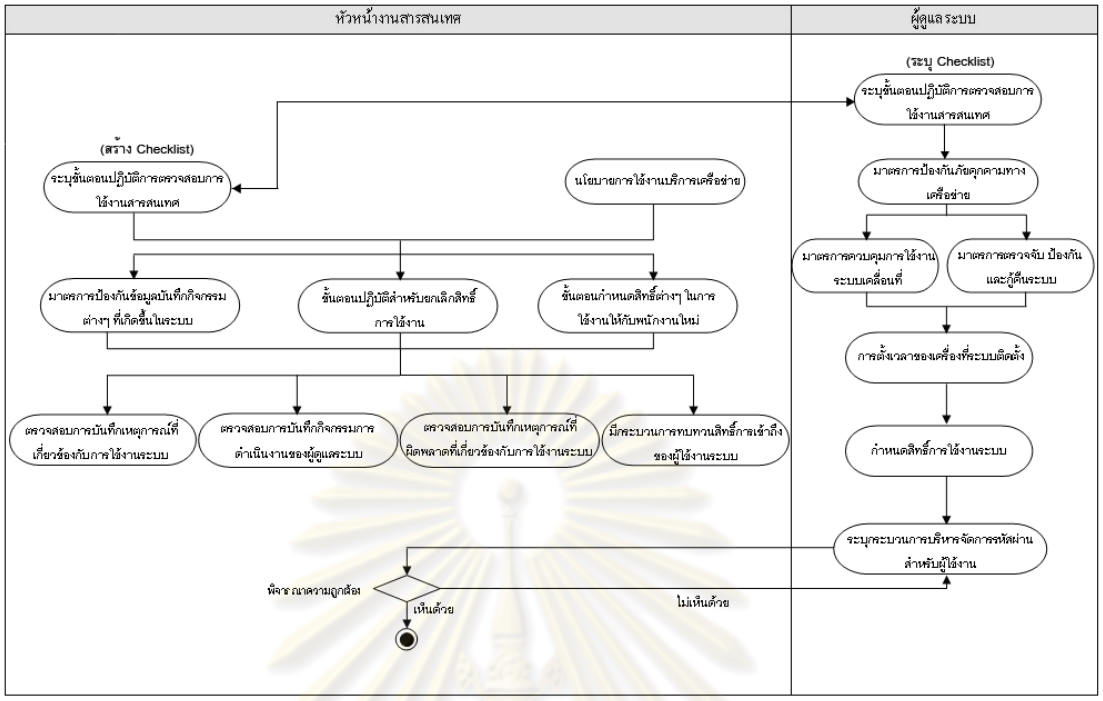
1. แผนการนำไปใช้
2. ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ
3. การควบคุมการแปลงข้อมูลเข้า/ออก



รูปที่ 5 แผนภาพกิจกรรมของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย ระยะการนำไปใช้จริง

สิ่งที่ถูกตรวจสอบหลักในกระบวนการที่ 6 (บำรุงรักษา)

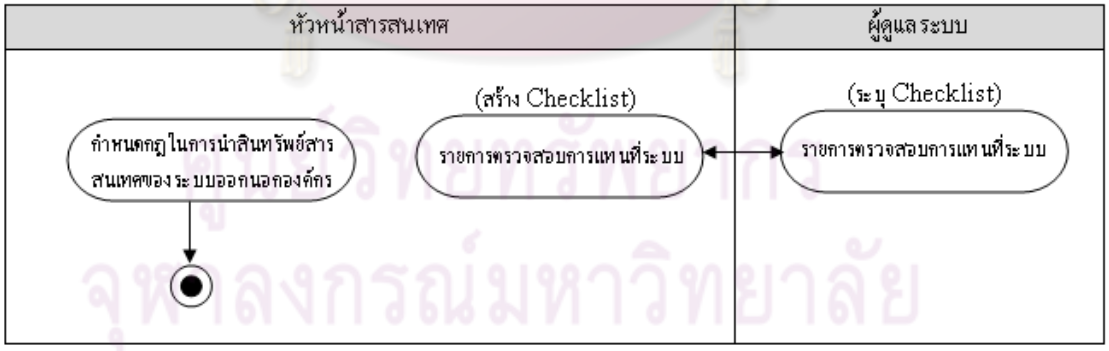
1. ระบุขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ
2. กำหนดนโยบายการใช้งานการบริการเครือข่าย
3. กำหนดมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆที่เกิดขึ้นในระบบ
4. กำหนด/ยกเลิก/ทบทวนสิทธิ์การใช้งาน
5. มีการตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ การดำเนินงานของผู้ดูแลระบบ เหตุการณ์ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ
6. กำหนดมาตรการป้องกันภัยคุกคามทางเครือข่าย
7. กำหนดมาตรการควบคุมการใช้งานระบบเคลื่อนที่
8. กำหนดมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ
9. ตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง
10. ระบุกระบวนการบริหารจัดการรหัสผ่าน



รูปที่ 6 แผนภาพกิจกรรมของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย ระยะบำรุงรักษาระบบ

สิ่งที่ถูกตรวจสอบหลักในกระบวนการที่ 7 (จัดการแทนที่ระบบ)

1. การกำหนดกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร
2. รายการตรวจสอบการแทนที่ระบบ



รูปที่ 7 แผนภาพกิจกรรมของกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย ระยะจัดการแทนที่ระบบ

จากการวิเคราะห์เพื่อหากิจกรรมและเอกสารที่ควรเกิดขึ้นทั้งหมดเพื่อความปลอดภัยในกระบวนการพัฒนาซอฟต์แวร์ ผู้วิจัยได้เชื่อมโยงกับมาตรฐาน ไอเอสโอ/ไออีซี 27002 เพื่อระบุว่า

กิจกรรมและเอกสารที่เกิดขึ้นนั้นตรงตามข้อระบุในมาตรฐาน ไอเอสโอ/ไออีซี 27002 ข้อใดบ้าง ดังตารางที่ 2

ตารางที่ 2 การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 27002

SDLC Phases	Activities	ISO/IEC 27002 mapping
1. ระยะเริ่มต้นโครงการ	กำหนดนโยบายองค์กร กำหนดนโยบายด้านความปลอดภัย การทบทวนนโยบายด้านความปลอดภัย กำหนดกฎการใช้งานสารสนเทศ การจัดการความเสี่ยงสารสนเทศ ระบุข้อกำหนดการทำงาน กำหนด แผนสร้างความต่อเนื่องทางธุรกิจ กำหนดวัตถุประสงค์ ขอบเขต ระยะเวลา งบประมาณ วางแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว วางแผนการทดสอบเบื้องต้น ระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	5.1.1 – Security Policy 5.1.2 – Review of the information security policy 6.1.1, 6.1.2, 6.1.3 – Organization of Information Security 12.1 – Security requirements of information systems 6.2.3 – Addressing security in third party agreements 14.1.3 – Business Continuity Management

ตารางที่ 2 (ต่อ) การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 27002

SDLC Phases	Activities	ISO/IEC 27002 mapping
2. ระยะออกแบบระบบ	กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร กำหนดมาตรการรักษาความปลอดภัยระหว่างองค์กร กำหนดนโยบายและมาตรการควบคุมการเข้าถึง วางแผนกำหนดความต้องการสารสนเทศ สร้างรายละเอียดของการออกแบบระบบ กำหนดสิ่งที่เกี่ยวข้องกลับความปลอดภัย กำหนดสิ่งที่เกี่ยวข้องกับความเสี่ยงและการประเมินความเสี่ยง	11.1 – Business requirement for access Control 6.2.1 – Identification of risks related to external parties 10.8.1 – Information exchange policies and procedure 10.3.1 – Capacity management

ตารางที่ 2 (ต่อ) การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 27002

SDLC Phases	Activities	ISO/IEC 27002 mapping
3. ระยะพัฒนา	กำหนดนโยบายควบคุมการใช้งานงานเข้ารหัส การบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส ระบุการประเมินการทดสอบย่อย ระบุการประเมินความเสี่ยง ระบุขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ กำหนดมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ กำหนดกลไกตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก กำหนดการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ	12.2.x – Correct processing in Applications 12.3.x – Cryptographic controls 12.4.x – Security of System Files
4. ระยะการยอมรับระบบ	กำหนดมาตรการรองรับความเสี่ยง ระบบเกณฑ์ในการตรวจรับระบบ ระบุรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ ระบุการทดสอบความปลอดภัยของระบบ สร้างคู่มือการใช้ระบบ	10.3.2 – System acceptance 12.6.1 – Technical vulnerability management 10.1.4 – Separation of development, test and operational facilities.

ตารางที่ 2 (ต่อ) การเชื่อมโยงมาตรฐาน ไอเอสโอ/ไออีซี 27002

SDLC Phases	Activities	ISO/IEC 27002 mapping
5. ระยะการนำไปใช้จริง	ระบุแผนการนำไปใช้ ระบุขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ ระบุการควบคุมการแปลงข้อมูลเข้า/ออก	12.5.1 – Change control procedures 10.1.4 – Separation of development, test and operational facilities
6. ระยะบำรุงรักษา	ระบุขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ กำหนดนโยบายการใช้งานการบริการเครือข่าย กำหนดมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆที่เกิดขึ้นในระบบ กำหนด/ยกเลิก/ทบทวนสิทธิ์การใช้งาน มีการตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ การดำเนินงานของผู้ดูแลระบบ เหตุการณ์ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ กำหนดมาตรการป้องกันภัยคุกคามทางเครือข่าย กำหนดมาตรการควบคุมการใช้งานระบบเคลื่อนที่ กำหนดมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ ตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง ระบุกระบวนการบริหารจัดการรหัสผ่าน	10.10.x – Monitoring 12.5.2 - Technical review of applications after operating system changes 10.6.x – Network security management 11.x – Access control 10.1.1 – Documented operating procedures 10.4.x – Protection Against malicious and mobile code
7. ระยะจัดการแทนที่ระบบ	กำหนดกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร รายการตรวจสอบการแทนที่ระบบ	9.2.6 – Secure disposal or reuse of equipment 9.2.7 – Removal of property

3.2 การจัดการเอกสารที่ใช้ในการควบคุมกระบวนการพัฒนาซอฟต์แวร์

เป็นการอำนวยความสะดวกให้กับผู้ใช้งานในการจัดการด้านเอกสาร โดยเอกสารที่ระบบมีให้ ได้แก่ เอกสารที่ต้องถูกควบคุมความปลอดภัย ข้อแนะนำในการควบคุมความปลอดภัยของแต่ละขั้นตอนของกระบวนการพัฒนาซอฟต์แวร์ ซึ่งระบบจะทำหน้าที่เป็นตัวควบคุมการเรียกใช้งานเอกสารดังกล่าว (ผู้เกี่ยวข้องเท่านั้นจึงจะสามารถเข้าถึงและแก้ไขได้เฉพาะหัวข้อที่ได้รับผิดชอบ)

3.3 ประวัติการพัฒนาซอฟต์แวร์ขององค์กร

ระบบจะช่วยอำนวยความสะดวกให้กับหัวหน้าสารสนเทศในส่วนของการเรียกดูประวัติการพัฒนาซอฟต์แวร์ย้อนหลัง โดยเลือกดูตามรายปีที่ต้องการหรือเลือกดูตามกลุ่มประเภทเป้าหมายของผู้ใช้ซอฟต์แวร์นั้น เช่น สำหรับอาจารย์ สำหรับนักศึกษา เป็นต้น

จากการศึกษากระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 ผู้วิจัยได้ทำการสรุปและออกแบบขั้นตอนการดำเนินงานของกระบวนการดังกล่าว ดังเช่นรูปที่ 1 และ 2 เป็นต้น โดยขั้นตอนการดำเนินงานนี้จะแสดงการไหลของข้อมูลและกระบวนการทำงานอย่างเป็นลำดับขั้นตอน พร้อมทั้งยังระบุหน้าที่หรือการกระทำต่างๆ ของผู้ที่เกี่ยวข้องทั้งหมดอย่างชัดเจน

งานวิจัยนี้จะเป็นการนำเสนอระบบต้นแบบสำหรับกระบวนการพัฒนาซอฟต์แวร์อย่างปลอดภัยให้กับองค์กรที่พัฒนาซอฟต์แวร์ โดยระบบจะช่วยอำนวยความสะดวกแก่ผู้ที่เกี่ยวข้องในการจัดเก็บรวบรวมข้อมูลที่เกิดขึ้นในกระบวนการพัฒนาซอฟต์แวร์ภายใต้กลไกควบคุมความมั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002

บทที่ 4

การพัฒนาระบบสนับสนุน

จากการศึกษาและออกแบบขั้นตอนการดำเนินงานกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 ตามที่ได้นำเสนอไปในบทที่ 3 แล้วนั้น ผู้เสนอวิทยานิพนธ์ได้ทำการสรุปความต้องการด้านหน้าที่และทำการพัฒนาระบบสนับสนุนขั้นตอนการดำเนินงานดังกล่าว

4.1 ความต้องการด้านหน้าที่ของระบบสนับสนุน

ความต้องการด้านหน้าที่ (Functional Requirements) ของระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 มีดังตารางที่ 3

ตารางที่ 3 ความต้องการด้านหน้าที่

รหัส	ชื่อ	คำอธิบาย
F01	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะเริ่มต้นโครงการ	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ
F02	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะ ออกแบบระบบ	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ รวมถึงมีรายการตรวจสอบที่ระบบมีให้อัตโนมัติโดยให้ผู้มีบทบาททำการระบุรายการตรวจสอบ และมีการอนุมัติผลการระบุในรายการตรวจสอบโดยผู้มีอำนาจการอนุมัติ

ตารางที่ 3 (ต่อ) ความต้องการด้านหน้าที่

F03	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะพัฒนา	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ รวมถึงมีรายการตรวจสอบที่ระบบมีให้อัตโนมัติโดยให้ผู้มีบทบาททำการระบุรายการตรวจสอบ และมีการอนุมัติผลการระบุในรายการตรวจสอบโดยผู้มีอำนาจการอนุมัติ
F04	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะการยอมรับระบบ	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ รวมถึงมีรายการตรวจสอบที่ระบบมีให้อัตโนมัติโดยให้ผู้มีบทบาททำการระบุรายการตรวจสอบ และมีการอนุมัติผลการระบุในรายการตรวจสอบโดยผู้มีอำนาจการอนุมัติ
F05	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะการนำไปใช้จริง	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ รวมถึงมีรายการตรวจสอบที่ระบบมีให้อัตโนมัติโดยให้ผู้มีบทบาททำการระบุรายการตรวจสอบ และมีการอนุมัติผลการระบุในรายการตรวจสอบโดยผู้มีอำนาจการอนุมัติ

ตารางที่ 3 (ต่อ) ความต้องการด้านหน้าที่

F06	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะบำรุงรักษา	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ รวมถึงมีรายการตรวจสอบที่ระบบมีให้อัตโนมัติโดยให้ผู้มีบทบาททำการระบุรายการตรวจสอบ และมีการอนุมัติผลการระบุในรายการตรวจสอบโดยผู้มีอำนาจการอนุมัติ
F07	การควบคุมกระบวนการพัฒนาซอฟต์แวร์ให้มีความปลอดภัย ระยะจัดการแทนที่ระบบ	การควบคุมให้ผู้เกี่ยวข้องกับขั้นตอนการพัฒนาซอฟต์แวร์ในแต่ละเฟสโดยแบ่งตามบทบาทของผู้เกี่ยวข้องในโปรเจค ต้องกรอกข้อมูลกิจกรรมที่ระบบร้องขอ และมีการอนุมัติเอกสารที่ต้องได้รับการตรวจสอบ รวมถึงมีรายการตรวจสอบที่ระบบมีให้อัตโนมัติโดยให้ผู้มีบทบาททำการระบุรายการตรวจสอบ และมีการอนุมัติผลการระบุในรายการตรวจสอบโดยผู้มีอำนาจการอนุมัติ
F08	การเรียก ไอเอสโอ/ไออีซี 27002 รายการตรวจสอบ	การเรียกดูรายงานการตรวจสอบความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 ของโปรเจคว่าตรงข้อใดบ้าง
F09	การจัดการโครงการ	การจัดการโครงการ มีหน้าที่ดังนี้ 1. การสร้างโครงการ 2. การแก้ไขชื่อโครงการ 3. การลบโครงการ 4. การเรียกดูรายละเอียดของโครงการ 5. การปิดโครงการ

ตารางที่ 3 (ต่อ) ความต้องการด้านหน้าที่

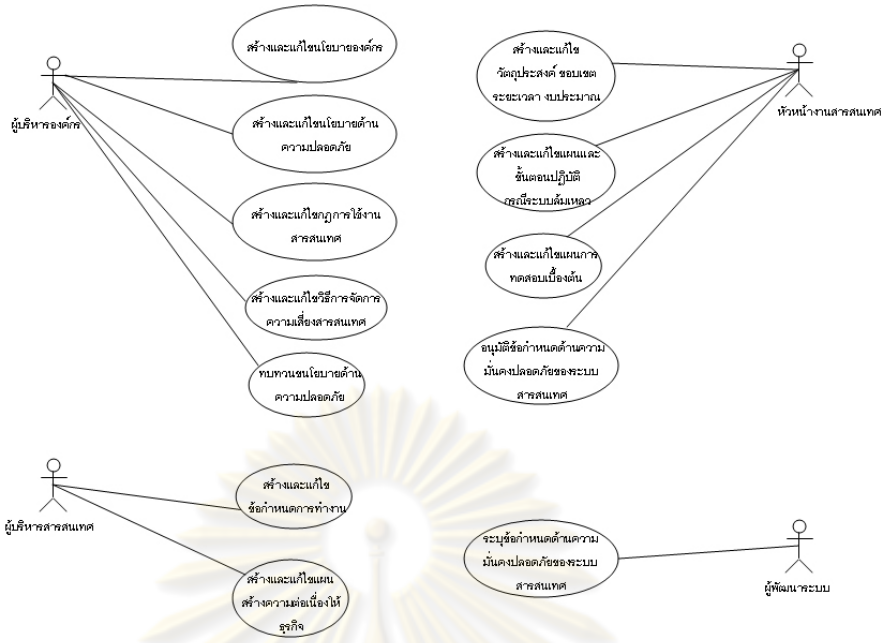
F10	การจัดการเอกสารการควบคุม	การบริหารจัดการเข้าถึงเอกสารที่ใช้ในการควบคุม โดยจะกำหนดให้ผู้เข้าถึงเอกสารเฉพาะหัวข้อที่ตนเองมีสิทธิ์เท่านั้น
F11	การเรียกดูประวัติการพัฒนาซอฟต์แวร์	ทำหน้าที่แสดงรายละเอียดของประวัติการพัฒนาซอฟต์แวร์ที่ผ่านมา

4.2 การออกแบบระบบสนับสนุน

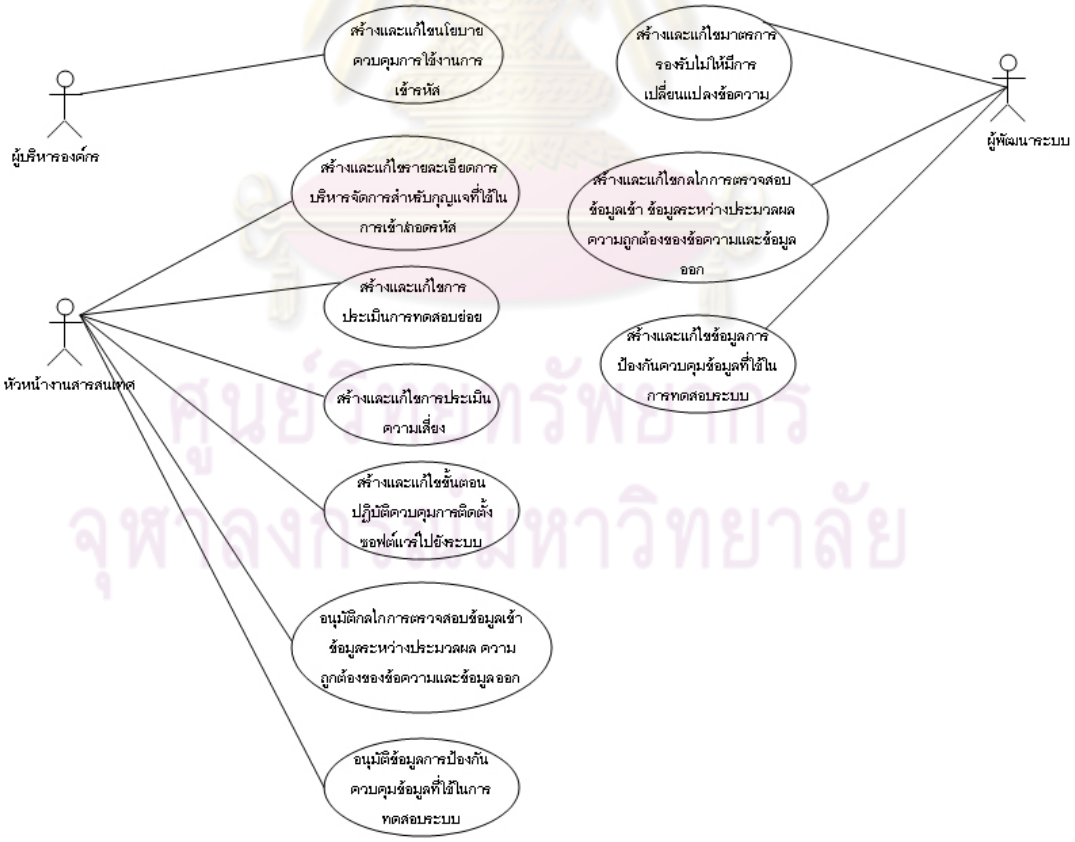
4.2.1 แผนภาพยูสเคส (Use Case Diagram)

แผนภาพยูสเคสนำมาใช้อธิบายหน้าที่การทำงานหลักของระบบ

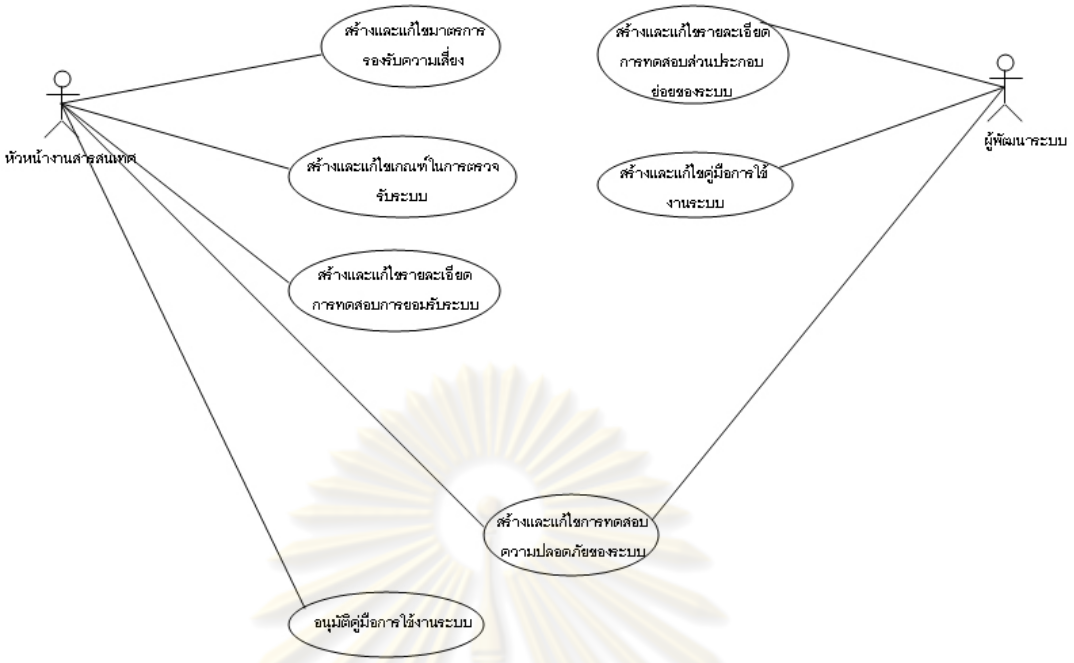
รูปที่ 8 แผนภาพยูสเคสกระบวนการในระยะเริ่มต้นโครงการ



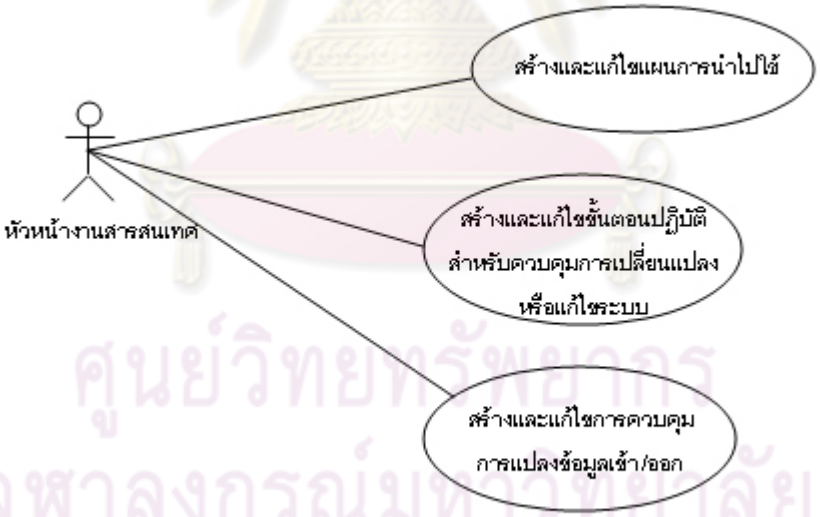
รูปที่ 9 แผนภาพยูสเคสกระบวนการในระยะออกแบบระบบ



รูปที่ 10 แผนภาพยูสเคสกระบวนการในระยะพัฒนา

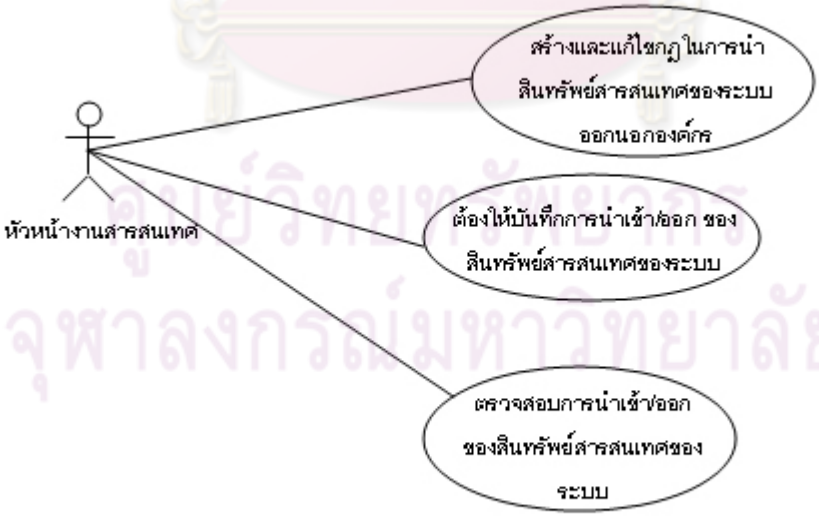


รูปที่ 11 แผนภาพยูสเคสกระบวนการในระยะการยอมรับระบบ



รูปที่ 12 แผนภาพยูสเคสกระบวนการในระยะการนำไปใช้จริง

รูปที่ 13 แผนภาพยูสเคสกระบวนการในระยะบำรุงรักษา

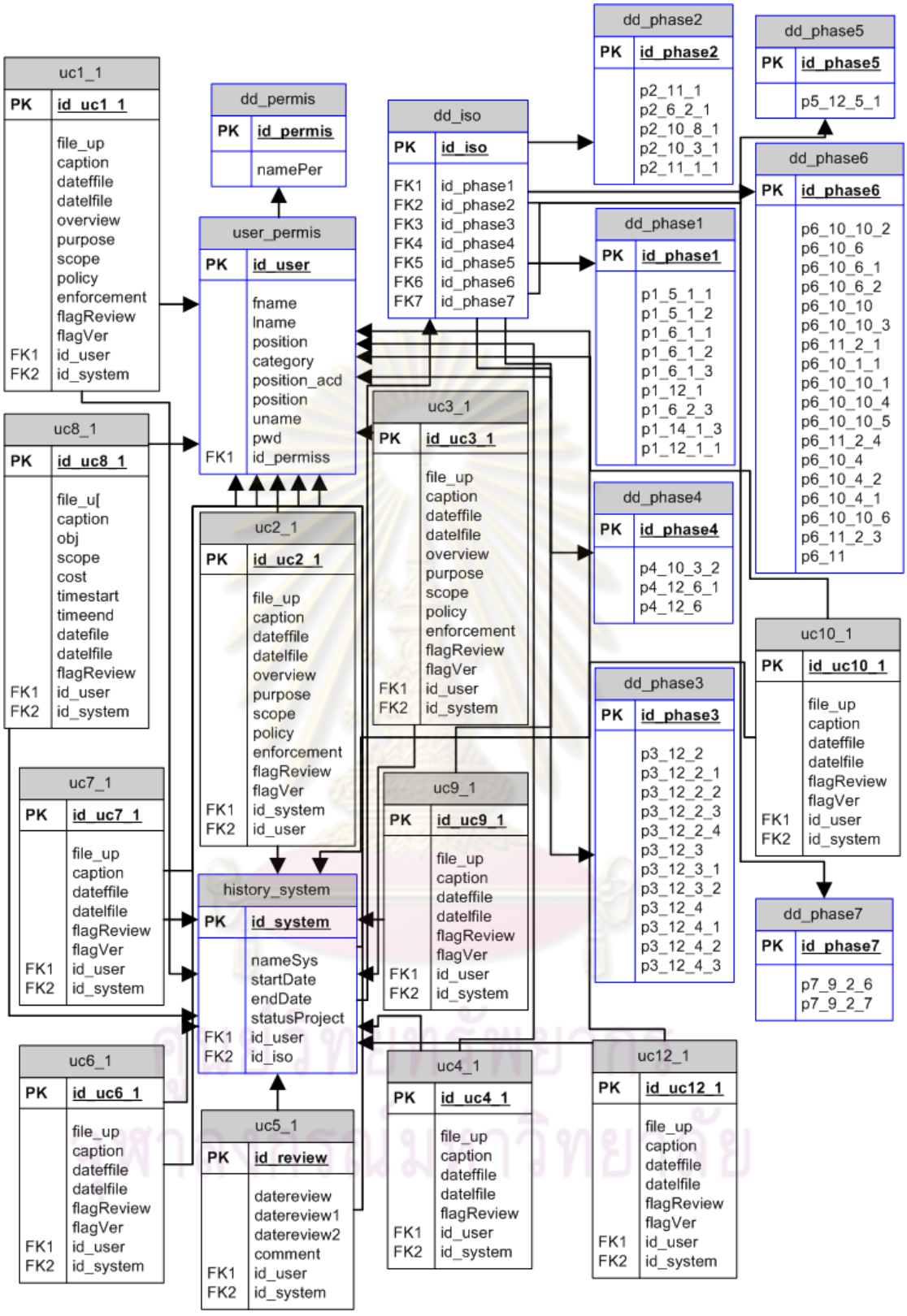


รูปที่ 14 แผนภาพยูสเคสกระบวนการในระยะจัดการแทนที่ระบบ

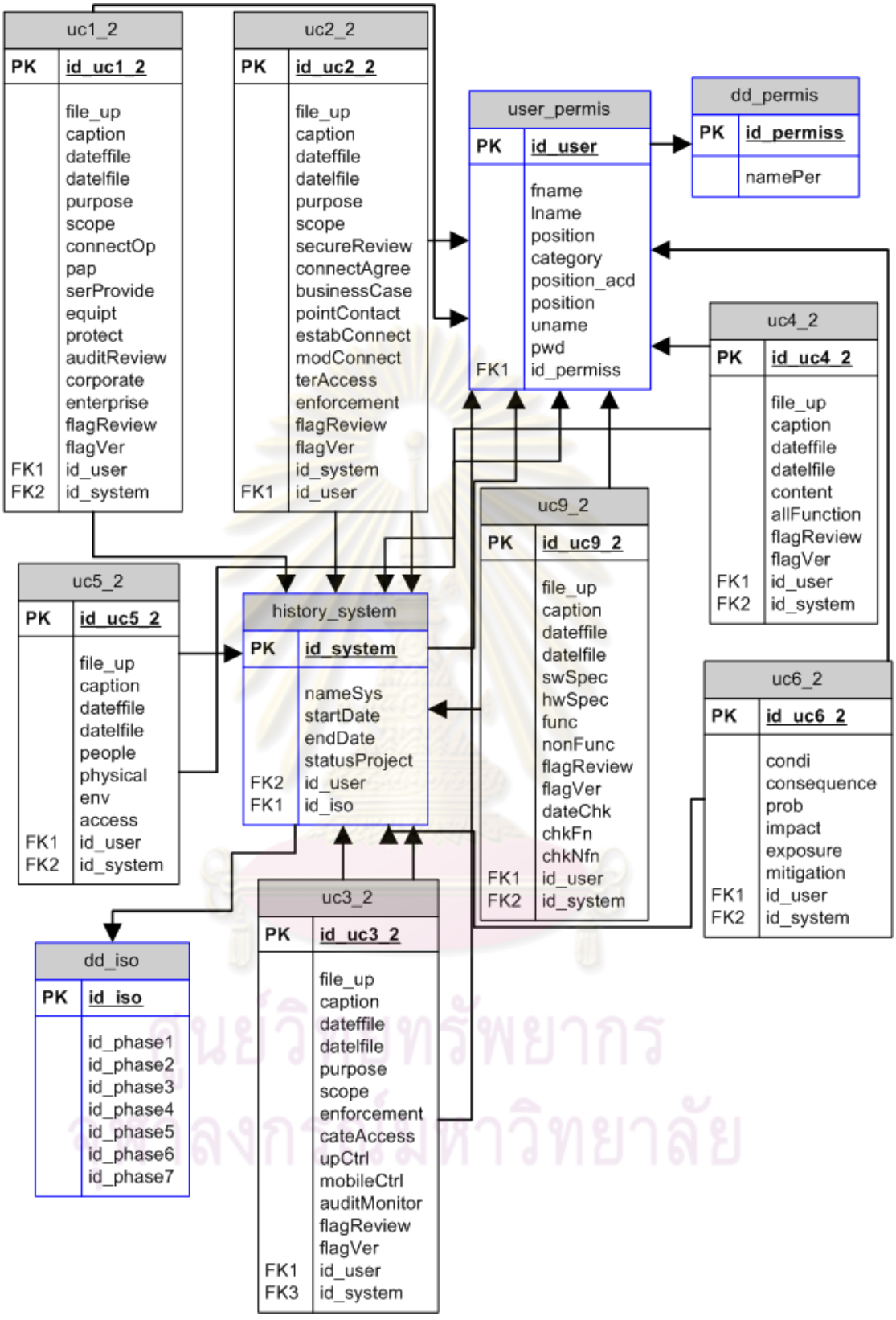
ในส่วนของคำอธิบายยูสเคสของแต่ละยูสเคสดังแสดงในรูปที่ 8 ถึงรูปที่ 14 สามารถดูรายละเอียดได้จากภาคผนวก ก ปรากฏในตารางที่ 5 ถึง ตารางที่ 64

4.2.2 **แผนภาพอีอาร์** (E-R Diagram)

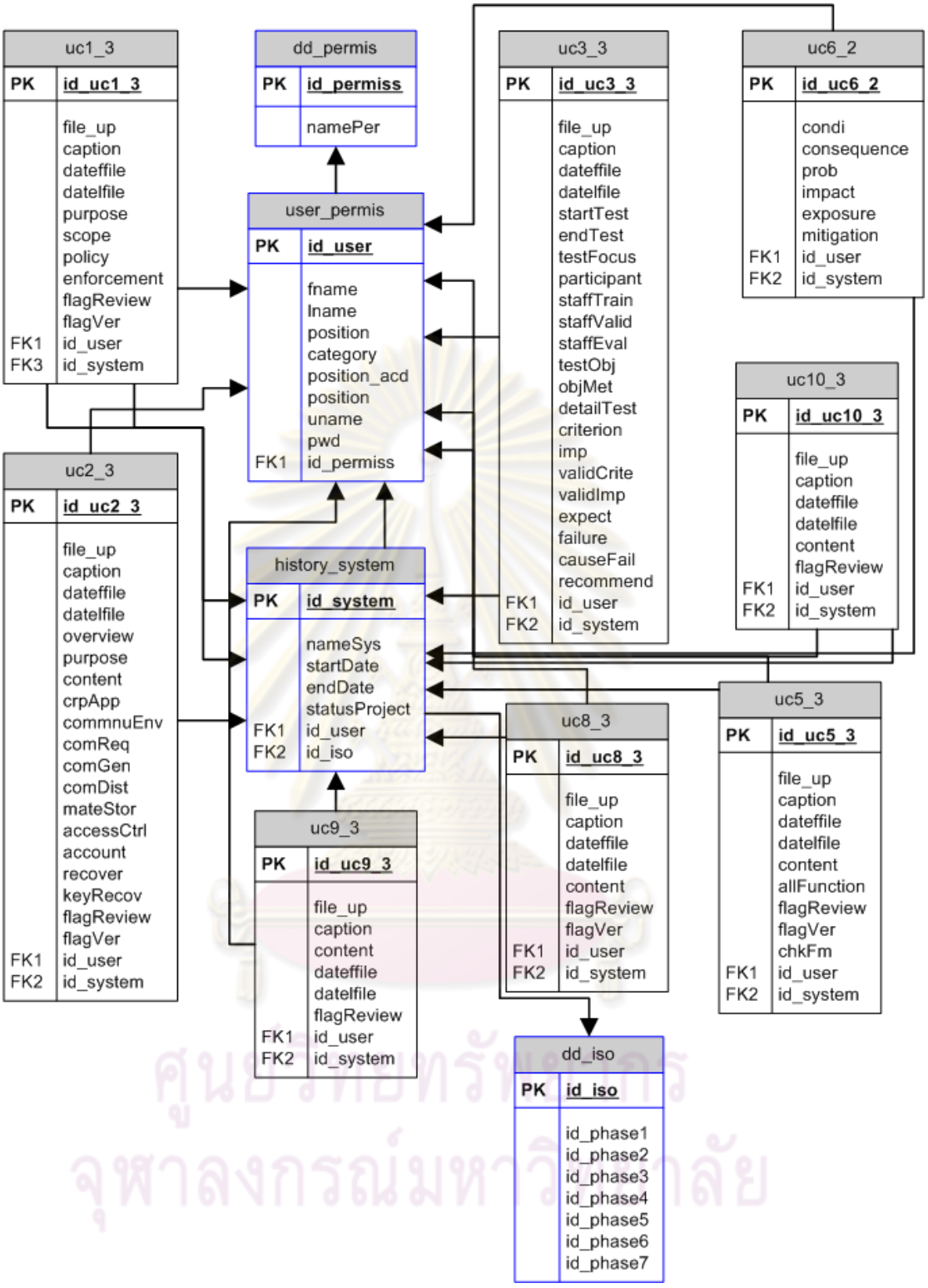
แผนภาพอีอาร์ เป็นแผนภาพที่ใช้ในการอธิบายโครงสร้างและความสัมพันธ์ระหว่างข้อมูลภายในฐานข้อมูล ดังแสดงในรูปที่ 15 ถึง รูปที่ 21



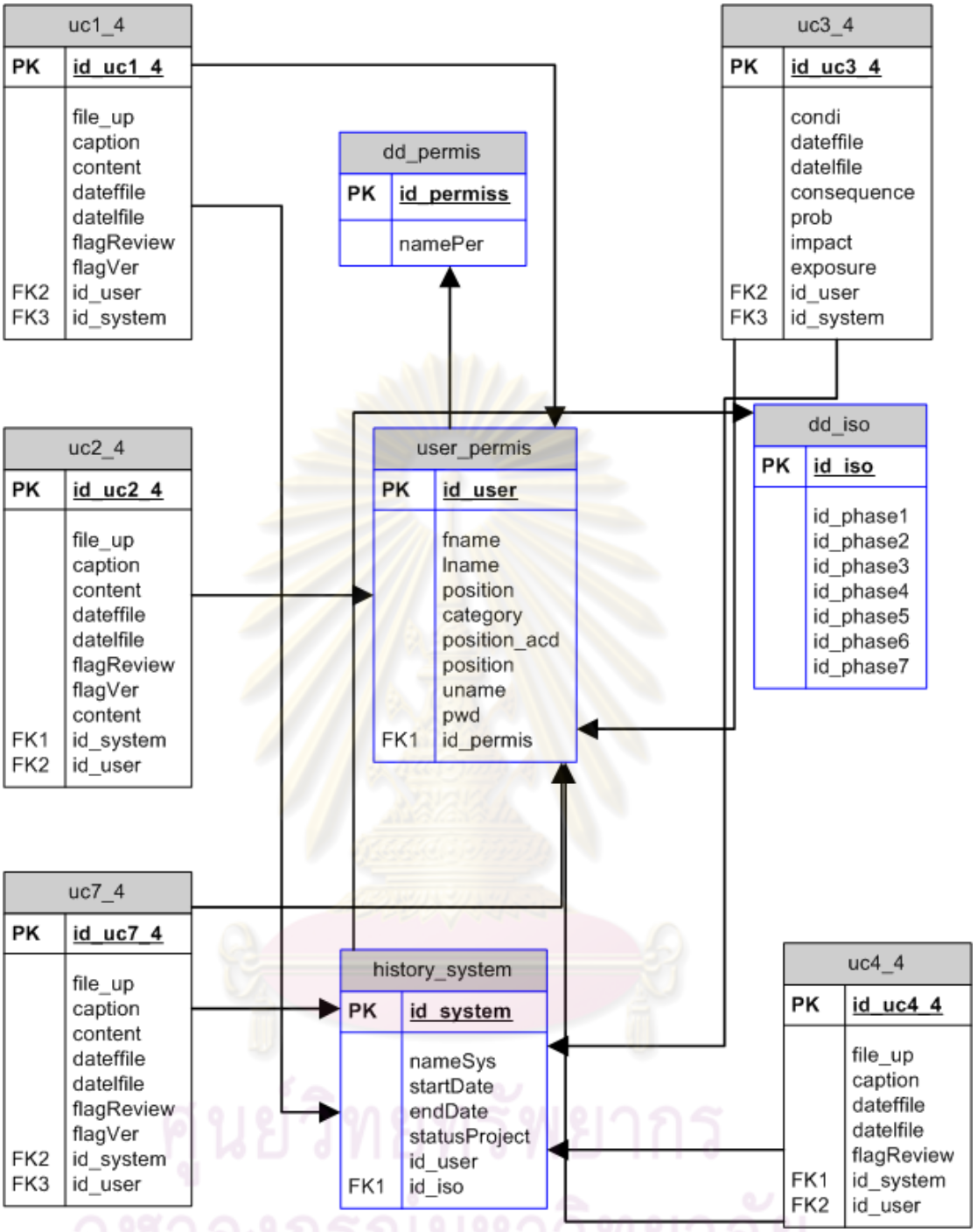
รูปที่ 15 แผนภาพอีอาร์ของฐานข้อมูลในระยะเริ่มต้นโครงการ



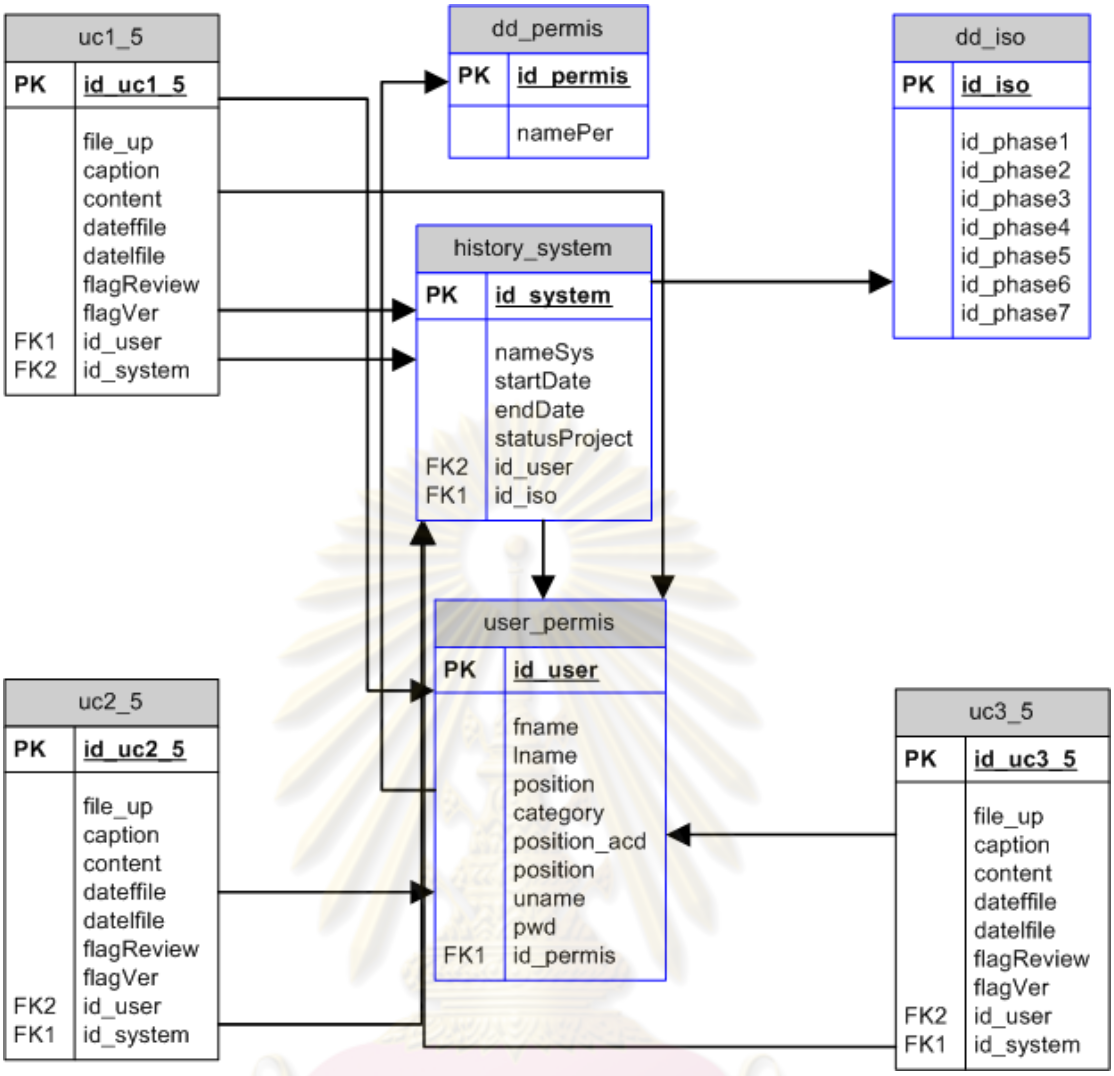
รูปที่ 16 แผนภาพอีอาร์ของฐานข้อมูลในระยะออกแบบระบบ



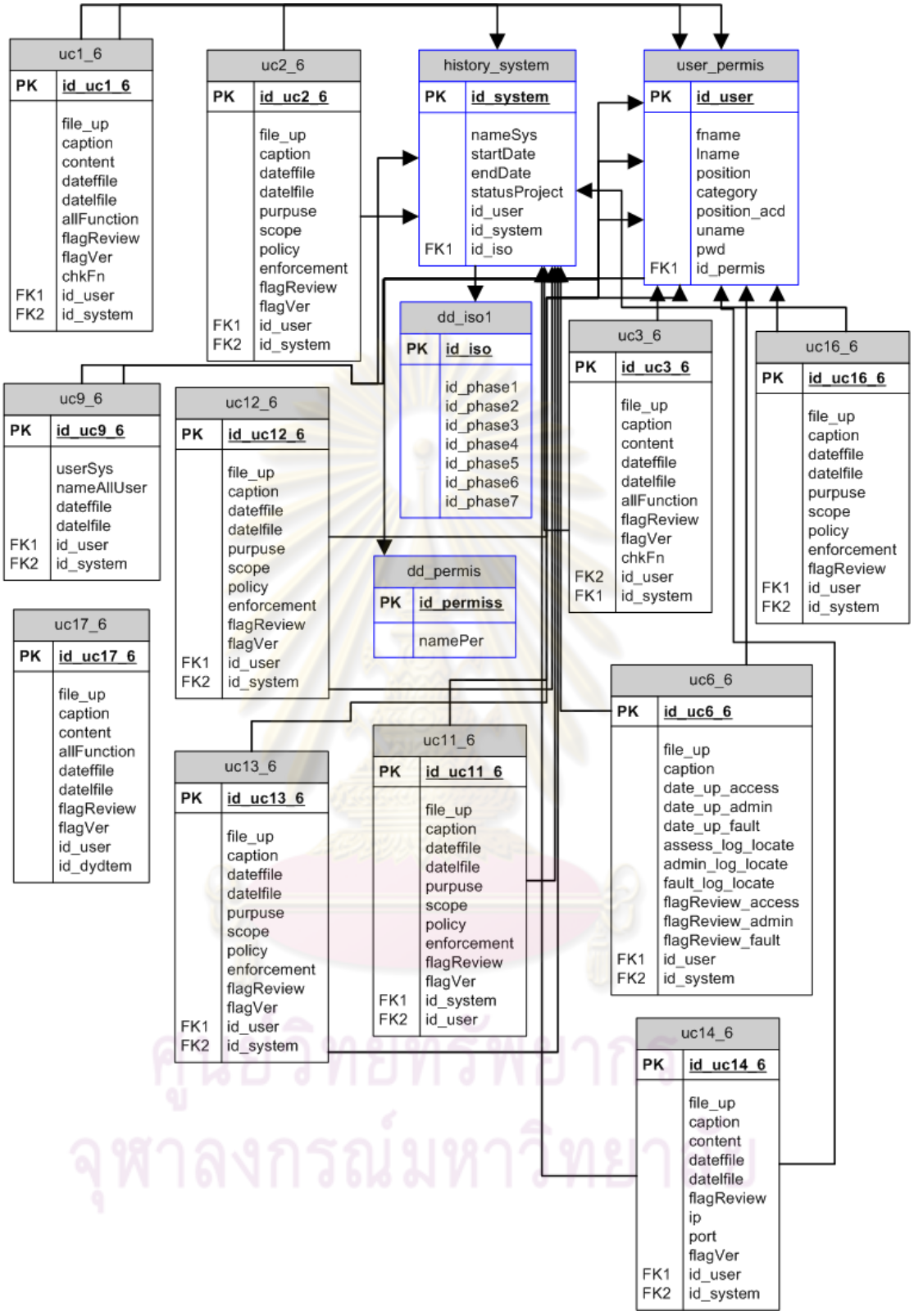
รูปที่ 17 แผนภาพอีอาร์ของฐานข้อมูลในระยะพัฒนา



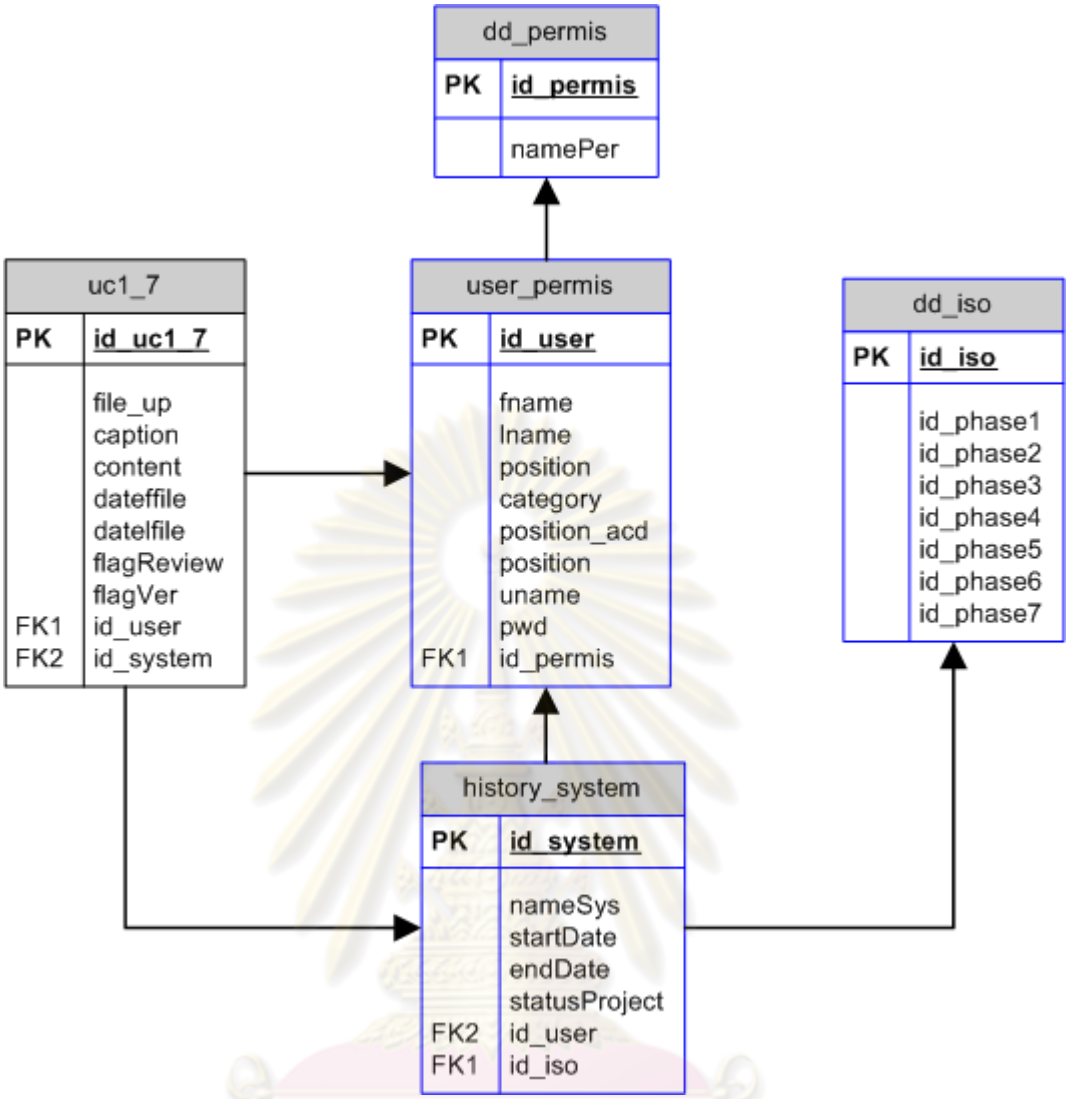
รูปที่ 18 แผนภาพอีอาร์ของฐานข้อมูลในระยะการยอมรับระบบ



รูปที่ 19 แผนภาพอีอาร์ของฐานข้อมูลในระยะการนำไปใช้จริง



รูปที่ 20 แผนภาพอีอาร์ของฐานข้อมูลในระยะบำรุงรักษา



รูปที่ 21 แผนภาพอีอาร์ของฐานข้อมูลในระยะจัดการแทนที่ระบบ

4.3 การพัฒนาระบบสนับสนุน

4.3.1 สภาพแวดล้อมและเครื่องมือที่ใช้ในการพัฒนา

สภาพแวดล้อมที่ใช้ในการพัฒนาระบบมีสภาพแวดล้อมทางด้านฮาร์ดแวร์และซอฟต์แวร์ดังต่อไปนี้

ฮาร์ดแวร์

1. หน่วยประมวลผล อินเทลเพนเทียม เอ็ม 1.73 กิกะเฮิร์ต (Pentium M 1.73 GHz.)

2. หน่วยความจำ (RAM) 2 กิกะไบต์ (2 GB)

3. ฮาร์ดดิสก์ (Hard Disk) 60 กิกะไบต์ (60 GB)

ซอฟต์แวร์

1. ระบบปฏิบัติการ วินโดวส์เอ็กซ์พี โปรเฟสชั่นนอล (Windows XP Professional)

2. เครื่องมือพัฒนาโปรแกรมมาโครมีเดีย ดรีมวีฟเวอร์ 8 (Macromedia Dreamweaver 8)

3. โปรแกรมระบบฐานข้อมูลมายเอสคิวแอล 5.0.45 (MySql 5.0.45)

4. ระบบจัดการฐานข้อมูลพีเอชพีมายแอดมิน 2.10.2 (phpMyAdmin Database Manager Version 2.10.2)

5. เว็บเซิฟเวอร์อพาเช่ 2.2.4 (Apache Web Server Version 2.2.4)

6. ชุดพัฒนาโปรแกรมภาษาพีเอชพี 5.2.3 (PHP 5.2.3)

7. โปรแกรมอินเตอร์เน็ต เอ็กซ์โพลเรอร์ เวอร์ชั่น 8.0

4.3.2 ขั้นตอนการพัฒนาระบบ

การติดตั้งซอฟต์แวร์ในการพัฒนาระบบ

เมื่อเตรียมเครื่องมือสำหรับการพัฒนาระบบเรียบร้อยแล้ว ขั้นต่อมาจึงเป็นส่วนของการติดตั้งเครื่องมือทั้งหมดลงในเครื่องคอมพิวเตอร์ที่ใช้พัฒนาระบบ โดยมีลำดับการติดตั้งเครื่องมือเป็นไปตามขั้นตอนต่อไปนี้

1. ติดตั้งระบบปฏิบัติการ เอ็กซ์พี โปรเฟสชั่นนอล และเว็บเซิฟร์เวอร์อพาเช 2.2.4

2. ติดตั้งโปรแกรมระบบฐานข้อมูลมายเอสคิวแอล 5.0.45

3. ติดตั้งระบบจัดการฐานข้อมูลพีเอชพีมายแอดมิน 2.10.2

4. สร้างฐานข้อมูลระบบ โดยกำหนดชื่อฐานข้อมูล คือ SUPPORTSDLC

5. ติดตั้งเครื่องมือพัฒนาโปรแกรมมาโครมีเดียร์ดรีมวีฟเวอร์ 8

6. สร้างโปรเจ็กเว็บแอพพลิเคชั่นชื่อ supportSDLC เก็บไว้ที่ไดเรคทอรี C:\AppServ\www\supportSDLC และเรียกแสดงผลได้จากที่อยู่ดังต่อไปนี้ http://localhost/supportSDLC

<u>การพัฒนาส่วนต่อประสานผู้ใช้</u>

การพัฒนาส่วนต่อประสานผู้ใช้ของระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 นี้ได้แบ่งส่วนต่อประสานผู้ใช้ออกเป็น 2 ส่วน คือ ส่วนหน้าที่เป็นหน้าที่การทำงานหลัก และส่วนที่เป็นการกำหนดค่าข้อมูลที่ใช้ในระบบสนับสนุน

<u>ส่วนที่ 1</u> การพัฒนาส่วนต่อประสานผู้ใช้ในส่วนที่เป็นหน้าที่การทำงานหลัก ออกแบบให้สอดคล้องกับขอบเขตของระบบที่ได้กล่าวไว้ในบทที่ 1 และมีการทำงานตรงกับความต้องการด้านหน้าที่ที่แสดงไว้ในตารางที่ 2 ในบทที่ 4 โดยสามารถดูตัวอย่างหน้าจอได้ตามรูปที่ 11 ถึงรูปที่ 23 จากภาคผนวก ข ดังนี้

1. การเข้าสู่ระบบ เป็นการตรวจสอบสิทธิ์การเข้าใช้ระบบของผู้ใช้งาน โดยผู้ใช้จะต้องทำการกรอกชื่อผู้ใช้ และ รหัสผ่าน ตัวอย่างหน้าจอดังรูปที่ 11
2. เลือกโปรเจคที่จะทำการควบคุมการพัฒนาระบบให้ปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002
3. แสดงหน้าจอการทำงานหลักของระบบซึ่งแตกต่างกันตามบทบาทของผู้ใช้ ตัวอย่างหน้าจอดังรูปที่ 17 ถึง รูปที่ 29 ซึ่งประกอบด้วยการทำงานหลัก ดังนี้

- ผู้บริหารองค์กร
    1. การจัดการข้อมูลและเอกสารในระยะการเริ่มต้นโครงการและกำหนดความต้องการและหน้าที่ของระบบ
    2. การจัดการข้อมูลและเอกสารในระยะการออกแบบระบบ
    3. เรียกดูรายงานความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002
- ผู้บริหารสารสนเทศ

1. การจัดการข้อมูลและเอกสารในระยะการเริ่มต้นโครงการและกำหนดความต้องการและหน้าที่ของระบบ
2. การจัดการข้อมูลและเอกสารในระยะการออกแบบระบบ
3. การจัดการข้อมูลและเอกสารในระยะการพัฒนาระบบ
4. เรียกดูรายงานความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002

- หัวหน้างานสารสนเทศ

1. การจัดการข้อมูลและเอกสารในการเริ่มต้นโครงการและกำหนดความต้องการและหน้าที่ของระบบ
2. การจัดการข้อมูลและเอกสารในการออกแบบระบบ
3. การจัดการข้อมูลและเอกสารในระยะการสร้าง/พัฒนาระบบ
4. การจัดการข้อมูลและเอกสารในระยะการยอมรับระบบที่พัฒนา
5. การจัดการข้อมูลและเอกสารในระยะการนำไปใช้จริง
6. การจัดการข้อมูลและเอกสารในระยะการบำรุงรักษา
7. การจัดการข้อมูลและเอกสารในระยะการจัดการแทนที่ระบบ
8. เรียกดูรายงานความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002

- ผู้พัฒนาระบบ

1. การจัดการข้อมูลและเอกสารในการเริ่มต้นโครงการและกำหนดความต้องการและหน้าที่ของระบบ
2. การจัดการข้อมูลและเอกสาร ในการออกแบบระบบ
3. การจัดการข้อมูลและเอกสารในระยะการสร้าง/พัฒนาระบบ
4. การจัดการข้อมูลและเอกสารในระยะการยอมรับระบบที่พัฒนา

5. เรียกดูรายงานความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002

- ผู้ดูแลระบบ

1. การจัดการข้อมูลและเอกสารในระยะการบำรุงรักษา
2. เรียกดูรายงานความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002

4. การจัดการข้อมูลและเอกสารในระยะการเริ่มต้นโครงการและกำหนดความต้องการและหน้าที่ของระบบ เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการเริ่มต้นโครงการและกำหนดความต้องการและหน้าที่ของระบบ ประกอบด้วยหน้าที่การทำงานย่อยดังนี้

- ผู้บริหารองค์กร

1. สร้างและแก้ไขนโยบายด้านความปลอดภัย
2. สร้างและแก้ไขนโยบายขององค์กร
3. สร้างและแก้ไขกฎการใช้งานสารสนเทศ
4. สร้างและแก้ไขวิธีการจัดการความเสี่ยงสารสนเทศ
5. ทบทวนนโยบายด้านความปลอดภัย

- ผู้บริหารสารสนเทศ

1. สร้างและแก้ไขข้อกำหนดการทำงาน
2. สร้างและแก้ไขแผนสร้างความต่อเนื่องให้ธุรกิจ

- หัวหน้างานสารสนเทศ

1. สร้างและแก้ไขวัตถุประสงค์ ขอบเขต ระยะเวลา งบประมาณ
2. สร้างและแก้ไขแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว
3. สร้างและแก้ไขแผนการทดสอบเบื้องต้น
4. อนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

- ผู้พัฒนาระบบ

1. ระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

5. การจัดการข้อมูลและเอกสารในระยะการออกแบบระบบ เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการออกแบบระบบ ประกอบด้วยหน้าที่การทำงานย่อยดังนี้

- ผู้บริหารองค์กร
    1. สร้างและแก้ไขขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร
    2. สร้างและแก้ไขมาตรการรักษาความปลอดภัยระหว่างองค์กร
- ผู้บริหารสารสนเทศ
    1. สร้างและแก้ไขนโยบายและมาตรการควบคุมการเข้าถึง
- หัวหน้างานสารสนเทศ
    2. สร้างและแก้ไขแผนกำหนดความต้องการสารสนเทศ
    3. สร้างและแก้ไขสิ่งที่เกี่ยวข้องกับความปลอดภัย
    4. สร้างและแก้ไขสิ่งที่เกี่ยวข้องกับความเสี่ยงและการประเมินความเสี่ยง
    5. อนุมัติรายละเอียดของการออกแบบระบบ
- ผู้พัฒนาระบบ
    1. สร้างและแก้ไขรายละเอียดของการออกแบบระบบ

6. การจัดการข้อมูลและเอกสารในระยะการสร้าง/พัฒนาระบบ เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการสร้าง/พัฒนาระบบ ประกอบด้วยหน้าที่การทำงานย่อยดังนี้

    - ผู้บริหารองค์กร
        1. สร้างและแก้ไขนโยบายควบคุมการใช้งานการเข้ารหัส
    - หัวหน้างานสารสนเทศ
        1. สร้างและแก้ไขรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส
        2. สร้างและแก้ไขการประเมินการทดสอบย่อย
        3. สร้างและแก้ไขการประเมินความเสี่ยง
        4. สร้างและแก้ไขขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ
        5. อนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก
        6. อนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ
    - ผู้พัฒนาระบบ

1. สร้างและแก้ไขมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ
2. สร้างและแก้ไขกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก
3. สร้างและแก้ไขข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ

7. การจัดการข้อมูลและเอกสารในระยะการยอมรับระบบที่พัฒนา เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการยอมรับระบบที่พัฒนา ประกอบด้วยหน้าที่การทำงานย่อยดังนี้
   - หัวหน้างานสารสนเทศ
     1. สร้างและแก้ไขมาตรการรองรับความเสี่ยง
     2. สร้างและแก้ไขเกณฑ์ในการตรวจรับระบบ
     3. สร้างและแก้ไขรายละเอียดการทดสอบการยอมรับระบบ
     4. สร้างและแก้ไขการทดสอบความปลอดภัยของระบบ(ร่วมกันกับผู้ดูแลระบบ)
     5. อนุมัติคู่มือการใช้งานระบบ
   - ผู้พัฒนาระบบ
     1. สร้างและแก้ไขรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ
     2. สร้างและแก้ไขคู่มือการใช้งานระบบ
     3. สร้างและแก้ไขการทดสอบความปลอดภัยของระบบ(ร่วมกันกับหัวหน้างานสารสนเทศ)

8. การจัดการข้อมูลและเอกสารในระยะการนำไปใช้จริง เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการนำไปใช้จริง ประกอบด้วยหน้าที่การทำงานย่อยดังนี้
   - หัวหน้างานสารสนเทศ
     1. สร้างและแก้ไขแผนการนำไปใช้
     2. สร้างและแก้ไขขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ
     3. สร้างและแก้ไขการควบคุมการแปลงข้อมูลเข้า/ออก

9. การจัดการข้อมูลและเอกสารในระยะการบำรุงรักษา เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการบำรุงรักษา ประกอบด้วยหน้าที่การทำงานย่อยดังนี้

    - หัวหน้างานสารสนเทศ
        1. สร้างและแก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ
        2. สร้างและแก้ไขนโยบายการใช้งานบริการเครือข่าย
        3. สร้างและแก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ
        4. สร้างและแก้ไขขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งาน
        5. สร้างและแก้ไขขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่
        6. ตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ
        7. ตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ
        8. ตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ
        9. ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบงานระบบ
        10. อนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
    - ผู้ดูแลระบบ
        1. สร้างและแก้ไขมาตรการป้องกันภัยคุกคามทางเครือข่าย
        2. สร้างและแก้ไขมาตรการควบคุมการใช้งานระบบเคลื่อนที่
        3. สร้างและแก้ไขมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ
        4. ตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง
        5. กำหนดสิทธิ์การใช้งานระบบ
        6. สร้างและแก้ไขรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

10. การจัดการข้อมูลและเอกสารในระยะการจัดการแทนที่ระบบ เป็นส่วนของการจัดการข้อมูลรายละเอียดของเอกสารที่ต้องมีเพื่อควบคุมความปลอดภัยของโครงการในระยะการจัดการแทนที่ระบบ ประกอบด้วยหน้าที่การทำงานย่อยดังนี้

    - หัวหน้างานสารสนเทศ

1. สร้างและแก้ไขกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร
2. สร้างรายการตรวจสอบการแทนที่ระบบ

- ผู้ดูแลระบบ
  1. ระบุรายการตรวจสอบการแทนที่ระบบ

11. การเรียกดูรายงานความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002

สามารถเรียกดูรายงานความปลอดภัยของโครงการว่ากระบวนการพัฒนาซอฟต์แวร์ของโครงการนี้มีความปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 หรือไม่ โดยแสดงหัวข้อที่ถูกควบคุมตามมาตรฐานไอเอสโอ/ไออีซี 27002 ในส่วนที่เกี่ยวข้องกับการพัฒนาซอฟต์แวร์

12. การจัดการโครงการ เป็นส่วนของการจัดการข้อมูลรายละเอียดของโครงการ ประกอบด้วยหน้าที่การทำงานย่อยดังนี้

- การสร้างโครงการ โดยหน้าที่การทำงานวนส่วนนี้จะมีการจำกัดสิทธิของผู้ใช้งาน คือ มีเพียงหัวหน้าสารสนเทศเท่านั้นที่สามารถสร้างโครงการใหม่ได้
- การแก้ไขชื่อโครงการ เป็นการแก้ไขข้อมูลชื่อของโครงการ
- การลบโครงการ เป็นการลบโครงการที่ไม่ต้องการออกจากระบบ
- การเรียกดูรายละเอียดของโครงการ เป็นส่วนของการเรียกดูรายละเอียดของโครงการ
- การปิดโครงการ เป็นการปิดโครงการเมื่อโครงการดังกล่าวดำเนินการเสร็จเรียบร้อยแล้ว

13. แสดงประวัติการพัฒนาซอฟต์แวร์ เป็นส่วนของการแสดงประวัติการพัฒนาซอฟต์แวร์ผ่านระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 นี้ โดยดูย้อนหลังได้ โดยเลือกดูตามรายปีที่ต้องการหรือเลือกดูตามกลุ่มประเภทเป้าหมายของผู้ใช้ซอฟต์แวร์นั้น

<u>ส่วนที่ 2</u> การพัฒนาส่วนที่เป็นการกำหนดค่าข้อมูลที่ใช้ในระบบสนับสนุน เพื่อให้ผู้ใช้สามารถทำการแก้ไขข้อมูลต่างๆ ในระบบสนับสนุนได้อย่างสะดวก โดยสามารถดูตัวอย่างหน้าจอได้ตามรูปที่ 22 ถึงรูปที่ 34 จากภาคผนวก ก ดังนี้

1. การเข้าสู่ระบบ เป็นการตรวจสอบสิทธิ์การเข้าใช้ระบบของผู้ใช้งาน โดยผู้ใช้จะต้องทำการกรอกชื่อผู้ใช้ และ รหัสผ่าน ตัวอย่างหน้าจอดังรูปที่ 22

2. แสดงหน้าจอรายการหลักของการกำหนดค่า ตัวอย่างอย่างหน้าจอดังรูปที่ 24 ซึ่งประกอบด้วยส่วนของการกำหนดค่าข้อมูลต่างๆ

3. การจัดการข้อมูลหัวข้อตามมาตรฐานไอเอสโอ/ไออีซี 27002 ในส่วนที่เกี่ยวข้องกับการพัฒนาซอฟต์แวร์เท่านั้น เป็นหน้าจอที่ใช้ในการแก้ไข ข้อมูลรายละเอียดต่างๆ ของหัวข้อตามมาตรฐานไอเอสโอ/ไออีซี 27002 ตัวอย่างหน้าจอดังรูปที่ 23 ถึง 33

บทที่ 5

การทดสอบระบบสนับสนุน

การทดสอบระบบสนับสนุนมีจุดประสงค์เพื่อตรวจสอบการทำงานที่ผิดพลาด และเพื่อตรวจสอบหน้าทีการทำงานของระบบว่าสามารถทำงานได้ถูกต้องตามความต้องการของผู้ใช้งานหรือไม่ ซึ่งระบบสนับสนุนนี้มีความสอดคล้องกับขั้นตอนของกระบวนการพัฒนาซอฟต์แวร์โดยอ้างอิงตามมาตรฐาน ไอเอสโอ/ไออีซี 27002 เฉพาะในส่วนที่เกี่ยวข้องกับกระบวน การพัฒนาซอฟต์แวร์โดยตรงเท่านั้น

5.1 ขั้นตอนปฏิบัติและผลการทดสอบระบบสนับสนุนด้วยกรณีทดสอบ

การดำเนินการทดสอบใช้หลักการทดสอบหน้าที่การทำงาน (Black Box Testing) ตามกรณีทดสอบที่ได้ออกแบบไว้ โดยมีขั้นตอนปฏิบัติและผลการทดสอบดังตารางที่ 4

ตารางที่ 4 การทดสอบตามความต้องการด้านหน้าที่

ลำดับ	การทดสอบ	คำอธิบาย	ผลการทดสอบที่คาดหวัง	ผลการทดสอบจริง
1.	เข้าสู่ระบบ	ทำการล๊อคอินเพื่อเข้าใช้งานระบบ	หากชื่อผู้ใช้และรหัสผ่านถูกต้องให้เข้าใช้งานได้ ถ้าผิดพลาดต้องไม่สามารถเข้าใช้งานได้	ถูกต้อง
2.	สร้างโครงการ	ทำการสร้างโครงการลงในระบบ	ปรากฏโครงการที่สร้างใหม่	ถูกต้อง

ตารางที่ 4 (ต่อ) การทดสอบตามความต้องการด้านหน้าที่

3.	แก้ไขโครงการ	แก้ไขรายละเอียดของโครงการที่สร้างขึ้น	สามารถแก้ไขรายละเอียดของโครงการที่สร้างขึ้น	ถูกต้อง
4.	ลบโครงการ	ลบโครงการที่ต้องการ	สามารถลบโครงการได้	ถูกต้อง
5.	ปิดโครงการ	ทำการปิดโครงการเมื่อกระบวนการพัฒนาซอฟต์แวร์ให้ปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซีเสร็จสิ้น	สามารถทำการปิดโครงการได้	ถูกต้อง
6.	การเลือกโครงการที่จะเริ่มพัฒนาซอฟต์แวร์	ทำการเลือกโครงการที่ต้องการเริ่มพัฒนาซอฟต์แวร์ได้	สามารถเลือกโครงการได้ตามต้องการ	ถูกต้อง
7.	การจัดการข้อมูลและเอกสารในแต่ระยะของกระบวนการการพัฒนาซอฟต์แวร์	สามารถจัดการข้อมูลและเอกสารโดยมีการควบคุมการเข้าถึงข้อมูลและเอกสารในแต่ละระยะของกระบวนการพัฒนา เช่น มีรายการตรวจสอบและการอนุมัติโดยผู้มีสิทธิ์ โดยจำแนกตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น	สามารถดู ลบ แก้ไขข้อมูลหรือเอกสารเฉพาะในส่วนที่มีสิทธิ์ได้	ถูกต้อง
8.	การเรียกดูประวัติการพัฒนาซอฟต์แวร์	เป็นการเรียกดูประวัติการพัฒนาซอฟต์แวร์ย้อนหลัง	สามารถเรียกดูประวัติการพัฒนาของซอฟต์แวร์ตามที่ต้องการได้	ถูกต้อง

ตารางที่ 4 (ต่อ) การทดสอบตามความต้องการด้านหน้าที่

9.	การเรียกดูรายงานความปลอดภัยของกระบวนการพัฒนาซอฟต์แวร์ อ้างอิงตามมาตรฐานไอเอสโอ/ไออีซี 27002	สามารถเรียกดูรายงานความปลอดภัย อ้างอิงตามมาตรฐาน ไอเอส/ไออีซี 27002 ของกระบวนการพัฒนาซอฟต์แวร์ตามที่ต้องการได้	สามารถเรียกดูรายงานความปลอดภัยได้	ถูกต้อง

5.2 **สรุปผลการทดลอง**

จากผลการทดลองข้างต้นสรุปได้ว่า ขั้นตอนการดำเนินงานในกระบวนการพัฒนาซอฟต์อย่างปลอดภัย ตามมาตรฐานไอเอสโอ/ไออีซี 27002 ตามที่ได้กำหนดไว้นี้สามารถบันทึกเปลี่ยนแปลง และจัดเก็บข้อมูลต่างๆ รวมทั้งนำมาแสดงผลผ่านหน้าจอการทำงานได้อย่างถูกต้อง นอกจากนี้ผู้วิจัยยังได้ทำการทดสอบระบบสนับสนุนนี้โดยการนำไปใช้จริงที่ศูนย์คอมพิวเตอร์ มหาวิทยาลัยกรุงเทพ เพื่อนำผลที่ได้จากการใช้งานจริงมาปรับปรุงด้านความสะดวกของการกรอกข้อมูล การเรียกดูนโยบายสำหรับอ้างอิงในแต่ละระยะของกระบวนการพัฒนาซอฟต์แวร์ การจัดรูปแบบข้อมูลที่กรอกผ่านระบบ เพื่อให้ระบบสนับสนุนนี้ให้มีประสิทธิภาพมากและใช้งานสะดวกยิ่งขึ้น

บทที่ 6

สรุปผลการวิจัย และข้อเสนอแนะ

6.1 สรุปผลการวิจัย

ผลลัพธ์ที่ได้จากงานวิจัยมีดังนี้

1. ได้ขั้นตอนการพัฒนาและดำเนินงานกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย อ้างอิงตามมาตรฐานไอเอสโอ/ไออีซี 27002 โดยระบุกระแสงาน บทบาท กิจกรรมและประดิษฐการต่างๆ ของกระบวนการพัฒนาซอฟต์แวร์ให้มั่นคงปลอดภัยได้อย่างถูกต้องและชัดเจน

2. ได้ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย เพื่อช่วยอำนวยความสะดวกให้กับองค์กรที่พัฒนาซอฟต์แวร์ อ้างอิงตามมาตรฐานไอเอสโอ/ไออีซี

งานวิจัยนี้ได้พัฒนาระบบให้อยู่ในรูปแบบของแอพพลิเคชั่น (Application Program) ที่ช่วยในการควบคุมความปลอดภัยในกระบวนการพัฒนาซอฟต์แวร์ อ้างอิงตามมาจรฐานไอเอสโอ/ไออีซี 27002 พร้อมทั้งช่วยจัดการงานเอกสารต่างๆ ให้สะดวกรวดเร็ว ง่ายต่อการค้นคืน และเป็นกลไกหนึ่งในการควบคุมความปลอดภัยระหว่างกระบวนการพัฒนาซอฟต์แวร์

6.2 ข้อจำกัด

จากการดำเนินงานวิจัยนี้พบปัญหาและข้อจำกัด ดังต่อไปนี้

1. ในส่วนของการกำหนดแผนงานและนโยบายต่างๆ ที่เกี่ยวข้องกับความปลอดภัยนั้นได้มีการกำหนดแบบฟอร์มเพื่อเป็นแนวทางในการดำเนินงาน แต่การนำไปใช้งานนั้นขึ้นอยู่กับความเหมาะสมของแต่ละองค์กร
2. ระบบนี้ไม่รองรับการจัดรูปแบบของข้อความที่ใส่ลงไปในกระบวนการต่างๆ อาจทำให้ผู้ใช้ไม่สะดวกในการจัดรูปแบบให้สวยงามได้ตามที่ต้องการ

6.3 แนวทางการวิจัยต่อ

ระบบสนับสนุนกระบวนการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยตามมาตรฐานไอเอสโอ/ไออีซี 27002 ที่พัฒนาขึ้นจากงานวิจัยนี้ สามารถนำไปพัฒนาต่อเพื่อปรับปรุงให้เข้ากับกระบวนการในการพัฒนาซอฟต์แวร์ของแต่ละองค์กร และยังสามารถนำไปพัฒนาฟังก์ชั่นการใช้งานใหม่ๆ ให้เหมาะสมกับแต่ละองค์กรได้ ไม่ว่าจะเป็นการแสดงผลรายงานในรูปแบบต่างๆ หรือการแจ้งเตือนข่าวสารภายในระบบ เป็นต้น

นอกจากนี้ สามารถนำแนวคิดจากงานวิจัยนี้ไปพัฒนาให้รองรับกับมาตรฐานไอเอสโอ/ไออีซีใหม่ๆ ที่กำลังจะออกมา ซึ่งจะช่วยเพิ่มความปลอดภัยให้กับระบบสารสนเทศขององค์กรได้ดียิ่งขึ้น และยังสามารถนำไปประยุกต์เพื่อพัฒนาระบบต่างๆ ที่นอกเหนือจากการพัฒนาซอฟต์แวร์ให้มีความปลอดภัยมากขึ้น

รายการอ้างอิง

[1] British Standards Institution, ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management, 15 June 2005.

[2] ThaiCert, มาตรฐาน แนวทางปฏิบัติ และกรอบงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ, 28 กุมภาพันธ์ 2550.

[3] PRAXIOM RESEARCH GROUP LIMITED, "ISO IEC 27002 2005" [Online]. Available from: http://www.praxiom.com/iso-17799-2005.htm, [2008, December 11].

[4] Lynn Futcher, and Rossouw von Solms, "Guidelines for Secure Software Development", SAICSIT, 2008, pp. 56-65.

[5] ThaiCert, มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชัน 2.5, 25 มกราคม 2551.

[6] [IN] SECURE, Integrating ISO 17799 into your Software Development Lifecycle, 11, May 2007, pp. 29-36.

ภาคผนวก

ภาคผนวก ก.

คำอธิบายยูสเคส

ตารางที่ 5 อธิบายยูสเคสสร้าง/แก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ

หมายเลขยูสเคส : UC1	**ชื่อยูสเคส** : สร้าง/แก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขขั้นตอนปฏิบัติงานการตรวจสอบการใช้งานสารสนเทศ	
ความสัมพันธ์ : Association : ผู้บริหารองค์กร Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดเอกสารของขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ a. หากเป็นการแก้ไขการอัพโหลดเอกสารของขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารของขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารของขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ 4. บันทึกข้อมูลของขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 6 อธิบายยูสเคสสร้างและแก้ไขนโยบายการใช้งานบริการเครือข่าย

หมายเลขยูสเคส : UC2	**ชื่อยูสเคส** : สร้างและแก้ไขนโยบายการใช้งานบริการเครือข่าย
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขนโยบายการใช้งานบริการเครือข่าย	
ความสัมพันธ์ : Association : ผู้บริหารองค์กร Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขนโยบายการใช้งานบริการเครือข่าย 2. ระบบแสดงหน้าจอสำหรับอัพโหลดเอกสารนโยบายการใช้งานบริการเครือข่าย a. หากเป็นการแก้ไขการอัพโหลดเอกสารนโยบายการใช้งานบริการเครือข่าย ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการ อัพโหลดเอกสารนโยบายการใช้งานบริการเครือข่ายเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารนโยบายการใช้งานบริการเครือข่าย 4. บันทึกข้อมูลนโยบายการใช้งานบริการเครือข่าย	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 7 คำอธิบายยูสเคสสร้างและแก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ

หมายเลขยูสเคส : UC3	**ชื่อยูสเคส** : สร้างและแก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	

รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ
ความสัมพันธ์ : Association : ผู้บริหารองค์กร Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดเอกสารมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ a. หากเป็นการแก้ไขการอัพโหลดเอกสารมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้วเพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ 4. บันทึกข้อมูลมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 8 อธิบายยูสเคสสร้างและแก้ไขวิธีการจัดการความเสี่ยงสารสนเทศ

หมายเลขยูสเคส : UC4	**ชื่อยูสเคส** : สร้างและแก้ไขวิธีการจัดการความเสี่ยงสารสนเทศ
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขวิธีการจัดการความเสี่ยงสารสนเทศ	
ความสัมพันธ์ : Association : ผู้บริหารองค์กร	

Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขวิธีการจัดการความเสี่ยงสารสนเทศ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดเอกสารวิธีการจัดการความเสี่ยงสารสนเทศ a. หากเป็นการแก้ไขการอัพโหลดเอกสารวิธีการจัดการความเสี่ยงสารสนเทศ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารวิธีการจัดการความเสี่ยงสารสนเทศเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารวิธีการจัดการความเสี่ยงสารสนเทศ 4. บันทึกข้อมูลวิธีการจัดการความเสี่ยงสารสนเทศ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 9 อธิบายยูสเคสทบทวนนโยบายด้านความปลอดภัย

หมายเลขยูสเคส : UC5	**ชื่อยูสเคส** : ทบทวนนโยบายด้านความปลอดภัย
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	
รายละเอียด : เพื่ออธิบายขั้นตอนในการทบทวนนโยบายด้านความปลอดภัย	
ความสัมพันธ์ : Association : ผู้บริหารองค์กร Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูทบทวนนโยบายด้านความปลอดภัย 2. ระบบแสดงหน้าจอสำหรับทบทวนนโยบายด้านความปลอดภัย และแสดงวันเวลาที่ได้ทำการทบทวนไปล่าสุด และสามารถดูประวัติการทบทวนที่แล้วมาได้	

a. หากพบว่าต้องมีการแก้ไขนโยบายด้านความปลอดภัย เลือกเมนูแก้ไขนโยบายด้านความปลอดภัย ระบบจะแสดงแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ • อัพโหลดเอกสารนโยบายด้านความปลอดภัย b. หากไม่มีการแก้ไขหรือเพิ่มนโยบายด้านความปลอดภัย ให้คลิกต่อไปเพื่อลงนามการทบทวนครั้งนี้ โดยระบบจะแสดงหน้าจอเพื่อใส่ชื่อผู้ทำการทบทวนนโยบายด้านความปลอดภัย 3. บันทึกข้อมูลการทบทวนนโยบายด้านความปลอดภัย
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 10 คำอธิบายยูสเคสสร้าง/แก้ไขข้อกำหนดการทำงาน

หมายเลขยูสเคส : UC6	**ชื่อยูสเคส** : สร้าง/แก้ไขข้อกำหนดการทำงาน
ผู้เกี่ยวข้องหลัก : ผู้บริหารสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขข้อกำหนดการทำงาน	
ความสัมพันธ์ : Association : ผู้บริหารสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขข้อกำหนดการทำงาน 2. ระบบแสดงหน้าจอสำหรับอัพโหลดเอกสารข้อกำหนดการทำงาน a. หากเป็นการแก้ไขการอัพโหลดเอกสารข้อกำหนดการทำงาน ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารข้อกำหนดการทำงานเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารข้อกำหนดการทำงาน 4. บันทึกข้อมูลข้อกำหนดการทำงาน	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 11 อธิบายยูสเคสสร้าง/แก้ไขแผนสร้างความต่อเนื่องให้ธุรกิจ

หมายเลขยูสเคส : UC7	**ชื่อยูสเคส** : สร้าง/แก้ไขแผนสร้างความต่อเนื่องให้ธุรกิจ
ผู้เกี่ยวข้องหลัก : ผู้บริหารสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขแผนสร้างความต่อเนื่องให้ธุรกิจ	
ความสัมพันธ์ : Association : ผู้บริหารสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขแผนสร้างความต่อเนื่องให้ธุรกิจ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดแผนสร้างความต่อเนื่องให้ธุรกิจ a. หากเป็นการแก้ไขการอัพโหลดเอกสารแผนสร้างความต่อเนื่องให้ธุรกิจระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารแผนสร้างความต่อเนื่องให้ธุรกิจเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารแผนสร้างความต่อเนื่องให้ธุรกิจ 4. บันทึกข้อมูลแผนสร้างความต่อเนื่องให้ธุรกิจ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 12 อธิบายยูสเคสสร้าง/แก้ไขวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ

หมายเลขยูสเคส : UC8	**ชื่อยูสเคส** : สร้าง/แก้ไขวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด :	

เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ a. หากเป็นการแก้ไขการอัพโหลดเอกสารวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ 4. บันทึกข้อมูลวัตถุประสงค์ ขอบเขตระยะเวลา งบประมาณ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 13 อธิบายยูสเคสสร้าง/แก้ไขแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว

หมายเลขยูสเคส : UC9	**ชื่อยูสเคส** : สร้าง/แก้ไขแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	

ขั้นตอนการทำงานหลัก :

1. เลือกเมนูสร้าง/แก้ไขแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว
2. ระบบแสดงหน้าจอสำหรับอัพโหลดแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว
    a. หากเป็นการแก้ไขการอัพโหลดเอกสารแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ
    b. หากเป็นการสร้างโดยการอัพโหลดเอกสารแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลวเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น
3. อัพโหลดเอกสารแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว
4. บันทึกข้อมูลแผนและขั้นตอนปฏิบัติกรณีระบบล้มเหลว

ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 14 คำอธิบายยูสเคสสร้าง/แก้ไขแผนการทดสอบเบื้องต้น

หมายเลขยูสเคส : UC10	**ชื่อยูสเคส** : สร้าง/แก้ไขแผนการทดสอบเบื้องต้น
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขแผนการทดสอบเบื้องต้น	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขแผนการทดสอบเบื้องต้น 2. ระบบแสดงหน้าจอสำหรับอัพโหลดแผนการทดสอบเบื้องต้น a. หากเป็นการแก้ไขการอัพโหลดเอกสารแผนการทดสอบเบื้องต้น ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารแผนการทดสอบเบื้องต้นเป็นครั้ง	

แรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารแผนการทดสอบเบื้องต้น 4. บันทึกข้อมูลแผนการทดสอบเบื้องต้น
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 15 คำอธิบายยูสเคสอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

หมายเลขยูสเคส : UC11	**ชื่อยูสเคส** : อนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ 2. ระบบแสดงหน้าจอสำหรับอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ โดยแสดงไฟล์ของข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ a. หากอนุมัติ กดปุ่มเพื่ออนุมัติข้อกำหนดหนดนี้ b. หากไม่อนุมัติ กดปุ่มไม่อนุมัติ เพื่อสามารถใส่รายละเอียดของเหตุผลที่ไม่อนุมัติ 3. บันทึกข้อมูลการอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 16 คำอธิบายยูสเคสสร้าง/แก้ไขข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

หมายเลขยูสเคส : UC12	**ชื่อยูสเคส** : สร้าง/แก้ไขข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
ผู้เกี่ยวข้องหลัก : ผู้พัฒนาระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	
ความสัมพันธ์ : Association : ผู้พัฒนาระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ a. หากเป็นการแก้ไขการอัพโหลดเอกสารข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ 4. บันทึกข้อมูลข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 17 คำอธิบายยูสเคสสร้างและแก้ไขนโยบายขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร

หมายเลขยูสเคส : UC13	**ชื่อยูสเคส** : สร้างและแก้ไขนโยบาย

	ขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขนโยบายขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร	
ความสัมพันธ์ : Association : ผู้บริหารองค์กร Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้างและแก้ไขนโยบาย ขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของนโยบาย ขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลนโยบาย ขั้นตอนปฏิบัติ และมาตรการป้องกันปัญหาแลกเปลี่ยนสารสนเทศระหว่างองค์กร	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 18 คำอธิบายยูสเคสสร้าง/แก้ไขมาตรการรักษาความปลอดภัยระหว่างองค์กร

หมายเลขยูสเคส : UC14	**ชื่อยูสเคส** : สร้าง/แก้ไขมาตรการรักษาความปลอดภัยระหว่างองค์กร
ผู้เกี่ยวข้องหลัก : ผู้บริหารองค์กร	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขมาตรการรักษาความปลอดภัยระหว่างองค์กร	

ความสัมพันธ์ : Association : ผู้บริหารองค์กร Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขมาตรการรักษาความปลอดภัยระหว่างองค์กร 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของมาตรการรักษาความปลอดภัยระหว่างองค์กร และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลมาตรการรักษาความปลอดภัยระหว่างองค์กร
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 19 คำอธิบายยูสเคสสร้าง/แก้ไขนโยบายและมาตรการควบคุมการเข้าถึง

หมายเลขยูสเคส : UC15	**ชื่อยูสเคส** : สร้าง/แก้ไขนโยบายและมาตรการควบคุมการเข้าถึง
ผู้เกี่ยวข้องหลัก : ผู้บริหารสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขนโยบายและมาตรการควบคุมการเข้าถึง	
ความสัมพันธ์ : Association : ผู้บริหารสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขนโยบายและมาตรการควบคุมการเข้าถึง 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของนโยบายและมาตรการควบคุมการเข้าถึง และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว	

เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลนโยบายและมาตรการควบคุมการเข้าถึง
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 20 คำอธิบายยูสเคสสร้าง/แก้ไขแผนกำหนดความต้องการสารสนเทศ

หมายเลขยูสเคส : UC16	**ชื่อยูสเคส** : สร้าง/แก้ไขแผนกำหนดความต้องการสารสนเทศ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขแผนกำหนดความต้องการสารสนเทศ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขแผนกำหนดความต้องการสารสนเทศ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดแผนการทดสอบเบื้องต้น a. หากเป็นการแก้ไขการอัพโหลดเอกสารแผนการทดสอบเบื้องต้น ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารแผนการทดสอบเบื้องต้นเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารแผนการทดสอบเบื้องต้น 4. บันทึกข้อมูลแผนการทดสอบเบื้องต้น	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 21 คำอธิบายยูสเคสสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความปลอดภัย

หมายเลขยูสเคส : UC17	**ชื่อยูสเคส** : สร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความปลอดภัย

ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความปลอดภัย
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความปลอดภัย 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของสิ่งที่เกี่ยวข้องกับความปลอดภัย และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลสิ่งที่เกี่ยวข้องกับความปลอดภัย
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 22 คำอธิบายยูสเคสสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความเสี่ยง

หมายเลขยูสเคส : UC18	**ชื่อยูสเคส** : สร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความเสี่ยง
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความเสี่ยง	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก :	

1. เลือกเมนูสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความเสี่ยง 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของสิ่งที่เกี่ยวข้องกับความเสี่ยง และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลสิ่งที่เกี่ยวข้องกับความเสี่ยง
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 23 คำอธิบายยูสเคสสร้าง/แก้ไขการประเมินความเสี่ยง

หมายเลขยูสเคส : UC19	**ชื่อยูสเคส** : สร้าง/แก้ไขการประเมินความเสี่ยง
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขการประเมินความเสี่ยง	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขสิ่งที่เกี่ยวข้องกับความเสี่ยง 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของสิ่งที่เกี่ยวข้องกับความเสี่ยง และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากองค์กรมีวิธีการประเมินความเสี่ยงอยู่แล้ว ใส่เพียงผลการประเมินความเสี่ยง b. หากองค์กรไม่มีวิธีการประเมินความเสี่ยง ระบบจะแสดงเทมเพลตการประเมินความเสี่ยง 3. บันทึกข้อมูลการประเมินความเสี่ยง	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 24 คำอธิบายยูสเคสอนุมัติรายละเอียดของการออกแบบระบบ

หมายเลขยูสเคส : UC20	**ชื่อยูสเคส** : อนุมัติรายละเอียดของการออกแบบระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการอนุมัติรายละเอียดของการออกแบบระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูอนุมัติข้อรายละเอียดของการออกแบบระบบ 2. ระบบแสดงหน้าจอสำหรับอนุมัติรายละเอียดของการออกแบบระบบ โดยแสดงไฟล์ของรายละเอียดของการออกแบบระบบ a. หากอนุมัติ กดปุ่มเพื่ออนุมัติข้อกำหนดหนดนี้ b. หากไม่อนุมัติ กดปุ่มไม่อนุมัติ เพื่อสามารถใส่รายละเอียดของเหตุผลที่ไม่อนุมัติ 3. บันทึกข้อมูลการอนุมัติรายละเอียดของการออกแบบระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 25 คำอธิบายยูสเคสสร้าง/แก้ไขรายละเอียดของการออกแบบระบบ

หมายเลขยูสเคส : UC21	**ชื่อยูสเคส** : สร้าง/แก้ไขรายละเอียดของการออกแบบระบบ
ผู้เกี่ยวข้องหลัก : ผู้พัฒนาระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขรายละเอียดของการออกแบบระบบ	
ความสัมพันธ์ : Association : ผู้พัฒนาระบบ	

Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดของการออกแบบระบบ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดรายละเอียดของการออกแบบระบบ a. หากเป็นการแก้ไขการอัพโหลดเอกสารรายละเอียดของการออกแบบระบบ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารรายละเอียดของการออกแบบระบบเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารรายละเอียดของการออกแบบระบบ 4. บันทึกข้อมูลรายละเอียดของการออกแบบระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 26 คำอธิบายยูสเคสสร้างและแก้ไขนโยบายควบคุมการใช้งานการเข้ารหัส

หมายเลขยูสเคส : UC22	**ชื่อยูสเคส** : สร้างและแก้ไขนโยบายนโยบายควบคุมการใช้งานการเข้ารหัส
ผู้เกี่ยวข้องหลัก : ผู้บริหารสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขนโยบายควบคุมการใช้งานการเข้ารหัส	
ความสัมพันธ์ : Association : ผู้บริหารสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้างและแก้ไขนโยบายควบคุมการใช้งานการเข้ารหัส 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของนโยบายควบคุมการใช้งานการเข้ารหัส และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง	

a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลนโยบายควบคุมการใช้งานการเข้ารหัส
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 27 คำอธิบายยูสเคสสร้าง/แก้ไขรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส

หมายเลขยูสเคส : UC23	**ชื่อยูสเคส** : สร้าง/แก้ไขรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลรายละเอียดการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้า/ถอดรหัส	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 28 คำอธิบายยูสเคสสร้าง/แก้ไขการประเมินการทดสอบย่อย

หมายเลขยูสเคส : UC24	**ชื่อยูสเคส** : สร้าง/แก้ไขการประเมินการทดสอบย่อย
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขการประเมินการทดสอบย่อย	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขการประเมินการทดสอบย่อย 2. ระบบแสดงเทมเพลตสำหรับกรอกรายละเอียดของการประเมินการทดสอบย่อย และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการประเมินการทดสอบย่อย	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 29 คำอธิบายยูสเคสสร้าง/แก้ไขการประเมินความเสี่ยง

หมายเลขยูสเคส : UC25	**ชื่อยูสเคส** : สร้าง/แก้ไขการประเมินความเสี่ยง
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขการประเมินความเสี่ยง	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend :	

Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขการประเมินความเสี่ยง 2. ระบบแสดงหน้าจอของระบบย่อยของการประเมินความเสี่ยง(ใครตรวจอะไร เมื่อไหร่ วันไหน โมดูลอะไร คือแทรคกิ้งได้นั่นเอง)
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 30 คำอธิบายยูสเคสสร้าง/แก้ไขขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ

หมายเลขยูสเคส : UC26	**ชื่อยูสเคส** : สร้าง/แก้ไขขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ a. หากเป็นการแก้ไขการอัพโหลดเอกสารขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ	

4. บันทึกข้อมูลขั้นตอนปฏิบัติควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 31 คำอธิบายยูสเคสอนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก

หมายเลขยูสเคส : UC27	**ชื่อยูสเคส** : อนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการอนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูอนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก 2. ระบบแสดงหน้าจอสำหรับอนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก โดยแสดงไฟล์ของกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก a. หากอนุมัติ กดปุ่มเพื่ออนุมัติ b. หากไม่อนุมัติ กดปุ่มไม่อนุมัติ เพื่อสามารถใส่รายละเอียดของเหตุผลที่ไม่อนุมัติ 3. บันทึกข้อมูลการอนุมัติกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 32 คำอธิบายยูสเคสอนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ

หมายเลขยูสเคส : UC28	**ชื่อยูสเคส** : อนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการอนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูอนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ 2. ระบบแสดงหน้าจอสำหรับอนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ โดยแสดงไฟล์ของกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก a. หากอนุมัติ กดปุ่มเพื่ออนุมัติ b. หากไม่อนุมัติ กดปุ่มไม่อนุมัติ เพื่อสามารถใส่รายละเอียดของเหตุผลที่ไม่อนุมัติ 3. บันทึกข้อมูลการอนุมัติข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 33 คำอธิบายยูสเคสสร้าง/แก้ไขมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ

หมายเลขยูสเคส : UC29	**ชื่อยูสเคส** : สร้าง/แก้ไขมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ
ผู้เกี่ยวข้องหลัก : ผู้พัฒนาระบบ	
รายละเอียด :	

เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ
ความสัมพันธ์ : Association : ผู้พัฒนาระบบ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ a. หากเป็นการแก้ไขการอัพโหลดเอกสารมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ 4. บันทึกข้อมูลมาตรการรองรับไม่ให้มีการเปลี่ยนแปลงข้อความ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 34 คำอธิบายยูสเคสสร้าง/แก้ไขกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก

หมายเลขยูสเคส : UC30	**ชื่อยูสเคส** : สร้าง/แก้ไขกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก
ผู้เกี่ยวข้องหลัก : ผู้พัฒนาระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก	
ความสัมพันธ์ : Association : ผู้พัฒนาระบบ	

Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลรายละเอียดกลไกการตรวจสอบข้อมูลเข้า ข้อมูลระหว่างประมวลผล ความถูกต้องของข้อความและข้อมูลออก
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 35 คำอธิบายยูสเคสสร้าง/แก้ไขข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ

หมายเลขยูสเคส : UC31	**ชื่อยูสเคส** : สร้าง/แก้ไขข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ
ผู้เกี่ยวข้องหลัก : ผู้พัฒนาระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ	
ความสัมพันธ์ : Association : ผู้พัฒนาระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบ	

ระบบ a. หากเป็นการแก้ไขการอัพโหลดเอกสารข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ 4. บันทึกข้อมูลข้อมูลการป้องกันควบคุมข้อมูลที่ใช้ในการทดสอบระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 36 คำอธิบายยูสเคสสร้างและแก้ไขมาตรการรองรับความเสี่ยง

หมายเลขยูสเคส : UC32	**ชื่อยูสเคส** : สร้างและแก้ไขมาตรการรองรับความเสี่ยง
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขมาตรการรองรับความเสี่ยง	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขมาตรการรองรับความเสี่ยง 2. ระบบแสดงหน้าจอสำหรับอัพโหลดมาตรการรองรับความเสี่ยง a. หากเป็นการแก้ไขการอัพโหลดเอกสารมาตรการรองรับความเสี่ยง ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารมาตรการรองรับความเสี่ยงเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น	

3. อัพโหลดเอกสารมาตรการรองรับความเสี่ยง 4. บันทึกข้อมูลมาตรการรองรับความเสี่ยง
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 37 คำอธิบายยูสเคสสร้าง/แก้ไขเกณฑ์ในการตรวจรับระบบ

หมายเลขยูสเคส : UC33	**ชื่อยูสเคส** : สร้าง/แก้ไขเกณฑ์ในการตรวจรับระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขเกณฑ์ในการตรวจรับระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขเกณฑ์ในการตรวจรับระบบ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของเกณฑ์ในการตรวจรับระบบและสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลเกณฑ์ในการตรวจรับระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 38 คำอธิบายยูสเคสสร้าง/แก้ไขรายละเอียดการทดสอบการยอมรับระบบ

หมายเลขยูสเคส : UC34	**ชื่อยูสเคส** : สร้าง/แก้ไขรายละเอียดการทดสอบการยอมรับระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด :	

เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขรายละเอียดการทดสอบการยอมรับระบบ
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดการทดสอบการยอมรับระบบ 2. ระบบแสดงเทมเพลตสำหรับกรอกรายละเอียดการทดสอบการยอมรับระบบ และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการทดสอบการยอมรับระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 39 คำอธิบายยูสเคสสร้าง/แก้ไขการทดสอบความปลอดภัยของระบบ

หมายเลขยูสเคส : UC35	**ชื่อยูสเคส** : สร้าง/แก้ไขการทดสอบความปลอดภัยของระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศและผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขการทดสอบความปลอดภัยของระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศและผู้ดูแลระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดการทดสอบความปลอดภัยของระบบ 2. ระบบแสดงเทมเพลตสำหรับกรอกรายละเอียดการทดสอบความปลอดภัยของระบบและสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง	

a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการทดสอบความปลอดภัยของระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 40 คำอธิบายยูสเคสอนุมัติคู่มือการใช้งานระบบ

หมายเลขยูสเคส : UC36	**ชื่อยูสเคส** : อนุมัติคู่มือการใช้งานระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการอนุมัติคู่มือการใช้งานระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูอนุมัติคู่มือการใช้งานระบบ 2. ระบบแสดงหน้าจอสำหรับอนุมัติกลไกคู่มือการใช้งานระบบ โดยแสดงไฟล์ของคู่มือการใช้งานระบบ a. หากอนุมัติ กดปุ่มเพื่ออนุมัติ b. หากไม่อนุมัติ กดปุ่มไม่อนุมัติ เพื่อสามารถใส่รายละเอียดของเหตุผลที่ไม่อนุมัติ 3. บันทึกข้อมูลการอนุมัติคู่มือการใช้งานระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 41 คำอธิบายยูสเคสสร้างและแก้ไขรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ

หมายเลขยูสเคส : UC37	**ชื่อยูสเคส** : สร้างและแก้ไขรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	

รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดการทดสอบส่วนประกอบย่อยของระบบ 2. ระบบแสดงเทมเพลตสำหรับกรอกรายละเอียดการทดสอบส่วนประกอบย่อยของระบบและสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการทดสอบส่วนประกอบย่อยของระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 42 คำอธิบายยูสเคสสร้าง/แก้ไขคู่มือการใช้งานระบบ

หมายเลขยูสเคส : UC38	**ชื่อยูสเคส** : สร้างและแก้ไขคู่มือการใช้งานระบบ
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขคู่มือการใช้งานระบบ	
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขคู่มือการใช้งานระบบ	

2. ระบบแสดงหน้าจอของระบบย่อยของคู่มือการใช้งานระบบ(Update คู่มือได้ โดยระบุว่าเป็นคู่มือของ Source Code Version ไหน)
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 43 คำอธิบายยูสเคสสร้างและแก้ไขแผนการนำไปใช้

หมายเลขยูสเคส : UC39	**ชื่อยูสเคส** : สร้างและแก้ไขแผนการนำไปใช้
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขแผนการนำไปใช้	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขแผนการนำไปใช้ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดแผนการนำไปใช้ a. หากเป็นการแก้ไขการอัพโหลดเอกสารแผนการนำไปใช้ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารแผนการนำไปใช้เป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารแผนการนำไปใช้ 4. บันทึกข้อมูลแผนการนำไปใช้	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 44 คำอธิบายยูสเคสสร้างและแก้ไขขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

หมายเลขยูสเคส : UC40	**ชื่อยูสเคส** : สร้างและแก้ไขขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	

รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไข 2. ระบบแสดงหน้าจอของระบบย่อยของขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไข(version control source code)
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 45 คำอธิบายยูสเคสสร้างและแก้ไขการควบคุมการแปลงข้อมูลเข้า/ออก

หมายเลขยูสเคส : UC41	**ชื่อยูสเคส** : สร้างและแก้ไขการควบคุมการแปลงข้อมูลเข้า/ออก
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขการควบคุมการแปลงข้อมูลเข้า/ออก	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้างและแก้ไขการควบคุมการแปลงข้อมูลเข้า/ออก 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของการควบคุมการแปลงข้อมูลเข้า/ออก และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง	

a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการควบคุมการแปลงข้อมูลเข้า/ออก
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 46 คำอธิบายยูสเคสสร้างและแก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ

หมายเลขยูสเคส : UC42	**ชื่อยูสเคส** : สร้างและแก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ
ผู้เกี่ยวข้องหลัก : ผู้บริหารสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้างและแก้ไขขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลขั้นตอนปฏิบัติการตรวจสอบการใช้งานสารสนเทศ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 47 คำอธิบายยูสเคสสร้าง/แก้ไขนโยบายการใช้งานบริการเครือข่าย

หมายเลขยูสเคส : UC43	**ชื่อยูสเคส** : สร้าง/แก้ไขนโยบายการใช้งานบริการเครือข่าย
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	

รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขนโยบายการใช้งานบริการเครือข่าย
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดนโยบายการใช้งานบริการเครือข่าย 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของนโยบายการใช้งานบริการเครือข่าย และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลรายละเอียดนโยบายการใช้งานบริการเครือข่าย
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 48 คำอธิบายยูสเคสสร้าง/แก้ไขการประเมินการทดสอบย่อย

หมายเลขยูสเคส : UC44	**ชื่อยูสเคส** : สร้าง/แก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก :	

1. เลือกเมนูสร้าง/แก้ไขมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ 2. ระบบแสดงหน้าจอของระบบย่อยของมาตรการป้องกันข้อมูลบันทึกกิจกรรมต่างๆ ที่เกิดขึ้นในระบบ(กำหนดสิทธิ์ว่าใครจะดูอะไรได้บ้าง เป็น application log)
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 49 คำอธิบายยูสเคสสร้าง/แก้ไขขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งาน

หมายเลขยูสเคส : UC45	**ชื่อยูสเคส** : สร้าง/แก้ไขขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งานง
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งาน	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งาน 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งาน และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้วเพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลรายละเอียดขั้นตอนสำหรับยกเลิกสิทธิ์การใช้งาน	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 50 คำอธิบายยูสเคสสร้าง/แก้ไขขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่

หมายเลขยูสเคส : UC46	**ชื่อยูสเคส** : สร้าง/แก้ไขขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	

รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่บ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่ a. หากเป็นการแก้ไขการอัพโหลดเอกสารขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้ว เพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่เป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่ 4. บันทึกข้อมูลขั้นตอนการกำหนดสิทธิ์ต่างๆ ในการใช้งานให้กับพนักงานใหม่
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 51 คำอธิบายยูสเคสตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ

หมายเลขยูสเคส : UC47	**ชื่อยูสเคส** : ตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ	

ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขการตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของการตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการตรวจสอบการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 52 คำอธิบายยูสเคสตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ

หมายเลขยูสเคส : UC48	**ชื่อยูสเคส** : ตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขการตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของการตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง	

a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการตรวจสอบการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 53 คำอธิบายยูสเคสตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ

หมายเลขยูสเคส : UC49	**ชื่อยูสเคส** : ตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขการตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของการตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการตรวจสอบการบันทึกเหตุการณ์ที่ผิดพลาดที่เกี่ยวข้องกับการใช้งานระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 54 คำอธิบายยูสเคสสร้าง/แก้ไขรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ

หมายเลขยูสเคส : UC50	**ชื่อยูสเคส** : สร้าง/แก้ไขรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้าง/แก้ไขรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ 2. ระบบแสดงหน้าจอสำหรับอัพโหลดเอกสารรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ a. หากเป็นการแก้ไขการอัพโหลดเอกสารรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ ระบบจะแสดงเอกสารเดิมที่ถูกอัพโหลดไปแล้วเพื่อลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ b. หากเป็นการสร้างโดยการอัพโหลดเอกสารรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบเป็นครั้งแรก ระบบจะแสดงหน้าจอสำหรับการอัพโหลดเอกสารเท่านั้น 3. อัพโหลดเอกสารรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ 4. บันทึกข้อมูลรายละเอียดของกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 55 คำอธิบายยูสเคสอนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

หมายเลขยูสเคส : UC51	**ชื่อยูสเคส** : อนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการอนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูอนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน 2. ระบบแสดงหน้าจอสำหรับอนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยแสดงไฟล์ของรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน a. หากอนุมัติ กดปุ่มเพื่ออนุมัติ b. หากไม่อนุมัติ กดปุ่มไม่อนุมัติ เพื่อสามารถใส่รายละเอียดของเหตุผลที่ไม่อนุมัติ 3. บันทึกข้อมูลการอนุมัติรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 56 คำอธิบายยูสเคสสร้างและแก้ไขมาตรการป้องกันภัยคุกคามทางเครือข่าย

หมายเลขยูสเคส : UC52	**ชื่อยูสเคส** : สร้างและแก้ไขมาตรการป้องกันภัยคุกคามทางเครือข่าย
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	

รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขมาตรการป้องกันภัยคุกคามทางเครือข่าย
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขมาตรการป้องกันภัยคุกคามทางเครือข่าย 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของมาตรการป้องกันภัยคุกคามทางเครือข่าย และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไข รายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลมาตรการป้องกันภัยคุกคามทางเครือข่าย
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 57 อธิบายยูสเคสสร้างและแก้ไขมาตรการควบคุมการใช้งานระบบเคลื่อนที่

หมายเลขยูสเคส : UC53	**ชื่อยูสเคส** : สร้างและแก้ไขมาตรการควบคุมการใช้งานระบบเคลื่อนที่
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขมาตรการควบคุมการใช้งานระบบเคลื่อนที่	
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก :	

1. เลือกเมนูสร้าง/แก้ไขมาตรการควบคุมการใช้งานระบบเคลื่อนที่ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของมาตรการควบคุมการใช้งานระบบเคลื่อนที่ a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไข รายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลมาตรการควบคุมการใช้งานระบบเคลื่อนที่
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 58 คำอธิบายยูสเคสสร้างและแก้ไขมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ

หมายเลขยูสเคส : UC54	**ชื่อยูสเคส** : สร้างและแก้ไขมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ	
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง b. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไข รายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลมาตรการตรวจจับ ป้องกัน และกู้คืนระบบ	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 59 คำอธิบายยูสเคสตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง

หมายเลขยูสเคส : UC55	**ชื่อยูสเคส** : ตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง	
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง 2. ระบบแสดงหน้าจอเทมเพลตสำหรับตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไข รายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลการตรวจสอบการตั้งเวลาของเครื่องที่ระบบติดตั้ง	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 60 คำอธิบายยูสเคสกำหนดสิทธิ์การใช้งานระบบ

หมายเลขยูสเคส : UC56	**ชื่อยูสเคส** : กำหนดสิทธิ์การใช้งานระบบ
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการกำหนดสิทธิ์การใช้งานระบบ	
ความสัมพันธ์ : Association : ผู้ดูแลระบบ	

Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูกำหนดสิทธิ์การใช้งานระบบ 2. ระบบแสดงสิทธิ์ของผู้ใช้งานระบบ โดยแสดงเป็น User Access Matrix(UMS) โดยแบ่งตามประเภทผู้ใช้งาน (แสดงว่าผู้ใช้งานมีสิทธิ์ใน Function ใดของระบบ)
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 61 คำอธิบายยูสเคสสร้างและแก้ไขรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

หมายเลขยูสเคส : UC57	**ชื่อยูสเคส** : สร้างและแก้ไขรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
ผู้เกี่ยวข้องหลัก : ผู้ดูแลระบบ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน	
ความสัมพันธ์ : Association : ผู้ดูแลระบบ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้างและแก้ไขรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน 2. ระบบแสดงหน้าจอเทมเพลตสำหรับสร้างและแก้ไขรายละเอียดของกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไข	

รายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
ขั้นตอนการทำงานกรณีพิเศษ :

ตารางที่ 62 คำอธิบายยูสเคสสร้างและแก้ไขกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร

หมายเลขยูสเคส : UC58	**ชื่อยูสเคส** : สร้างและแก้ไขกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้างและแก้ไขกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร 2. ระบบแสดงหน้าจอเทมเพลตสำหรับกรอกรายละเอียดของกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร และสำหรับอัพโหลดเอกสารที่เกี่ยวข้อง a. หากเป็นการแก้ไข ระบบจะแสดงข้อมูลเดิมและเอกสารที่ถูกอัพโหลดไปแล้ว เพื่อแก้ไขรายละเอียดและลบเอกสารหรือเพิ่มเอกสารใหม่เข้าสู่ระบบ 3. บันทึกข้อมูลของกฎในการนำสินทรัพย์สารสนเทศของระบบออกนอกองค์กร	
ขั้นตอนการทำงานกรณีพิเศษ :	

ตารางที่ 63 คำอธิบายยูสเคสสร้างและแก้ไขการบันทึกการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ

หมายเลขยูสเคส : UC59	**ชื่อยูสเคส** : สร้างและแก้ไขการบันทึกการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ

ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ
รายละเอียด : เพื่ออธิบายขั้นตอนในการสร้างและแก้ไขการบันทึกการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :
ขั้นตอนการทำงานหลัก : 1. เลือกเมนูสร้าง/แก้ไขข้อมูลการบันทึกการนำเข้า/ออก ของสินทรัพย์สารสนทเศของระบบ 2. ระบบแสดงหน้าจอของระบบย่อยของการบันทึกการนำเข้า/ออก ของสินทรัพย์สารสนทเศของระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

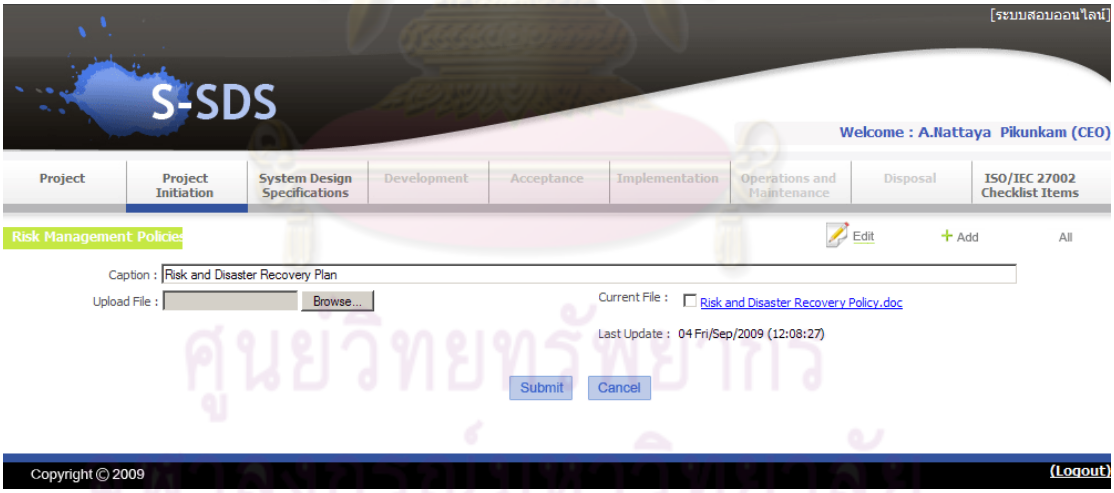
ตารางที่ 64 คำอธิบายยูสเคสตรวจสอบการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ

หมายเลขยูสเคส : UC60	**ชื่อยูสเคส** : ตรวจสอบการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ
ผู้เกี่ยวข้องหลัก : หัวหน้างานสารสนเทศ	
รายละเอียด : เพื่ออธิบายขั้นตอนในการตรวจสอบการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ	
ความสัมพันธ์ : Association : หัวหน้างานสารสนเทศ Use : Extend : Generalization :	
ขั้นตอนการทำงานหลัก :	

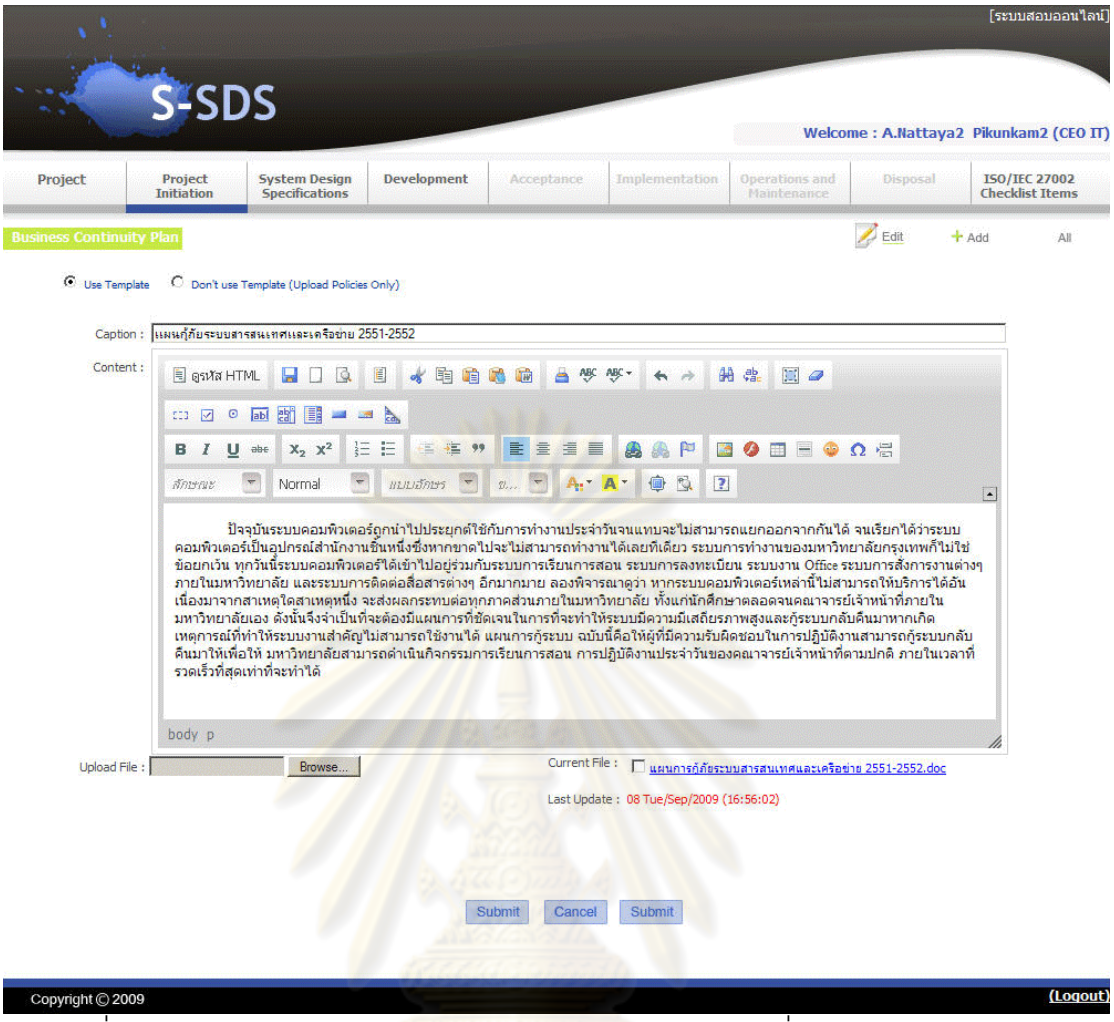
1. เลือกเมนูตรวจสอบการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ 2. ระบบแสดงหน้าจอของระบบย่อยของการบันทึกการนำเข้า/ออก ของสินทรัพย์สารสนเทศของระบบ
ขั้นตอนการทำงานกรณีพิเศษ :

ภาคผนวก ข.
ตัวอย่างหน้าจอของส่วนต่อประสานผู้ใช้

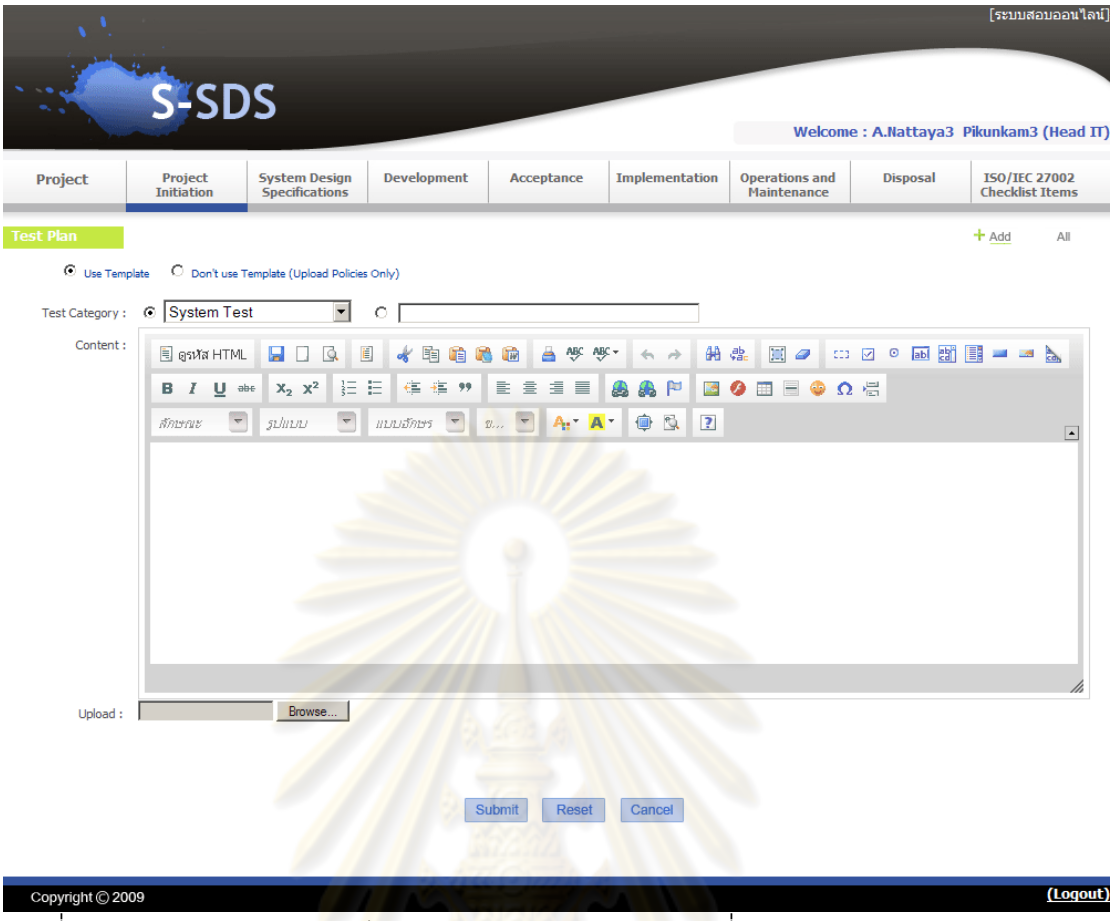
รูปที่ 22 ตัวอย่างหน้าจอการเข้าสู่ระบบ



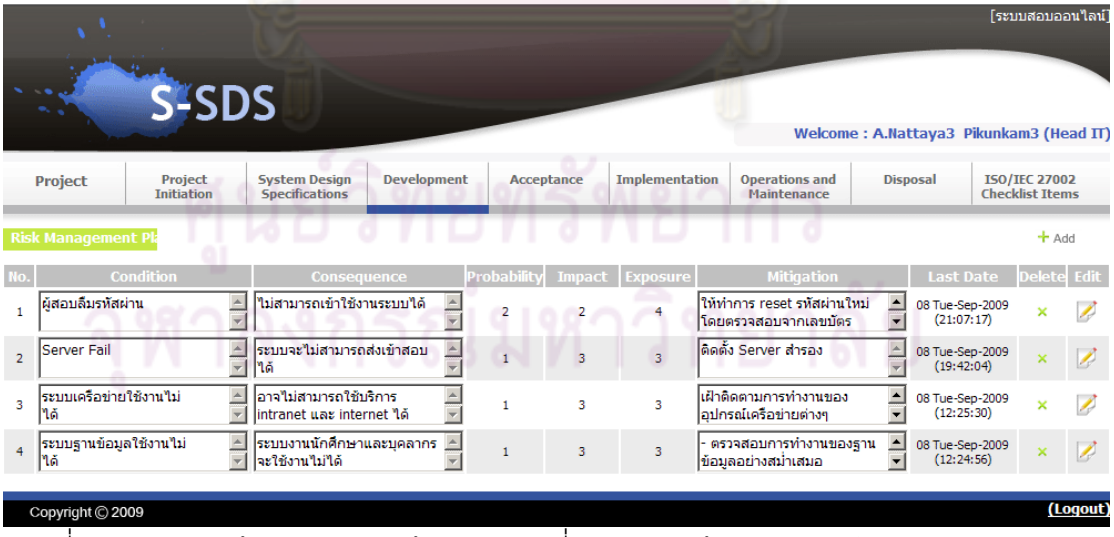
รูปที่ 23 ตัวอย่างหน้าจอการแก้ไขข้อมูลการจัดการความเสี่ยงของผู้บริหารสารองค์กรในระยะการเริ่มต้นโครงการ



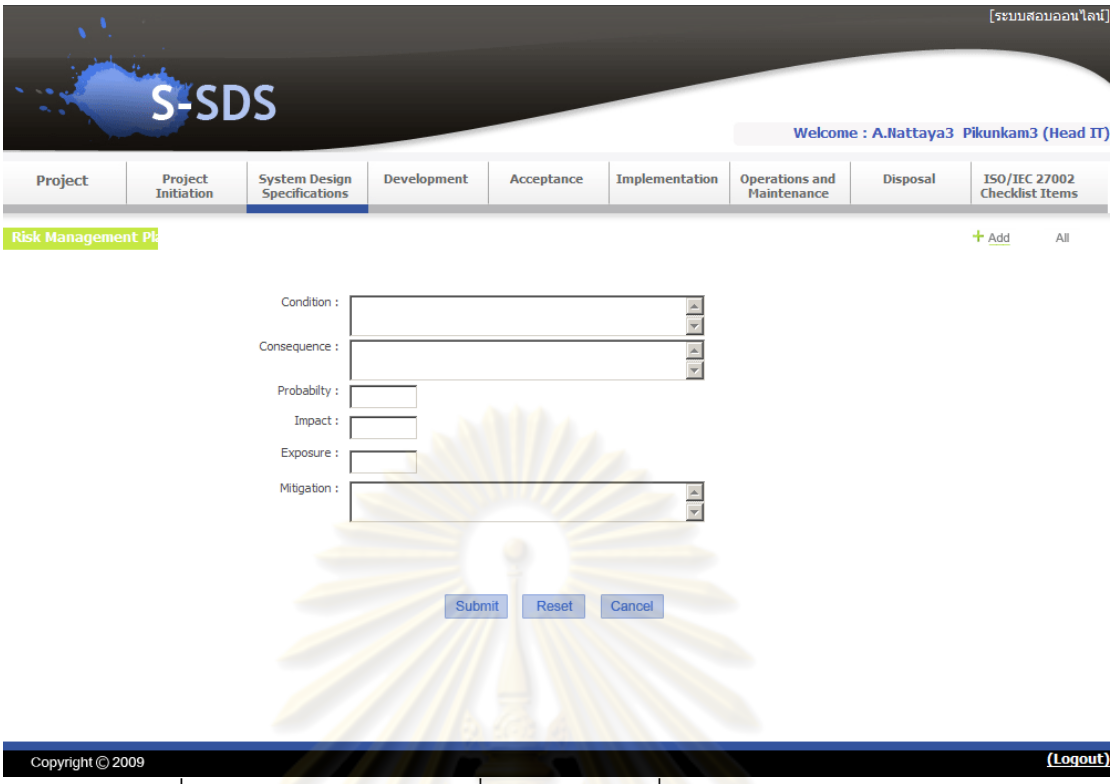
รูปที่ 24 ตัวอย่างหน้าจอการแก้ไขข้อมูลแผนการสร้างความต่อเนื่องให้ธุรกิจของผู้บริหารสารสนเทศในระยะการเริ่มต้นโครงการ



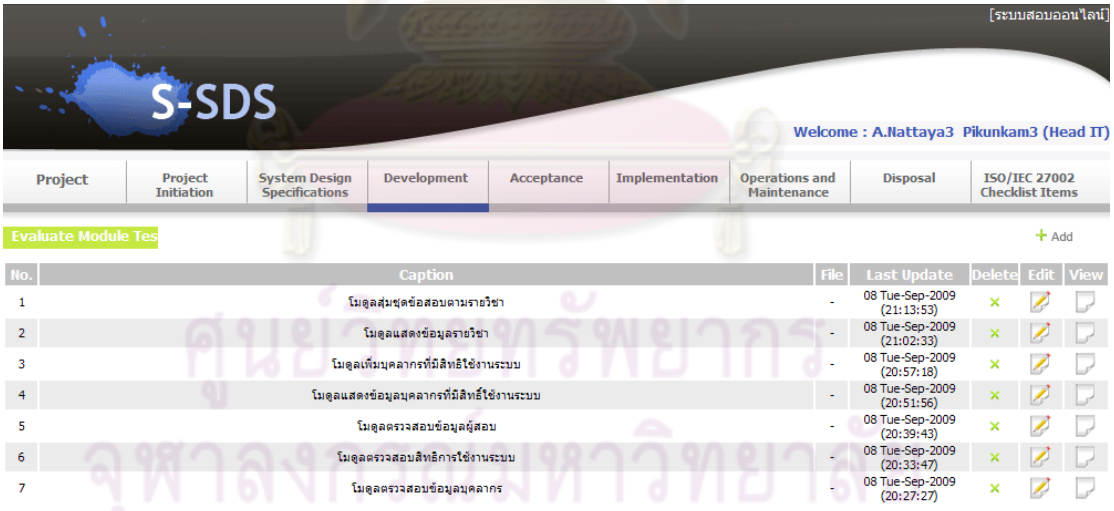
รูปที่ 25 ตัวอย่างหน้าจอการแก้ไขข้อมูลแผนการทดสอบระบบที่พัฒนาของหัวหน้าสารสนเทศในระยะการเริ่มต้นโครงการ



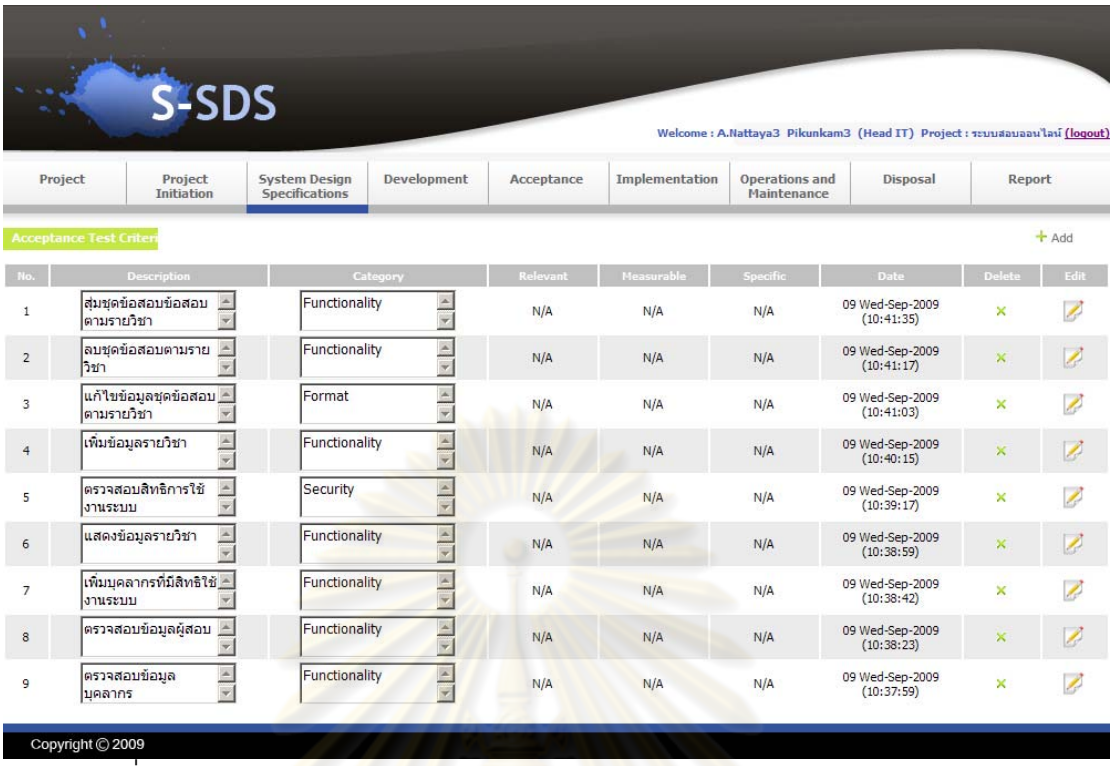
รูปที่ 26 ตัวอย่างหน้าจอการแสดงข้อมูลความเสี่ยงของหัวหน้าสารสนเทศในระยะพัฒนาระบบ



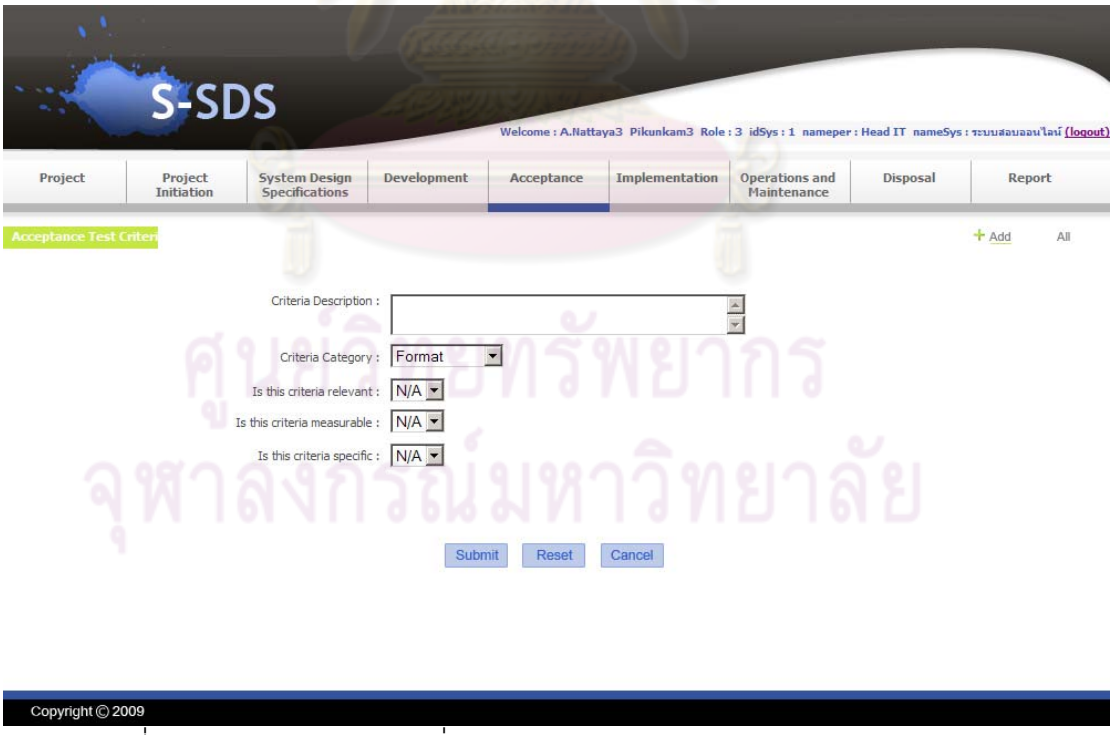
รูปที่ 27 ตัวอย่างหน้าจอการเพิ่มข้อมูลความเสี่ยงของหัวหน้าสารสนเทศในระยะการออกแบบระบบ



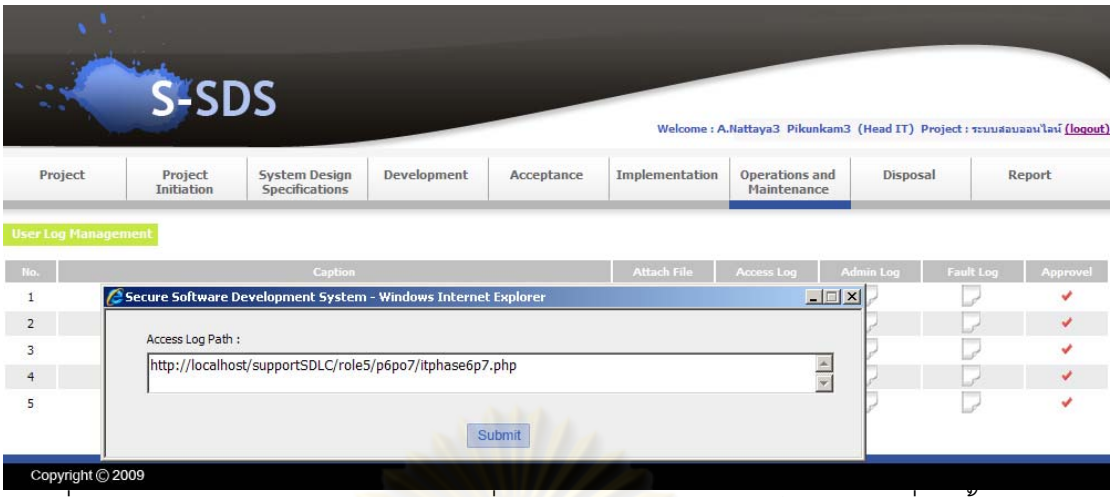
รูปที่ 28 ตัวอย่างหน้าจอการแสดงข้อมูลการทดสอบย่อยของหัวหน้าสารสนเทศในระยะพัฒนาระบบ



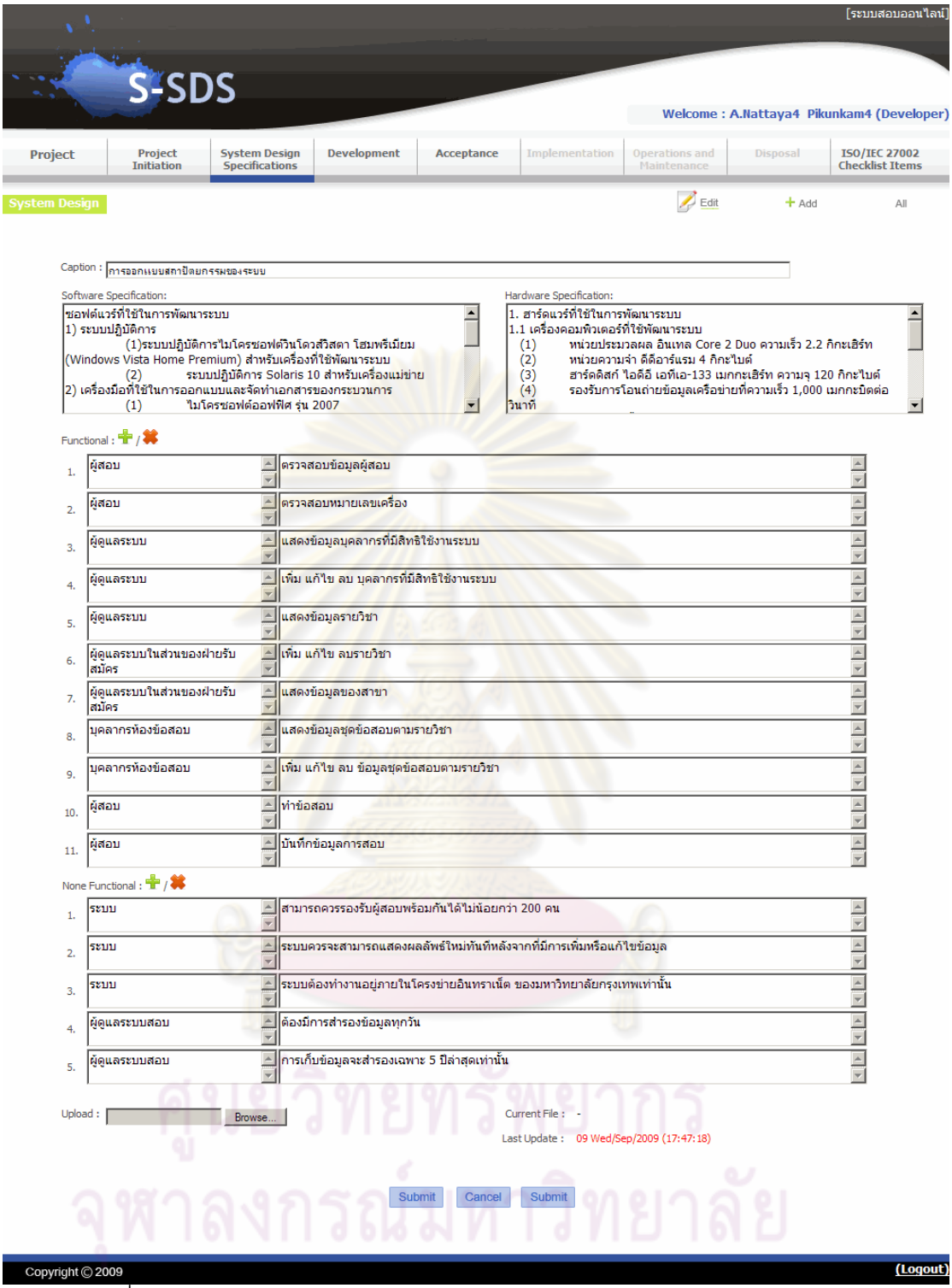
รูปที่ 29 ตัวอย่างหน้าจอการแสดงข้อมูลการยอมรับระบบของหัวหน้าสารสนเทศในระยะการยอมรับระบบ



รูปที่ 30 ตัวอย่างหน้าจอการเพิ่มข้อมูลการยอมรับระบบของหัวหน้าสารสนเทศในระยะการยอมรับระบบ



รูปที่ 31 ตัวอย่างหน้าจอการแสดงข้อมูลเรื่องการตรวจสอบการบันทึกกิจกรรมที่เกิดขึ้นในระบบของหัวหน้าสารสนเทศในระยะการบำรุงรักษา



รูปที่ 32 ตัวอย่างหน้าจอการแก้ไขข้อมูลการออกแบบระบบของผู้พัฒนาระบบในระยะพัฒนาระบบ

รูปที่ 33 ตัวอย่างหน้าจอการตรวจสอบข้อมูลการทดสอบย่อยของระบบของผู้พัฒนาระบบในระยะพัฒนาการยอมรับระบบ

รูปที่ 34 ตัวอย่างหน้าจอการแสดงรายงานความปลอดภัยของระบบ

อ้างอิงตามมาตรฐานไอเอสโอ/ไออีซี 27002

ภาคผนวก ค.
พจนานุกรมข้อมูลของระบบฐานข้อมูล

ตารางที่ 65 ตาราง dd_permis

ชื่อ	dd_permis		
คำอธิบาย	ค่าคงที่รหัสของสิทธิ์การเข้าถึงระบบ		
คีย์หลัก	id_permiss		
ความสัมพันธ์	user_permis		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
id_permiss	int(3)	ไม่ได้	รหัสของสิทธิ์การเข้าถึงระบบ
namePer	varchar(50)	ได้	ชื่อสิทธิ์การเข้าถึงระบบ

ตารางที่ 66 ตาราง dd_phase1

ชื่อ	dd_phase1		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะเริ่มต้นโครงการ		
คีย์หลัก	id_phase1		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
id_phase1	int(2)	ไม่ได้	รหัสกระบวนการในระยะเริ่มต้นโครงการ
p1_5_1_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 5.1.1
p1_5_1_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 5.1.2
p1_6_1_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 6.1.1
p1_6_1_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 6.1.2

p1_6_1_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 6.1.3
p1_12_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.1
p1_12_1_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.1.1
p1_6_2_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 6.2.3
p1_14_1_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 14.1.3

ตารางที่ 67 ตาราง dd_phase2

ชื่อ	dd_phase2		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะออกแบบระบบ		
คีย์หลัก	Id_phase2		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
Id_phase2	int(2)	ไม่ได้	รหัสกระบวนการในระยะออกแบบระบบ
P2_11_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 11.1
P2_11_1_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 11.1.1
P2_6_2_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 6.2.1
P2_10_8_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.8.1
P2_10_3_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.3.1

ตารางที่ 68 ตาราง dd_phase3

ชื่อ	dd_phase3		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะพัฒนา		
คีย์หลัก	Id_phase3		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
Id_phase3	int(2)	ไม่ได้	รหัสกระบวนการในระยะพัฒนา
P3_12_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.2
P3_12_2_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.2.1
P3_12_2_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.2.2
P3_12_2_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.2.3
P3_12_2_4	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.2.4
P3_12_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.3
P3_12_3_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.3.1
P3_12_3_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.3.2
P3_12_4	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.4
P3_12_4_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.4.1
P3_12_4_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.4.2

P3_12_4_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.4.3

ตารางที่ 69 ตาราง dd_phase4

ชื่อ	dd_phase4		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะการยอมรับระบบ		
คีย์หลัก	Id_phase4		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
Id_phase4	int(2)	ไม่ได้	รหัสกระบวนการในระยะการยอมรับระบบ
P4_10_3_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.3.2
P4_12_6	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.6
P4_12_6_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 12.6.1

ตารางที่ 70 ตาราง dd_phase5

ชื่อ	dd_phase5		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะการนำไปใช้จริง		
คีย์หลัก	Id_phase5		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
Id_phase5	int(2)	ไม่ได้	รหัสกระบวนการในระยะการนำไปใช้จริง
P5_12_5_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี

			27002 ข้อที่ 12.5.1

ตารางที่ 71 ตาราง dd_phase6

ชื่อ	dd_phase6		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะบำรุงรักษา		
คีย์หลัก	Id_phase6		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
Id_phase6	int(2)	ไม่ได้	รหัสกระบวนการในระยะบำรุงรักษา
P6_10_10_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10.2
P6_10_6	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.6
P6_10_6_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.6.1
P6_10_6_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.6.2
P6_10_10	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10
P6_10_10_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10.3
P6_11_2_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 11.2.1
P6_10_1_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.1.1
P6_10_10_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10.1

P6_10_10_4	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10.4
P6_10_10_5	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10.5
P6_11_2_4	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 11.2.4
P6_10_4	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.4
P6_10_4_2	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.4.2
P6_10_4_1	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.4.1
P6_10_10_6	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 10.10.6
P6_11	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 11
P6_11_2_3	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 11.2.3

ตารางที่ 72 ตาราง dd_phase7

ชื่อ	dd_phase7		
คำอธิบาย	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ที่เกี่ยวข้องกับกระบวนการในระยะจัดการแทนที่ระบบ		
คีย์หลัก	id_phase7		
ความสัมพันธ์	dd_iso		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
Id_phase7	int(2)	ไม่ได้	รหัสกระบวนการในระยะจัดการแทนที่ระบบ
P7_9_2_6	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี

			27002 ข้อที่ 9.2.6
P7_9_2_7	varchar(100)	ได้	ชื่อของข้อระบุไอเอสโอ/ไออีซี 27002 ข้อที่ 9.2.7

ตารางที่ 73 ตาราง history_system

ชื่อ	history_system		
คำอธิบาย	ชื่อของระบบ		
คีย์หลัก	id_system		
ความสัมพันธ์	uc1_1, uc2_1, uc3_1, uc4_1, uc6_1, uc7_1, uc8_1, uc9_1, uc10_1, uc12_1, uc1_2, uc2_2, uc3_2, uc4_2, uc5_2, uc6_2, uc9_2, uc1_3, uc2_3, uc3_3, uc4_3, uc5_3, uc8_3, uc9_3, uc10_3, uc1_4, uc2_4, uc3_4, uc4_4, uc6_4, uc7_4, uc1_5, uc2_5, uc3_5, uc1_6, uc2_6, uc3_6, uc6_6, uc9_6, uc11_6, uc12_6, uc13_6, uc14_6, uc16_6, uc17_6, uc1_7, uc5_1		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
id_system	int(3)	ไม่ได้	รหัสของระบบ
nameSys	varchar(100)	ไม่ได้	ชื่อของระบบ
startDate	varchar(50)	ไม่ได้	วันที่เริ่มกรอกข้อมูลระบบ
endDate	varchar(50)	ไม่ได้	วันที่สิ้นสุดการกรอกข้อมูลระบบ
Id_iso	varchar(5)	ไม่ได้	รหัสไอเอสโอ/ไออีซี 27002
id_user	varchar(6)	ไม่ได้	ชื่อของผู้กรอกชื่อระบบ
statusProject	varchar(1)	ไม่ได้	สถานะของระบบ ดังนี้ 0=ไม่ใช้งาน, 1-ใช้งาน

ตารางที่ 74 ตาราง phase_iso

ชื่อ	phase_iso
คำอธิบาย	สถานะการกรอกข้อมูลปัจจุบัน
คีย์หลัก	id_update

ความสัมพันธ์	history_system, user_permis, dd_phase1, dd_phase2, dd_phase3, dd_phase4, dd_phase5, dd_phase6, dd_phase7		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
id_update	int(3)	ไม่ได้	รหัสของสถานะ
id_phase	varchar(2)	ไม่ได้	รหัสของระยะกระบวนการ
id_user	varchar(6)	ไม่ได้	รหัสของผู้ใช้งาน
policies	varchar(2)	ไม่ได้	ลำดับข้อมูลที่กรอกล่าสุด
id_system	int(3)	ไม่ได้	รหัสระบบ

ตารางที่ 75 ตาราง user_permis

ชื่อ	user_permis		
คำอธิบาย	รายละเอียดของผู้ใช้งาน		
คีย์หลัก	id_user		
ความสัมพันธ์	dd_permis, history_system, uc1_1, uc2_1, uc3_1, uc4_1, uc6_1, uc7_1, uc8_1, uc9_1, uc10_1, uc12_1, uc1_2, uc2_2, uc3_2, uc4_2, uc5_2, uc6_2, uc9_2, uc1_3, uc2_3, uc3_3, uc4_3, uc5_3, uc6_3, uc8_3, uc9_3, uc10_3, uc1_4, uc2_4, uc3_4, uc4_4, uc6_4, uc7_4, uc1_5, uc2_5, uc3_5, uc1_6, uc2_6, uc3_6, uc6_6, uc9_6, uc11_6, uc12_6, uc13_6, uc14_6, uc16_6, uc17_6, uc1_7, uc5_1		
ชื่อสดมภ์	**ประเภทข้อมูล**	**ค่าเป็น null**	**หมายเหตุ**
id_user	varchar(6)	ไม่ได้	รหัสของผู้ใช้
fname	varchar(50)	ไม่ได้	ชื่อของผู้ใช้
lname	varchar(50)	ไม่ได้	นามสกุลของผู้ใช้
category	varchar(50)	ไม่ได้	ประเภทบุคลากร
position_acd	varchar(50)	ไม่ได้	ตำแหน่งวิชาการ
position	varchar(50)	ไม่ได้	ตำแหน่งของผู้ใช้

uname	varchar(20)	ไม่ได้	ชื่อใช้ในการเข้าสู่ระบบ
pwd	varchar(20)	ไม่ได้	รหัสผ่านเข้าสู่ระบบ
id_permis	int(3)	ไม่ได้	รหัสสิทธิ์การใช้งานระบบ

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวเนตยา พิกุลแกม เกิดเมื่อวันที่ 3 มกราคม พ.ศ. 2524 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาหลักสูตรปริญญาวิทยาศาสตรบัณฑิต (วท.บ.) สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยกรุงเทพ ในปีการศึกษา 2546 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2550