การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์องค์กรประเภทสารสนเทศ โดยใช้แบบรูปความมั่นคง

นางสาวเมธยา ราชคมน์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

A DESIGN OF PROCESS MODEL FOR INFORMATION ASSETS OF ACCESS CONTROL USING SECURITY PATTERNS

Miss Mathaya Ratchakom

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Software Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2010

หัวข้อวิทยานิพนธ์	การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์องค์กรประเภทสารสนเทศโดยใช้แบบรูปความมั่นคง
โดย	นางสาวเมธยา ราชคมน์
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

..... กรรมการ
(รองศาสตราจารย์ ดร.ธาราทิพย์ สุวรรณศาสตร์)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.เฉลิมศักดิ์ เลิศวงศ์เสถียร)

เมธยา ราชคมน์: การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์องค์กรประเภทสารสนเทศโดยใช้แบบรูปความมั่นคง. (A DESIGN OF PROCESS MODEL FOR INFORMATION ASSETS OF ACCESS CONTROL USING SECURITY PATTERNS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. นครทิพย์ พร้อมพูล, 301 หน้า

การดำเนินการด้านเทคโนโลยีสารสนเทศขององค์กรทำให้เกิดสินทรัพย์ประเภทสารสนเทศ ซึ่งถูกจัดเก็บไว้เพื่อใช้เป็นหลักฐานสำหรับอ้างอิงที่สำคัญขององค์กร หากมีการเปลี่ยนแปลงหรือแก้ไขจากบุคคลที่ไม่มีสิทธิในการเข้าถึง ที่ก่อให้เกิดการสูญหายหรือเผยแพร่ออกนอกองค์กร อาจส่งผลกระทบต่อการดำเนินการโดยรวมและมูลค่าทางธุรกิจ ดังนั้นจึงสำคัญอย่างยิ่งที่องค์กรต้องคำนึงถึงการหาแนวทางป้องกันทางด้านความมั่นคงปลอดภัยของสินทรัพย์ประเภทสารสนเทศ โดยเฉพาะการสร้างกระบวนการและระบบการจัดการการควบคุมการเข้าถึง ทั้งนี้เพื่อควบคุมสิทธิของบุคคลในการเข้าถึงและเข้าใช้สินทรัพย์ประเภทสารสนเทศเหล่านั้น

งานวิจัยนี้ได้นำเสนอการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยใช้แบบรูปความมั่นคงและมีการอ้างอิงการดำเนินการจากมาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 27002:2005 กระบวนการดังกล่าวนั้นประกอบไปด้วย 3 ชั้นแบบจำลอง คือ ชั้นแบบจำลองกระบวนการเชิงภาพรวม ชั้นแบบจำลองกระบวนการเชิงกระแสงาน และชั้นแบบจำลองกระบวนการเชิงนิยาม พร้อมทั้งออกแบบเอกสารแผ่นแบบที่เกี่ยวข้องและพัฒนาเครื่องมือสนับสนุน ซึ่งช่วยให้การประยุกต์ใช้กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศมีประสิทธิภาพมากยิ่งขึ้น

กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและเครื่องมือที่พัฒนาขึ้นจะช่วยเป็นแนวทางให้องค์กรต่างๆ สามารถสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศ ทั้งยังช่วยลดความเสี่ยงของการเกิดผลกระทบต่อการดำเนินการขององค์กรอีกด้วย

ภาควิชา...วิศวกรรมคอมพิวเตอร์... ลายมือชื่อนิสิต.....เมธยา ราชคมน์.....

สาขาวิชา...วิศวกรรมซอฟต์แวร์..... ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก.....

ปีการศึกษา...2553.....

5070409021 : MAJOR SOFTWARE ENGINEERING

KEYWORDS: PROCESS MODEL DESIGN / SECURITY PATTERN / ACCESS CONTROL / INFORMATION ASSET

MATHAYA RATCHAKOM: A DESIGN OF PROCESS MODEL FOR INFORMATION ASSETS OF ACCESS CONTROL USING SECURITY PATTERNS. ADVISOR: ASST.PROF. NAKORNTHIP PROMPOON, 301 pp.

An information technology process of any organization produces many assets. Information assets are stored as an evidence for organizational operation. These assets may be damaged by any unexpected actions such as information modification and disruption or released to outside by unauthorized person. These actions may affect the overall operation and business value. Thus, the organizations should focus on security and safety of information assets by creating the access control management system to manage information authorization.

This thesis proposes process design for information assets access control based on security patterns and ISO/IEC 27001:2005 standard and ISO/IEC 27002:2005 standard. The proposed access control process consists of three model layers: overview layer, workflow layer, and definition layer. Moreover, the related template documents and supporting tool are also developed to help implementing the proposed access control process effectively.

The access control process for information assets proposed in this thesis helps any organizations to create security for their information assets and to reduce the risks that may impact organizational operations.

Department: Computer Engineering Student's Signature: Mathaya Ratchakom

Field of Study: Software Engineering Advisor's Signature: Nakornthip Prompoon

Academic Year: 2010

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วงด้วยความเมตตาและความช่วยเหลืออย่างยิ่งจากผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล อาจารย์ที่ปรึกษา ที่เสียสละเวลาช่วยให้คำปรึกษา ข้อคิดและคำแนะนำที่มีประโยชน์ต่องานวิจัย ตลอดจนความเอาใจใส่และความเชื่อมั่นที่อาจารย์มีให้ผู้วิจัย ซึ่งเป็นกำลังใจและเป็นแรงส่งเสริมให้ผู้วิจัยสามารถพัฒนางานวิจัยที่มีคุณภาพและมีคุณค่า

ขอขอบพระคุณอาจารย์ ดร.ยรรยง เต็งอำนวย ประธานกรรมการสอบวิทยานิพนธ์ รองศาสตราจารย์ ดร.ธาราทิพย์ สุวรรณศาสตร์ และดร.เฉลิมศักดิ์ เลิศวงศ์เสถียร กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาสละเวลาให้คำแนะนำสำหรับโครงร่างวิทยานิพนธ์และวิทยานิพนธ์ให้มีคุณภาพยิ่งขึ้น

ขอขอบพระคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่าน ที่ประสิทธิ์ประสาทความรู้อันมีค่ายิ่งแก่ผู้วิจัย

ขอขอบคุณบุคลากรในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่าน ที่ให้ข้อมูล คำแนะนำและความช่วยเหลือในการดำเนินการทั้งในเรื่องการศึกษาและการสอบวิทยานิพนธ์ได้สำเร็จลุล่วง

ขอขอบคุณ เพื่อนๆ พี่ๆ และน้องๆ ทุกคนที่ผ่านเข้ามาในชีวิตของผู้วิจัย ที่ห่วงใยและให้ความช่วยเหลือในทุกๆ ด้านจนผู้วิจัยสามารถทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วง ขอบคุณสมาชิกในห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ สำหรับน้ำใจ ความห่วงใยความช่วยเหลือและคำแนะนำที่มีประโยชน์แต่ผู้วิจัย

ขอขอบพระคุณสมาชิกในครอบครัวทุกท่าน ที่ให้การสนับสนุนและให้กำลังใจแก่ผู้วิจัยเสมอมา

และท้ายที่สุดนี้ ขอกราบขอบพระคุณบิดา มารดา ที่คอยเลี้ยงดู สั่งสอนผู้วิจัยจนเติบใหญ่ ท่านทั้งสองเปรียบเสมือนดั่งแรงผลักดันให้ผู้วิจัยมีกำลังใจในการดำรงชีวิต เป็นดั่งแสงสว่างในทุกๆ ครั้งที่ผู้วิจัยเกิดความท้อแท้ใจ เป็นดั่งความหวังให้ผู้จัยมีกำลังที่จะลุกขึ้นสู้ต่อไป ไม่ว่าจะเจอปัญหาใดๆ ก็ตาม และวิทยานิพนธ์ฉบับนี้ผู้วิจัยขอมอบให้กับบิดา มารดา เป็นการตอบแทนคุณซึ่งล้นพ้นหาที่สุดมิได้ ผู้วิจัยเองขอสัญญาว่าจะประพฤติตัวเป็นบุตรที่ดีและจะสร้างสรรค์องค์ความรู้ที่ได้รับจากสถานศึกษาแห่งนี้ให้ก่อเกิดประโยชน์ต่อสังคมให้มากที่สุดเท่าที่จะมากได้ต่อไป

สารบัญ

บทที่ หน้า

สารบัญตาราง

หน้า

หน้า

หน้า

หน้า

หน้า

หน้า

หน้า

หน้า

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

สินทรัพย์ประเภทสารสนเทศ เช่น นโยบายองค์กร ข้อมูลพนักงาน ข้อมูลลูกค้า หรือข้อมูลการทำธุรกรรม เป็นต้น มีความสำคัญอย่างยิ่งต่อองค์กรทั้งทางภาครัฐและเอกชน เนื่องจากมีผลต่อการดำเนินการโดยรวมขององค์กรและเป็นสิ่งที่กระทบต่อมูลค่าทางธุรกิจ หากมีการเปลี่ยนแปลงหรือแก้ไขสินทรัพย์ประเภทสารสนเทศดังกล่าวจากบุคคลที่ไม่มีสิทธิการเข้าถึงหรือเข้าใช้ เกิดการสูญหายหรือเผยแพร่ออกนอกองค์กรซึ่งเกิดจากความไม่หวังดีของผู้บุกรุกหรือผู้ที่ต้องการผลประโยชน์บางอย่าง อาจส่งผลกระทบต่อองค์กรอย่างมหาศาลจนเกี่ยวพันไปสู่การดำรงอยู่ขององค์กร เพื่อเป็นการป้องกันเหตุการณ์ดังกล่าวจึงมีความจำเป็นที่องค์กรจะต้องสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศของตน โดยเฉพาะการสร้างการควบคุมการเข้าถึง ทั้งนี้เพื่อควบคุมสิทธิของบุคคลในการเข้าถึงและเข้าใช้สินทรัพย์ประเภทสารสนเทศเหล่านั้น

เมื่อองค์กรเกิดความต้องการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศของตน ขั้นตอนแรกจะต้องเริ่มจากการศึกษาและทำความเข้าใจในเรื่องของความมั่นคงองค์กรที่เกี่ยวข้องกับสินทรัพย์ประเภทสารสนเทศ ทั้งในเรื่องความจำเป็นพื้นฐานทางด้านความมั่นคง ความเสี่ยงที่อาจจะเกิดขึ้น รวมถึงแนวคิด วิธีการป้องกันและบริการความมั่นคง แต่อย่างไรก็ตาม ศาสตร์ทางด้านความมั่นคงถือเป็นศาสตร์ที่มีความลึกซึ้งละเอียดอ่อน ซับซ้อนและยากต่อการทำความเข้าใจ ดังนั้นแบบรูปความมั่นคง (Security Patterns) [1, 2, 3] จึงถือเป็นตัวเลือกหนึ่งที่จะช่วยให้องค์กรมีแนวทางในการดำเนินการสร้างความมั่นคงอย่างชัดเจนมากยิ่งขึ้น โดยแบบรูปความมั่นคงนั้นได้อธิบายเกี่ยวกับแนวทางหรือผลเฉลยของปัญหาทางด้านความมั่นคงต่างๆ ซึ่งถูกแก้ปัญหาไว้ก่อนหน้านี้แล้ว สามารถที่จะนำกลับมาแก้ปัญหาใหม่ที่มีลักษณะคล้ายเดิม ซึ่งถือเป็นการสนับสนุนการนำกลับมาใช้ใหม่ (Reusable) แต่เนื่องจากแบบรูปความมั่นคงเป็นการอธิบายปัญหาที่เฉพาะเจาะจงในแต่ละปัญหาใดปัญหาหนึ่ง โดยในการนำมาประยุกต์ใช้ในการทำงานจริงนั้นจะต้องมีการอธิบายเป็นลำดับขั้นตอนของการดำเนินการ ดังนั้นองค์กรจะต้องทำการศึกษาว่า ในการออกแบบกระบวนการทางความมั่นคงนั้นจะต้องทำอย่างไรบ้าง ซึ่งมาตรฐานที่จะช่วยเป็นแนวทางในการออกแบบ นั่นคือ มาตรฐาน ISO/IEC 27001:2005 [4] และ 27002:2005 [5] ได้กล่าวถึงข้อกำหนดและข้อปฏิบัติสำหรับการสร้างความมั่นคง ซึ่งกำหนดเป็นระบบของการจัดการความมั่นคงสารสนเทศ โดยมีรายละเอียดเริ่มตั้งแต่การจัดตั้ง การปฏิบัติใช้งาน การทวนสอบ และการปรับปรุงอย่างต่อเนื่อง ทั้งนี้มาตรฐานทั้ง 2 สามารถนำมาใช้เป็นแนวทางในการ

ออกแบบกระบวนการได้อย่างเฉพาะเจาะจง เนื่องจากมีความเกี่ยวข้องกับความมั่นคงของสินทรัพย์ประเภทสารสนเทศโดยตรง

ดังนั้นงานวิจัยนี้จึงมุ่งเน้นที่จะออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยใช้แบบรูปความมั่นคงและมีการอ้างอิงการดำเนินการจากมาตรฐาน ISO/IEC 27001:2005 และ 27002:2005 ซึ่งจะทำให้การออกแบบกระบวนการมีความเป็นแบบแผนมากยิ่งขึ้น พร้อมกันนี้ยังได้ออกแบบเอกสารแผ่นแบบ (Template Documents) ที่มีความเกี่ยวข้องกับกระบวนการและพัฒนาเครื่องมือสนับสนุน ทั้งนี้เพื่อให้องค์กรสามารถนำไปประยุกต์ใช้เป็นแนวทางในการสร้างการป้องกันให้กับสินทรัพย์ประเภทสารสนเทศของตนต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1) เพื่อออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศโดยใช้แบบรูปความมั่นคง และจัดทำเอกสารแผ่นแบบที่เกี่ยวข้องตามกระบวนการดังกล่าว

2) เพื่อพัฒนาเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศตามข้อที่ 1)

1.3 ขอบเขตการวิจัย

1.3.1 ออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศโดยใช้แบบรูปความมั่นคง ซึ่งครอบคลุม 3 กลุ่ม 14 แบบรูป [3] ดังต่อไปนี้

1) **การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง** (Enterprise Security and Risk Management) เป็นกลุ่มแบบรูปความมั่นคงที่เกี่ยวข้องกับการกำหนดและการจัดการทั้ง 3 เรื่อง ได้แก่ การระบุความจำเป็นพื้นฐานด้านความมั่นคง การประเมินความเสี่ยง แนวคิดและบริการความมั่นคง ซึ่งแบบรูปในกลุ่มนี้ประกอบด้วย

1.1) **การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร** (Security Needs Identification for Enterprise Assets) เป็นแบบรูปที่เกี่ยวข้องกับความมั่นคงขององค์กร ซึ่งจะช่วยให้เข้าใจถึงความต้องการพื้นฐานด้านความมั่นคงที่จำเป็นต้องมีในองค์กร

1.2) **การกำหนดมูลค่าสินทรัพย์** (Asset Valuation) เป็นการกำหนดนัยสำคัญให้กับสินทรัพย์ขององค์กรที่เป็นเจ้าของ เพื่อระบุว่าเมื่อเกิดความเสียหายต่อสินทรัพย์ใดๆ จะส่งผลกระทบอย่างไรบ้างต่อองค์กร

1.3) **การประเมินภัยคุกคาม** (Threat Assessment) เป็นการระบุภัยคุกคามใดๆ ที่อาจมีโอกาสเกิดและมีผลกระทบต่อสินทรัพย์ โดยกำหนดเป็นความถี่ของภัยคุกคามที่อาจเกิดขึ้น

1.4) **การประเมินจุดอ่อน** (Vulnerability Assessment) เป็นการระบุจุดอ่อนซึ่งอาจเป็นเป้าหมายของภัยคุกคาม เพื่อที่ระบบสามารถเข้าไปดูแลจัดการจุดอ่อนดังกล่าว ไม่ให้เกิดการโจมตีได้โดยง่าย

1.5) **การกำหนดความเสี่ยง** (Risk Determination) เป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง ใช้ร่วมกับผลการประเมินภาวะเสี่ยง การประเมินภัยคุกคาม และการกำหนดมูลค่าสินทรัพย์ ซึ่งข้อมูลนำเข้าเหล่านี้ จะทำให้สามารถนำมาหาค่าความเสี่ยงของสินทรัพย์ได้

1.6) **แนวคิดความมั่นคงองค์กร** (Enterprise Security Approaches) เป็นการแนะนำให้องค์กรเลือกแนวทางบริหารความเสี่ยง เช่น การป้องกัน ตรวจจับ และ ตอบสนองของระบบ เป็นต้น ซึ่งมีผลต่อความต้องการความมั่งคงของสินทรัพย์ของตนที่ได้กำหนดไว้ก่อนหน้า

1.7) **บริการความมั่นคงองค์กร** (Enterprise Security Services) เป็นการแนะนำให้องค์กรเลือกบริการความมั่นคง (Security Services) ให้กับสินทรัพย์ของตน ซึ่งต้องสอดคล้องกับแนวทางความมั่นคงที่ได้กำหนดไว้ก่อนหน้า

2) **การระบุและการพิสูจน์ตัวตน** (Identification and Authentication) เป็นกลุ่มแบบรูปความมั่นคงที่มุ่งเน้นการตรวจสอบการเข้าถึงและเข้าใช้ทรัพยากรภายในระบบของผู้ใช้งาน โดยแบบรูปในกลุ่มนี้ประกอบด้วย

2.1) **ความต้องการด้านการระบุและการพิสูจน์ตัวตน** (Identification and Authentication Requirements) เป็นแบบรูปที่กำหนดความต้องการด้านการระบุและพิสูจน์ตัวตนทั่วไป ซึ่งจะช่วยให้สามารถกำหนดความต้องการได้อย่างเหมาะสมกับสถานการณ์ใดๆ ที่อาจเกิดขึ้น

2.2) **การออกแบบและใช้งานรหัสผ่าน** (Password Design and Use) แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและการพิสูจน์ตัวตน

3) **แบบจำลองควบคุมการเข้าถึง** (Access Control Models) เป็นกลุ่มแบบรูปความมั่นคงที่มุ่งเน้นการควบคุมการเข้าถึงทรัพยากรภายในระบบ โดยกำหนดเป็นเงื่อนไข

ข้อบังคับในระดับต่างๆ ทั้งระดับสถาปัตยกรรม ระดับโปรแกรมประยุกต์ และระดับล่างของการปฏิบัติงาน โดยแบบรูปในกลุ่มนี้ประกอบด้วย

3.1) **การให้อำนาจ** (Authorization) แบบรูปนี้ช่วยในการกำหนดว่าใครที่จะได้สิทธิในการเข้าถึงทรัพยากรภายในระบบ ภายใต้สภาพแวดล้อมที่ต้องมีการควบคุมการเข้าถึงและเข้าใช้ทรัพยากรของระบบ

3.2) **การควบคุมการเข้าถึงเชิงบทบาท** (Role-Based Access Control) แบบรูปนี้เป็นการกำหนดสิทธิบนพื้นฐานของฟังก์ชันของผู้ใช้งาน ภายใต้สภาพแวดล้อมที่ต้องมีการควบคุมการเข้าถึงและเข้าใช้ทรัพยากรของระบบ

3.3) **ความมั่นคงหลายระดับ** (Multilevel Security) แบบรูปนี้เป็นการอธิบายว่าจะทำการจัดกลุ่มข้อมูลและการป้องกันข้อมูลอย่างไร เช่น การจัดกลุ่มของผู้ใช้ การจัดกลุ่มของข้อมูล เป็นต้น

3.4) **การตรวจสอบการเข้าถึง** (Reference Monitor) แบบรูปนี้เป็นข้อบังคับการเข้าถึง โดยเพิ่มความเข้มงวดเมื่อมีการร้องขอการเข้าถึงและเข้าใช้ทรัพยากรของระบบ

3.5) **การนิยามบทบาทและสิทธิ** (Role Rights Definition) แบบรูปนี้เป็นการนำเสนอแนวทางที่แน่นอนในการกำหนดสิทธิให้กับบทบาทใดๆ สำหรับระบบที่ต้องการความมั่นคง

1.3.2 แนวทางการดำเนินการของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ มีความสอดคล้องเป็นไปตามมาตรฐาน ISO/IEC 27001:2005 และ 27002:2005

1.3.3 จัดทำเอกสารแผ่นแบบเพื่อเป็นแนวทางในการดำเนินการตามกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1.3.4 พัฒนาเครื่องมือเพื่อใช้ในการสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งประกอบด้วยฟังก์ชันการทำงานหลัก ดังต่อไปนี้

1) สนับสนุนการกำหนดข้อมูลตั้งต้นสำหรับการจัดตั้งกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

2) สนับสนุนการกำหนดสินทรัพย์ประเภทสารสนเทศที่ต้องการการควบคุมการเข้าถึงรายละเอียดความเสี่ยงที่มีความเกี่ยวข้อง รวมถึงแนวคิดและบริการความมั่นคงองค์กร

3) สนับสนุนการกำหนดวิธีการของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

4) สนับสนุนการกำหนดวิธีการของการออกแบบและใช้งานรหัสผ่าน

5) สนับสนุนการตรวจสอบความถูกต้องของข้อกำหนดต่างๆ ทั้งข้อกำหนดความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ ข้อกำหนดวิธีการของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ และข้อกำหนดวิธีการของการออกแบบและใช้งานรหัสผ่าน

6) สนับสนุนการวางแผนภายใต้การดำเนินการกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

7) สนับสนุนขั้นตอนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

8) สนับสนุนขั้นตอนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

9) สนันสนุนขั้นตอนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1.3.5 ทดสอบเครื่องมือโดยพิจารณาว่า เป็นไปตามฟังก์ชันงานที่ได้กำหนดไว้และสามารถสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้อย่างครบถ้วนและถูกต้องหรือไม่

1.3.6 ตัวอย่างกรณีทดสอบที่ได้จำลองขึ้น จะใช้ในการทดสอบแบบกล่องดำ (Black Box Testing) เท่านั้น

1.4 ขั้นตอนการวิจัย

1) ศึกษาและวิเคราะห์รายละเอียดของแบบรูปความมั่นคงที่เกี่ยวข้องกับการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ รวมถึงความสัมพันธ์ระหว่างกัน

2) ศึกษาและวิเคราะห์มาตรฐาน ISO/IEC 27001:2005 และ 27002:2005

3) วิเคราะห์และออกแบบกระบวนการการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ รวมถึงทวนสอบการดำเนินการของกระบวนการกับสิ่งที่ได้ศึกษามาแล้วข้างต้น

4) วิเคราะห์และออกแบบเอกสารแผ่นแบบที่เกี่ยวข้องตามกระบวนการที่ได้ออกแบบไว้ในข้อที่ 3)

5) วิเคราะห์และออกแบบหน้าที่การทำงานของเครื่องมือ เพื่อใช้ในการสนับสนุนกระบวนการดังกล่าว

6) พัฒนาส่วนต่อประสานกับผู้ใช้และส่วนประกอบภายใน รวมถึงเอกสารต่างๆ ที่มีความเกี่ยวข้อง

7) ทดสอบและตรวจสอบคุณภาพของเครื่องมือ

8) สรุปผลการวิจัย และจัดทำรายงานวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศโดยใช้แบบรูปความมั่นคงในการออกแบบ ซึ่งจะช่วยให้องค์กรใดๆ สามารถนำไปใช้เป็นแนวทางในการกำหนดเป็นกระบวนการสำหรับความต้องการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศของตน

2) ได้เอกสารแผ่นแบบที่เกี่ยวข้อง ซึ่งจะช่วยสนับสนุนกระบวนการตามข้อที่ 1)

3) ได้เครื่องมือสนับสนุนกระบวนการดังกล่าว เพื่อที่องค์กรสามารถนำไปประยุกต์ใช้ต่อไป

4) ช่วยให้องค์กรสามารถลดความเสี่ยงของการเกิดผลกระทบต่อทั้งการดำเนินการโดยรวมและผลกระทบต่อมูลค่าทางธุรกิจขององค์กร

1.6 บทความวิชาการที่ได้รับการตีพิมพ์

ในการวิจัยนี้ ผู้วิจัยมีผลงานทางวิชาการร่วมกับคณะผู้วิจัย ซึ่งเป็นบทความวิชาการระดับชาติและนานาชาติ รวมเป็น 2 บทความ ดังนี้

1) บทความวิชาการเรื่อง “การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์สารสนเทศโดยใช้แบบรูปความมั่นคง (A Design of Process Model for Information Assets Access Control using Security Patterns)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทางวิทยาศาสตร์และวิศวกรรมคอมพิวเตอร์ระดับชาติ ครั้งที่ 13 (The13th National Computer Science and Engineering Conference: NCSEC 2009)” ระหว่างวันที่ 4 - 6 พฤศจิกายน 2552 ณ โรงแรม มนเฑียร ริเวอร์ไซต์ กรุงเทพฯ ประเทศไทย

2) บทความวิชาการเรื่อง “A Process Model Design and Tool Support for Information Assets Access Control using Security Patterns” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการร่วมสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมซอฟต์แวร์ ครั้งที่ 8 (The 8th International Joint Conference on Computer Science and Software Engineering: JCSSE 2011)” ระหว่างวันที่ 11 - 13 พฤษภาคม 2554 ณ คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล วิทยาเขตศาลายา นครปฐม ประเทศไทย

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 แบบรูปความมั่นคง (Security Patterns)

แบบรูปความมั่นคง [1, 2, 3] เป็นแบบแผนหรือแนวทางในการอธิบายปัญหาด้านความมั่นคงที่เคยปรากฏมาบ่อยครั้ง และนำเสนอผลเฉลยของปัญหานั้นที่ได้รับการพิสูจน์มาเป็นอย่างดี ซึ่งสามารถนำไปประยุกต์ใช้กับการออกแบบโครงสร้างของการแก้ปัญหาความมั่นคงได้อย่างเป็นรูปธรรม เนื่องจากแบบรูปความมั่นคงดังกล่าวได้รวบรวมองค์ความรู้ด้านความมั่นคงไว้อย่างมีโครงสร้างจากผู้ชำนาญการด้านความมั่นคง วิศวกรรมความมั่นคง และวิศวกรรมซอฟต์แวร์ แบบรูปความมั่นคงนั้นสามารถแบ่งแยกได้เป็น 3 ประเภท ดังนี้

1) **แบบรูปการวิเคราะห์ความมั่นคง** (Security Analysis Patterns) คือ แบบรูปที่แก้ปัญหาด้านการวิเคราะห์ความมั่นคงของระบบ

2) **แบบรูปการออกแบบความมั่นคง** (Security Design Patterns) คือ แบบรูปที่แก้ปัญหาการออกแบบโครงสร้างความมั่นคงของระบบ

3) **แบบรูปกระบวนการความมั่นคง** (Security Process Patterns) คือ แบบรูปที่แก้ปัญหาการออกแบบความมั่นคงให้กับกระบวนการของระบบ

แบบรูปความมั่นคงเมื่อแรกๆ นั้น Yoder J. และ Barcalow J. [6] ได้นำเสนอแง่มุมต่างๆ ด้านความมั่นคงไว้หลากหลายแบบรูป หลังจากนั้นมีผู้ให้ความความสนใจและบางส่วนก็ได้นำเสนอแบบรูปความมั่นคงมาอย่างต่อเนื่อง อาทิเช่น Kienzle D. M. และ Elder M. C. [7] นำเสนอแบบรูปความมั่นคงเกี่ยวกับการพัฒนาโปรแกรมประยุกต์บนเว็บไซต์จำนวน 2 กลุ่ม 29 แบบรูป Blakley B. และ Heath C. [1] นำเสนอแบบรูปความมั่นคงจำนวน 2 กลุ่ม 13 แบบรูป และ Schumacher M. และคณะ [3] นำเสนอแบบรูปความมั่นคงจำนวน 8 กลุ่ม 46 แบบรูป ในช่วงระหว่างที่มีการนำเสนอแบบรูปความมั่นคงในหลากหลายมุมมองอยู่นั้น มีการประชุมร่วมกันระหว่าง PLoP และ EuroPLOP ในปี ค.ศ. 2002-2003 เกิดขึ้น ซึ่งเป็นการนำเสนอแผ่นแบบ (Template) เพื่อกำหนดเป็นรายละเอียดที่จำเป็นสำหรับแบบรูปความมั่นคง

แบบรูปความมั่นคงที่จะนำมาใช้ในงานวิจัยนี้ มาจากแบบรูปความมั่นคงของ Schumacher M. และคณะ [3] ที่นำเสนอในหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) เหตุที่นำมาใช้เนื่องจากแบบรูปมีการอธิบายรายละเอียดของความมั่นคงโดย

แบ่งเป็นหัวข้ออย่างชัดเจน รวมถึงการแสดงถึงความสัมพันธ์ระหว่างกันของแบบรูป จึงทำให้สามารถนำไปออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้เป็นอย่างดี นอกจากนี้ยังถือว่าเป็นแบบรูปที่ได้รับความนิยม

แบบรูปความมั่นคงดังกล่าวประกอบไปด้วยองค์ประกอบทั้งหมด14 องค์ประกอบ ซึ่งในแต่ละแบบรูปความมั่นคงไม่จำเป็นต้องมีองค์ประกอบครบทั้งหมด ขึ้นอยู่กับแต่ละความเหมาะสมของการนำไปใช้สำหรับปัญหาด้านความมั่นคงปัญหาใดปัญหาหนึ่ง โดยรายละเอียดขององค์ประกอบทั้งหมดมีดังนี้

1) ชื่อ (Name) เป็นชื่อของแบบรูปความมั่นคง

2) ชื่อที่รู้จัก (Also Known As) เป็นชื่ออื่นของแบบรูปความมั่นคง

3) ตัวอย่าง (Example) เป็นตัวอย่างของปัญหาและความต้องการของแบบรูปความมั่นคง

4) บริบท (Context) เป็นสถานการณ์ที่ควรใช้แบบรูปความมั่นคง

5) ปัญหา (Problem) เป็นปัญหาที่แบบรูปความมั่นคงต้องทำการแก้ไข

6) ผลเฉลย (Solution) เป็นคำตอบหรือผลเฉลยของปัญหาภายใต้แบบรูปความมั่นคง

7) โครงสร้าง (Structure) เป็นรายละเอียดโครงสร้างของแบบรูปความมั่นคง

8) ไดนามิก (Dynamics) เป็นเหตุการณ์ที่อธิบายถึงการทำงานของแบบรูปความมั่นคง

9) การทำให้เกิดผล (Implementation) เป็นการแนะนำการปฏิบัติในการทำให้เกิดผล

10) ตัวอย่างการแก้ไข (Example Resolved) เป็นตัวอย่างของการแก้ไขปัญหาด้วยแบบรูปความมั่นคง

11) รูปแปร (Variants) เป็นคำอธิบายที่มีลักษณะแตกต่างหรือพิเศษออกไป

12) การใช้งาน (Know Uses) เป็นตัวอย่างการใช้แบบรูปความมั่นคงในระบบเป็นจริง

13) ผลที่ได้ (Consequence) เป็นประโยชน์ที่ได้จากแบบรูปความมั่นคง

14) แหล่งข้อมูลอื่น (See Also) เป็นการอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาในลักษณะเดียวกัน

2.1.2 **มาตรฐาน** ISO/IEC 27001:2005 (Information Security Management System: ISMS)

มาตรฐาน ISO/IEC 27001:2005 [4] เป็นข้อกำหนดสำหรับใช้เป็นเกณฑ์ในการตรวจรับรองความมีมาตรฐานของ “ระบบการจัดการความมั่นคงสารสนเทศหรือระบบ ISMS” ซึ่งกำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International Organization for Standardization) และ IEC (The International

Electrotechnical Commission) โดยมาตรฐานดังกล่าวมีรายละเอียดนับตั้งแต่การจัดตั้ง การปฏิบัติใช้งาน การทวนสอบ และการปรับปรุงอย่างต่อเนื่อง ทั้งนี้ในการนำเอามาตรฐานไปใช้งานจริง จะต้องมีการอ้างอิงมาตรการความมั่นคง (Control Objective) และการควบคุม (Controls) ทั้ง 133 หัวข้อภายใต้มาตรฐาน ISO/IEC 27002:2005 ตามความเหมาะสมกับสภาพการดำเนินการขององค์กร

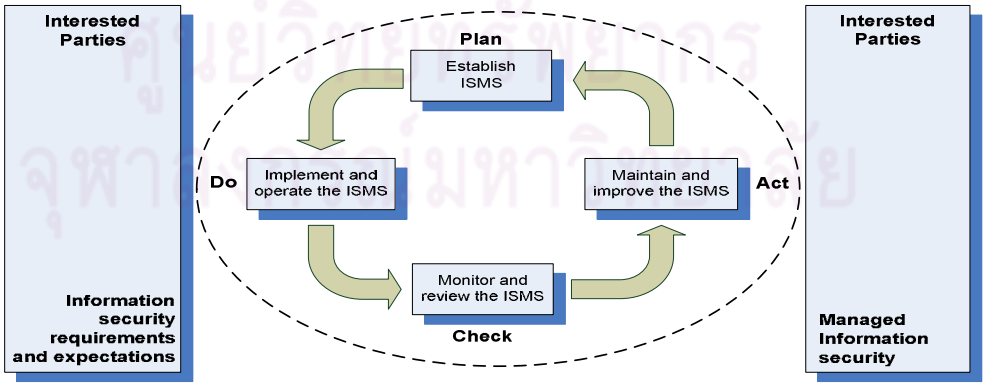
แนวคิดของมาตรฐานนี้จะเป็นแนวทางสำคัญสำหรับองค์กรที่ต้องการนำไปใช้เพื่อปกป้องข้อมูล กระบวนการธุรกิจ และสินทรัพย์ประเภทสารสนเทศ โดยมีความครอบคลุมหลักการด้านความมั่นคงทั้ง 3 ด้าน ดังต่อไปนี้

1) **การถือความลับ** (Confidentiality) เพื่อให้แน่ใจว่าสารสนเทศต่างๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิการเข้าถึงเท่านั้น

2) **การบูรณาภาพ** (Integrity) เพื่อป้องกันให้สารสนเทศมีความสมบูรณ์และถูกต้อง

3) **สภาพพร้อมใช้งาน** (Availability) เพื่อให้แน่ใจว่าผู้ที่มีสิทธิการเข้าถึงสารสนเทศสามารถเข้าถึงได้เมื่อมีต้องการ

มาตรฐานนี้ได้ถูกจัดทำขึ้นโดยยึดตามแนวคิดของโมเดล PDCA (Plan-Do-Check-Act Model) ซึ่งเป็นโมเดลเดียวกับระบบการบริหารที่เป็นสากลที่ใช้กันทั่วโลก ทั้งนี้นำมาใช้เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาขึ้นอย่างต่อเนื่อง (Continuous improvement) เริ่มต้นตั้งแต่การจัดตั้ง (Establish) การนำระบบไปใช้ (Implement) การดำเนินงาน (Operate) การติดตามและวัดผล (Monitor) การทวนสอบ (Review) การบำรุงรักษาระบบ (Maintain) และการปรับปรุงพัฒนาระบบให้ดียิ่งขึ้น (Improve) ซึ่งสามารถแสดงดังรูปที่ 2.1



รูปที่ 2.1 โมเดล PDCA ที่นำมาประยุกต์ใช้ในมาตรฐาน ISO/IEC 27001:2005 [4]

จากรูปที่ 2.1 รายละเอียดแต่ละขั้นตอนของโมเดล PDCA [7] สามารถอธิบายได้ดังต่อไปนี้

1) **การจัดตั้งระบบบริหารจัดการความมั่นคง** (Plan) โดยองค์กรควรกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงและนโยบายความมั่นคง โดยพิจารณาถึงลักษณะของธุรกิจ โครงสร้างองค์กร สถานที่ตั้ง สินทรัพย์ประเภทสารสนเทศ และเทคโนโลยี นอกจากนี้ยังต้องกำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร ระบบความเสี่ยง วิเคราะห์และประเมินความเสี่ยง ระบุและประเมินทางเลือกของมาตรการในการจัดการกับความเสี่ยงนั้น

2) **การดำเนินการระบบบริหารจัดการความมั่นคง** (Do) จัดทำแผนการจัดการความเสี่ยง ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงและตามมาตรการที่ได้เลือกไว้ กำหนดวิธีการในการวัดความสัมฤทธิ์ผล จัดทำและลงมือปฏิบัติตามแผนการอบรม บริหารจัดการการดำเนินการและทรัพยากรสำหรับระบบบริหารจัดการความมั่นคง

3) **การเฝ้าสังเกตและทวนสอบระบบบริหารจัดการความมั่นคง** (Check) ดำเนินการทบสอบและวัดความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงอย่างสม่ำเสมอ ทวนสอบผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่ยอมรับได้ ปรับปรุงแผนทางด้านความปลอดภัยโดยนำผลของการเฝ้าสังเกตและทวนสอบมาพิจารณาร่วมด้วย และบันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคง

4) **การบำรุงรักษาและปรับปรุงระบบบริหารจัดการด้านความมั่นคง** (Act) โดยองค์กรควรปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้ รวมถึงการใช้มาตรการเชิงแก้ไข การป้องกัน และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงขององค์กรเองและจากองค์กรอื่น แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้อง และตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

จากการอธิบายขั้นตอนของโมเดล PDCA จะเห็นได้ว่ามาตรฐานนี้มีการวางโครงสร้างเพื่อให้สามารถใช้งานร่วมกับระบบบริหารอื่นๆ ได้ แม้ว่าข้อกำหนดต่างๆ นั้นมีความแตกต่างกัน นอกจากนี้ยังสามารถนำมาใช้ประยุกต์ได้กับทุกๆ ประเภทขององค์กรที่เกี่ยวข้องกับความมั่นคงได้อย่างบูรณาการทั้งองค์กรที่มีขนาดใหญ่และขนาดย่อม

และสำหรับในงานวิจัยนี้ได้นำแนวคิดของมาตรฐานไปใช้เพื่อเป็นแนวทางในการออกแบบกระบวนการของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งจะทำให้กระบวนการมีความสมบูรณ์และถูกต้องมากยิ่งขึ้น เนื่องจากเป็นมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการสารสนเทศภายใต้หลักการด้านความมั่นคงโดยตรง

2.1.3 มาตรฐาน ISO/IEC 27002:2005 (Code of Practice for Information Security Management)

มาตรฐาน ISO/IEC 27002:2005 [5] แต่เดิมคือมาตรฐาน ISO/IEC 17799:2005 เป็นมาตรฐานที่กล่าวถึงวิธีปฏิบัติที่จะนำไปสู่ระบบการจัดการความมั่นคงของสารสนเทศที่มีความปลอดภัย ซึ่งวิธีปฏิบัติจะต้องสอดคล้องเป็นไปตามข้อกำหนดภายใต้มาตรฐาน ISO/IEC 27001:2005 โดยรายละเอียดของมาตรฐานนี้จะบ่งบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบ โดยได้แบ่งเป็นหัวข้อหลักที่มีเกี่ยวข้องกับระบบและได้ให้แนวทางว่าควรมีการปฏิบัติอย่างไร เมื่อมีการนำมาใช้จริงสามารถที่จะเพิ่มเติมวิธีปฏิบัติที่มีความเหมาะสมภายใต้สภาวะแวดล้อมขององค์กรเข้าไปในระบบได้ ซึ่งวิธีปฏิบัติดังกล่าวมีทั้งหมด 133 หัวข้อ แบ่งออกเป็น 11 หมวดหลัก ได้แก่ 1) นโยบายด้านความมั่นคง (Security Policy) 2) โครงสร้างด้านความมั่นคงสารสนเทศ (Organization of Information Security) 3) การจัดการทรัพย์สิน (Asset Management) 4) ความมั่นคงด้านบุคลากร (Human Resources Security) 5) ความมั่นคงด้านทางกายภาพและสภาวะแวดล้อม (Physical and Environmental Security) 6) การจัดการการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and Operations Management) 7) การควบคุมการเข้าถึง (Access Control) 8) การจัดการการได้มาซึ่งการพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance) 9) การจัดการเหตุการณ์ละเมิดความมั่นคงสารสนเทศ (Information security incident management) 10) การจัดการความต่อเนื่องในการดำเนินงาน (Business Continuity Management) และ 11) การปฏิบัติตามข้อกำหนดทางกฎหมายและบทลงโทษ (Compliance)

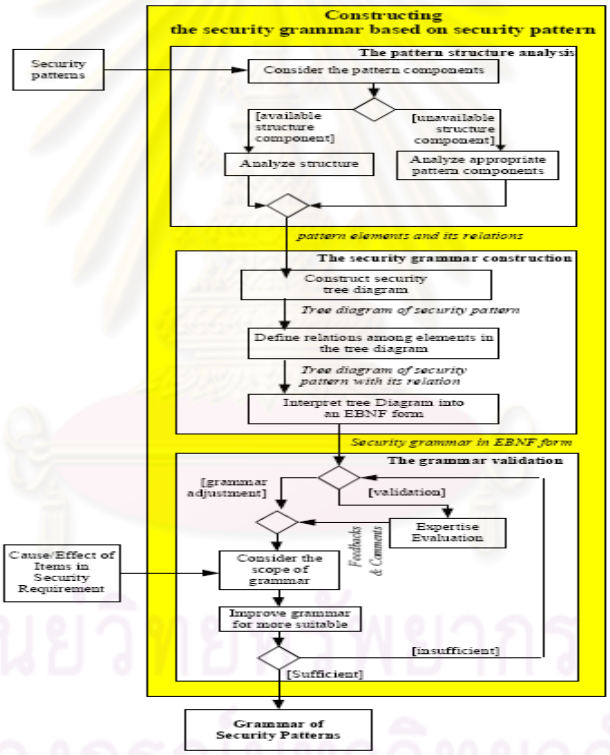
และสำหรับในงานวิจัยนี้ได้นำวิธีปฏิบัติที่สำคัญ โดยเฉพาะในส่วนของการควบคุมการเข้าถึงไปใช้ ซึ่งพิจารณาควบคู่กับมาตรฐาน ISO/IEC 27001:2005 ทั้งนี้จะทำให้การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศมีการดำเนินการที่ถูกต้องสอดคล้องเป็นไปตามหลักการด้านความมั่นคงของมาตรฐานทั้งสอง

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง (Defining Security Requirements Using Grammar of Security Patterns)

งานวิจัยนี้มีวัตถุประสงค์เพื่อสร้างไวยากรณ์สำหรับกำหนดความต้องการความมั่นคงจากแบบรูปความมั่นคง [8] โดยแสดงออกมาในรูปของไวยากรณ์อีบีเอ็นเอฟ (Extended Backus-Naur Form: EBNF) และเพื่อสร้างเครื่องมือสนับสนุนที่นำไวยากรณ์ดังกล่าวมาประยุกต์ใช้ในการ

กำหนดความต้องการความมั่นคงของระบบ โดยแบบรูปความมั่นคงที่นำมาใช้นั้นมาจากแบบรูปความมั่นคงของ Schumacher M. และคณะ ประยุกต์ใช้จำนวนทั้งสิ้น 20 แบบรูป จาก 4 กลุ่ม ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management) การระบุตัวตนและการพิสูนจ์ตัวจริง (Identification and Authentication: I&A) แบบจำลองควบคุมการเข้าถึง (Access Control Model) และสถาปัตยกรรมไฟล์วอลล์ (Firewall Architecture) แบบรูปทั้งหมดได้ถูกนำมาสร้างเป็นแผนภาพต้นไม้ความมั่นคง (Security Tree Diagram) เพื่อแสดงความสัมพันธ์กันระหว่างองค์ประกอบของแบบรูปความมั่นคง จากนั้นแปลงไปเป็นไวยากรณ์ความมั่นคง (Security Grammar) ในรูปไวยากรณ์อีบีเอ็นเอฟ ซึ่งกรอบงานการสร้างไวยากรณ์ความมั่นคงโดยใช้แบบรูปความมั่นคงเป็นพื้นฐานนั้นแสดงได้ดังรูปที่ 2.2



รูปที่ 2.2 กรอบงานการสร้างไวยากรณ์ความมั่นคงโดยใช้แบบรูปความมั่นคงเป็นพื้นฐาน [8]

สิ่งที่นำมาพิจารณาใช้ในงานวิจัยนี้ คือ การวิเคราะห์รายละเอียดโครงสร้างของแบบรูปความมั่นคง และแบบรูปความมั่นคงที่สัมพันธ์กัน รวมถึงไวยากรณ์ความมั่นคงที่ใช้ในการกำหนดความต้องการความมั่นคง ช่วยในการพิจารณาถึงข้อมูลนำเข้าที่สำคัญ เงื่อนไขและลำดับการทำงานที่เป็นไปได้ ซึ่งจะทำให้กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ออกแบบมีความชัดเจนมากยิ่งขึ้น

2.2.2 การศึกษาสถาปัตยกรรมของแบบรูปความมั่นคง (A Study of Security Architectural Patterns)

งานวิจัยนี้นำเสนอการศึกษากลุ่มแบบรูปความมั่นคง [9] เพื่อเป็นแนวทางในการออกแบบและพัฒนาระบบให้เป็นไปตามความต้องการความมั่งคง ทั้งนี้ได้เสนอเป็นการสรุปใจความสำคัญและการเปรียบเทียบของแต่ละแบบรูป โดยมีแบบรูปความมั่นคงทั้งหมด 9 แบบรูป ได้แก่ แบบรูปการให้อำนาจ (Authorization Pattern) แบบรูปการเข้าถึงเชิงบทบาท (RBAC Pattern) แบบรูปความมั่นคงหลายระดับ (Multilevel Security Pattern) แบบรูปการเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor Pattern) แบบรูปการเข้าถึงหน่วยความจำแบบเสมือน (Virtual Address Space Access Control Pattern) แบบรูปการกำหนดขอบเขตสำหรับการประมวลผลกระบวนการ (Execution Domain Pattern) แบบรูปการจัดเตรียมสภาวะแวดล้อมสำหรับสิทธิการเข้าถึง (Session Pattern) แบบรูปการเข้าถึงเชิงทางเดี่ยว (Single Access Point Pattern) และแบบรูปการตรวจสอบเชิงทางเดี่ยว (Check Point Pattern) สำหรับการศึกษาในแต่ละแบบรูปความมั่นคงสามารถสรุปรายละเอียดตามหัวข้อย่อย 8 หัวข้อ ได้แก่ จุดมุ่งหมาย (Intent) บริบท (Context) ปัญหา (Problem) คำอธิบาย (Description) ผลเฉลย (Solution) ผลลัพธ์ (Consequences) ความรู้เพิ่มเติม (Known Uses) และแบบรูปที่เกี่ยวข้อง (Related Pattern) ส่วนการเปรียบเทียบของแบบรูปความมั่นคง งานวิจัยนี้ได้นำเสนอเป็นกรอบงานของการเปรียบเทียบทั้งในด้านของหลักเกณฑ์ความมั่นคง ด้านประสิทธิภาพ และหลักเกณฑ์การประเมิน โดยการเปรียบเทียบของแต่ละแบบรูปในด้านหลักเกณฑ์ความมั่นคงสามารถแสดงได้ดังรูปที่ 2.3

	Authentication	Authorization	Integrity	Confidentiality	Attackers detection	No-Repudiation	Auditability	Maintainability	Availability	Reliability	Error management
Authoriz.			0		0	1			0	0		
RBAC			0		0	1			0	0		
Multilevel			0	5	6	1				0	0	
Reference Monitor			0	7	7	1				0	7	
Virtual Address			0	7	7	1				0		
Execution Domain			0	7	7	1				0	4	
SAP	0	0	2	0	0	0	0			0	0	0
Check Point	0	0	2	2	0	0				0	0	0
Session			0	0	0	1			3	0	4	

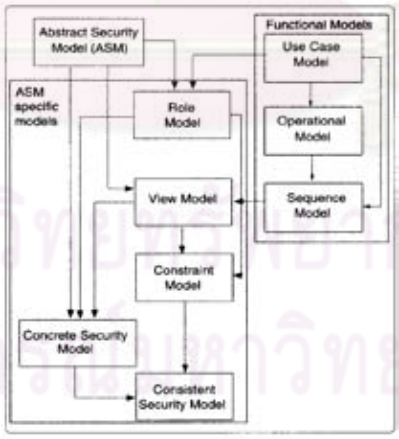
0. Always fulfilled. 1. Only detection. 2. Efficient check algorithm. 3. First step development. 4. Subset of the authorizations activated. 5. Biba model. 6. Bell LaPadula model. 7. To process level.

รูปที่ 2.3 การเปรียบเทียบด้านหลักเกณฑ์ความมั่นคงของแต่ละแบบรูปความมั่นคง [9]

สิ่งที่นำมาพิจารณาใช้ในงานวิจัยนี้ คือ การศึกษาในรายละเอียดทั้ง 8 หัวข้อย่อยของแต่ละแบบรูปความมั่นคง โดยเฉพาะแบบรูปที่เกี่ยวข้องกับการควบคุมการเข้าถึงที่ได้นำมาประยุกต์ใช้ในงานวิจัยนี้ ทั้งแบบรูปการให้อำนาจ แบบรูปการเข้าถึงเชิงบทบาท แบบรูปความมั่นคงหลายระดับ และแบบรูปการเฝ้าสังเกตเชิงอ้างอิง ซึ่งทำให้เกิดความเข้าใจในบริบทของแต่ละแบบรูปมากยิ่งขึ้น

2.2.3 การวิเคราะห์การควบคุมการเข้าถึงในกระบวนการพัฒนาซอฟต์แวร์ (Formal Access Control Analysis in the Software Development Process)

งานวิจัยนี้นำเสนอโมเดลขับเคลื่อนสำหรับการจัดเตรียมโมเดลความมั่นคงเข้าสู่กระบวนการออกแบบและพัฒนาซอฟต์แวร์เชิงวัตถุ [10] โดยเฉพาะในเฟสของการออกแบบ กล่าวคือเป็นการวิเคราะห์ว่า จะทำการออกแบบและพัฒนาความต้องการความมั่นคงที่กำหนดไว้ได้อย่างไรโดยพิจารณาจากแนวคิดของโมเดลความมั่นคงที่เกี่ยวข้องกับความต้องการความมั่นคงดังกล่าว ทั้งนี้ได้สนใจในส่วนของการวิเคราะห์ทางด้านการควบคุมการเข้าถึงเป็นสำคัญ ซึ่งโมเดลความมั่นคงภายใต้การควบคุมการเข้าถึงนั้นจะถูกระบุโดยโมเดลที่เรียกว่า โมเดลความมั่นคงแบบนามธรรม (Abstract Security Model) โดยภาพรวมของการดำเนินการซึ่งใช้โมเดลความมั่นคงดังกล่าวสามารถแสดงได้ดังรูปที่ 2.4

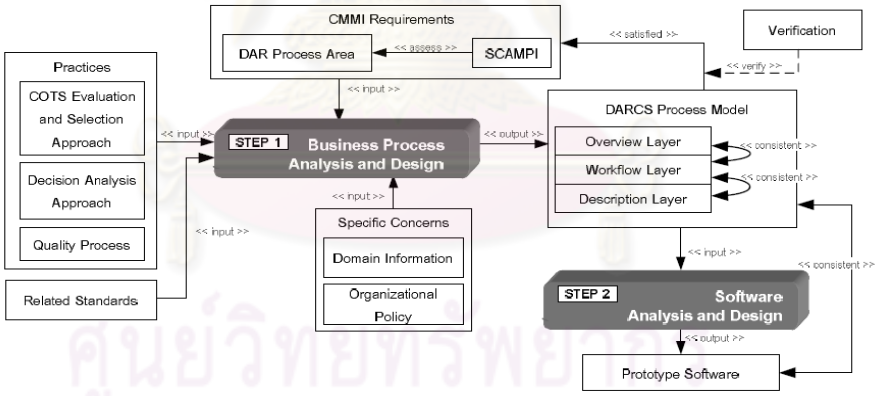


รูปที่ 2.4 ภาพรวมของการดำเนินการโดยใช้โมเดลความมั่นคง [10]

สิ่งที่นำมาพิจารณาใช้ในงานวิจัยนี้ คือ แนวคิดของการนำโมเดลความมั่นคงภายใต้การควบคุมการเข้าถึงมาใช้ในการออกแบบและพัฒนาซอฟต์แวร์ ซึ่งจะทำให้เข้าใจถึงวิธีการของการควบคุมการเข้าถึงมากยิ่งขึ้น เนื่องจากการมองเห็นภาพรวมของวัตถุที่เกิดขึ้น รวมถึงการปฏิสัมพันธ์ระหว่างกันภายใต้ข้อกำหนดของวิธีการดังกล่าว

2.2.4 การออกแบบและพัฒนากระบวนการการคัดเลือกผลิตภัณฑ์ซอฟต์แวร์เชิงพาณิชย์ที่ใช้แบบจำลองวุฒิภาวะความสามารถแบบบูรณาการเป็นฐาน (CMMI-Based Process Model Design and Development for COTS Software Product Selection Process)

งานวิจัยนี้นำเสนอกระบวนการสำหรับกลุ่มกระบวนการการวิเคราะห์การตัดสินใจและการแก้ปัญหา (Decision Analysis and Resolution) ในประเด็นของการคัดเลือกซอฟต์แวร์เชิงพาณิชย์ภายใต้แบบจำลองวุฒิภาวะความสามารถแบบบูรณาการหรือซีเอ็มเอ็มไอ [11] ซึ่งกระบวนการดังกล่าวประกอบด้วย 3 ชั้นแบบจำลอง คือ ชั้นแบบจำลองเชิงภาพรวม ชั้นแบบจำลองเชิงกระแสงาน และชั้นแบบจำลองเชิงนิยาม พร้อมกันนี้ยังได้นำเสนอเครื่องมือสนับสนุนกระบวนการอีกด้วย โดยทั้งกระบวนการและเครื่องมือสนับสนุนที่พัฒนาขึ้นมานั้น มีวัตถุประสงค์เพื่อสนับสนุนให้องค์กรมีความสามารถที่จะนำไปประยุกต์ใช้ในการดำเนินงานตามส่วนประกอบสำคัญต่างๆ ของกระบวนการได้อย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ โดยการออกแบบและพัฒนากระบวนการตัดสินใจคัดเลือกซอฟต์แวร์เชิงพาณิชย์สามารถแสดงได้ดังรูปที่ 2.5

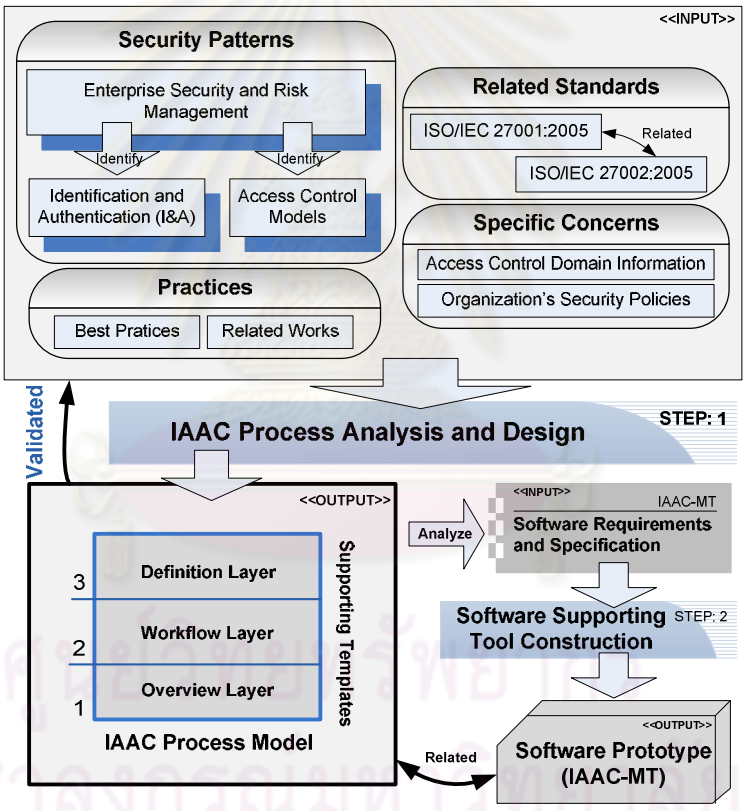


รูปที่ 2.5 การออกแบบและพัฒนากระบวนการตัดสินใจคัดเลือกซอฟต์แวร์เชิงพาณิชย์ [11]

สิ่งที่นำมาพิจารณาใช้ในงานวิจัยนี้ คือ แนวคิดในการออกแบบและพัฒนากระบวนการทั้งนี้เพื่อช่วยเป็นแนวทางหรือแบบอย่างในการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ทำให้ทราบว่าควรปฏิบัติอย่างไรตั้งแต่เริ่มต้นจนถึงสิ้นสุด ซึ่งจะทำให้กระบวนการที่ได้สามารถอธิบายรายละเอียดที่สำคัญได้อย่างชัดเจน เกิดความเข้าใจในกระบวนการได้โดยง่าย

บทที่ 3
การวิเคราะห์และออกแบบกระบวนการ

งานวิจัยนี้ผู้วิจัยได้นำเสนอการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยเกิดจากการพิจารณาและวิเคราะห์แบบรูปความมั่นคง มาตรฐาน ISO/IEC 27001:2005 และ 27002:2005 และส่วนนำเข้าที่เกี่ยวข้องเป็นสำคัญ ทั้งนี้กระบวนการที่ได้จะถูกนำไปวิเคราะห์และออกแบบ เพื่อพัฒนาเครื่องมือสนับสนุนกระบวนการดังกล่าวต่อไป โดยแนวคิดการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศสามารถแสดงได้ดังรูปที่ 3.1



รูปที่ 3.1 แนวคิดการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จากรูปที่ 3.1 สามารถแบ่งแนวคิดการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศออกเป็น 2 ขั้นตอนหลัก คือ *การวิเคราะห์และออกแบบกระบวนการ (Information Assets Access Control (IAAC) Process Analysis and Design)* และ*การพัฒนาเครื่องมือสนับสนุน (Software Supporting Tool Construction)* สำหรับขั้นตอนแรกการวิเคราะห์และออกแบบกระบวนการ มีส่วนนำเข้าที่เกี่ยวข้องแบ่งออกเป็น 4 ประเภท ได้แก่

1) ***แบบรูปความมั่นคง*** *(Security Patterns)* มีทั้งหมด 3 กลุ่มแบบรูป คือ กลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง กลุ่มการระบุตัวตนและพิสูจน์ตัวตน และกลุ่มแบบจำลองควบคุมการเข้าถึง

2) ***มาตรฐานที่เกี่ยวข้อง*** *(Related Standards)* มีอยู่ด้วยกัน 2 มาตรฐาน คือ มาตรฐาน ISO/IEC 27001:2005 และมาตรฐาน ISO/IEC 27002:2005

3) ***วิธีปฏิบัติ*** *(Best Practices)* เป็นวิธีปฏิบัติที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ที่ได้รับการยอมรับในระดับสากล รวมถึงการประยุกต์ใช้แบบรูปความมั่นคงและหลักการออกแบบกระบวนการต่างๆ ภายใต้งานวิจัยที่ได้รับการตีพิมพ์

4) ***สิ่งสำคัญที่เกี่ยวข้องเฉพาะด้าน*** *(Specific Concerns)* เป็นส่วนของข้อมูลที่มีความแตกต่างกันในแต่ละองค์กร โดยเกี่ยวข้องกับความต้องการสร้างความมั่นคงให้กับสินทรัพย์ของตน ทั้งนโยบายองค์กร โดยเฉพาะในด้านความมั่นคง รวมถึงข้อมูลต่างๆ ที่เกี่ยวข้องกับการเข้าถึงสินทรัพย์ดังกล่าว

ส่วนนำเข้าทั้ง 4 ประเภท จะถูกนำมาศึกษาและวิเคราะห์โดยละเอียดเพื่อให้ได้มาซึ่งองค์ประกอบจำเป็นและการดำเนินการที่สำคัญ จากนั้นนำสิ่งที่ได้มาทำการออกแบบกระบวนการได้เป็นกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Information Assets Access Control Process Model: IAAC Process Model) ซึ่งประกอบด้วยกระบวนการและเอกสารแผ่นแบบ (Template Documents) โดยกระบวนการนั้นสามารถนำเสนอรายละเอียดออกเป็นแบบจำลองต่างๆ ซึ่งมีความสัมพันธ์กันตั้งแต่ชั้นบนสุดไปจนถึงชั้นล่างสุด เรียงลำดับดังนี้

1) **แบบจำลองกระบวนการเชิงภาพรวม** (Overview Process Model Layer) อธิบายถึงองค์ประกอบพื้นฐานของการดำเนินการกระบวนการ ซึ่งจะทำให้องค์กรที่นำไปประยุกต์ใช้มองเห็นภาพรวมและเข้าใจถึงสภาวะแวดล้อมของกระบวนการได้อย่างชัดเจนมากยิ่งขึ้น

2) **แบบจำลองกระบวนการเชิงกระแสงาน** (Workflow Process Model Layer) อธิบายถึงลำดับขั้นตอนของกิจกรรมภายใต้การดำเนินการกระบวนการ นอกจากนี้ยังอธิบายถึงส่วนนำเข้าและออกเพื่อใช้ขับเคลื่อนการดำเนินกิจกรรมนั้นๆ

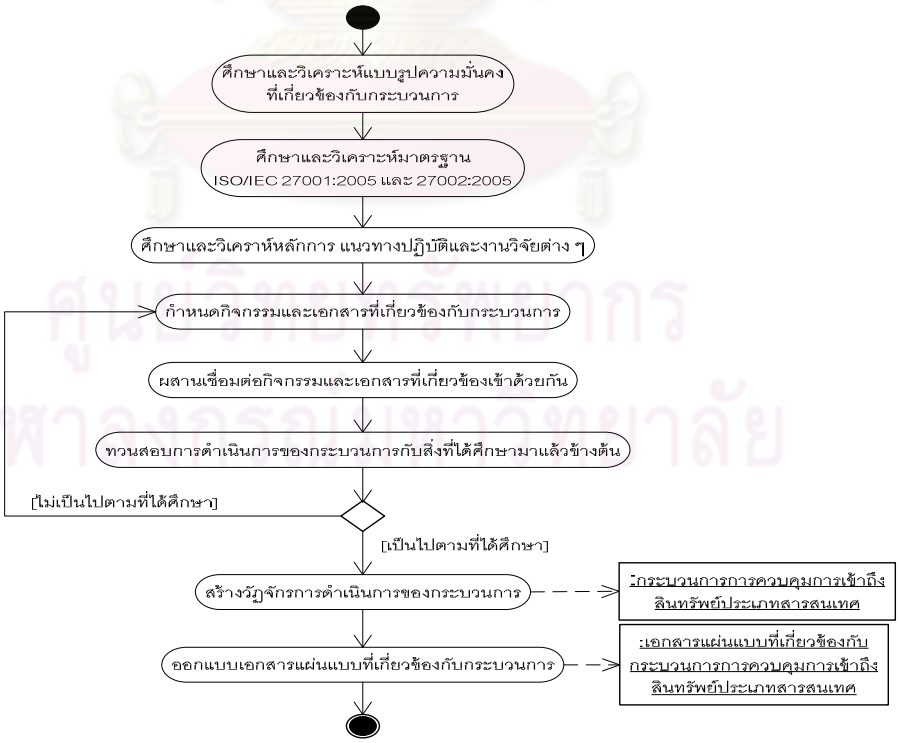
และ 3) **แบบจำลองกระบวนการเชิงนิยาม** (Definition Process Model Layer) เป็นการนิยามพื้นฐานที่จะช่วยให้องค์กรเกิดความเข้าใจในกระบวนการได้อย่างเป็นรูปธรรม ซึ่งเป็นประโยชน์อย่างมากต่อการนำไปประยุกต์ใช้

โดยรายละเอียดของแบบจำลองทั้ง 3 ประเภทนั้นจะอธิบายในบทที่ 4 ต่อไป

กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ได้มานั้นจะถูกนำมายังขั้นตอนที่สอง คือ การพัฒนาเครื่องมือสนับสนุนกระบวนการ และก่อนที่กระบวนการจะถูกนำมาวิเคราะห์และออกแบบเพื่อพัฒนาเป็นเครื่องมือสนับสนุน จะต้องทำการทวนสอบกระบวนการกับส่วนนำเข้าทั้ง 4 ประเภท โดยเฉพาะแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้อง ทั้งนี้เพื่อให้ได้กระบวนการที่มีการดำเนินการเป็นไปตามหลักการด้านความมั่นคงที่สมบูรณ์และถูกต้องอย่างที่สุด สำหรับผลลัพธ์ที่ได้จากการพัฒนาเครื่องมือนั้นจะได้เป็นข้อกำหนดความต้องการของเครื่องมือ (Software Requirements and Specification) และซอฟต์แวร์ต้นแบบ (Software Prototype) เพื่อนำมาใช้สนับสนุนกระบวนการดังกล่าวต่อไป

3.1 การวิเคราะห์และออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

การวิเคราะห์และออกแบบกระบวนการเริ่มจากการศึกษาข้อมูลพื้นฐานสำคัญต่างๆ ที่มีความเกี่ยวข้อง ทั้งนี้เพื่อต้องการให้ได้มาซึ่งการดำเนินการ รวมถึงองค์ประกอบที่สัมพันธ์กัน โดยขั้นตอนของการวิเคราะห์และออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศจะแบ่งเป็น 8 ขั้นตอนหลัก ซึ่งสามารถแสดงได้ดังรูปที่ 3.2



รูปที่ 3.2 ขั้นตอนการวิเคราห์และออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

3.1.1 ศึกษาและวิเคราะห์แบบรูปความมั่นคงที่เกี่ยวข้องกับกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ในขั้นตอนนี้มีวัตถุประสงค์เพื่อทำการศึกษาและวิเคราะห์รายละเอียดของแบบรูปความมั่นคงที่เกี่ยวข้องกับกระบวนการ รวมถึงความสัมพันธ์ระหว่างกันของแบบรูป โดยมีรายละเอียดที่ต้องศึกษาเป็นไปตามทฤษฎีที่เกี่ยวข้อง 2.1.1 ในส่วนขององค์ประกอบทั้ง 14 องค์ประกอบครอบคลุมทั้งหมด 3 กลุ่ม 14 แบบรูปความมั่นคง ทั้งนี้เพื่อให้เข้าใจถึงจุดมุ่งหมาย สิ่งที่จะต้องดำเนินการ และองค์ประกอบสำคัญที่เกิดขึ้นภายใต้แบบรูปดังกล่าว โดยแบบรูปความมั่นคงที่ต้องศึกษามีดังต่อไปนี้

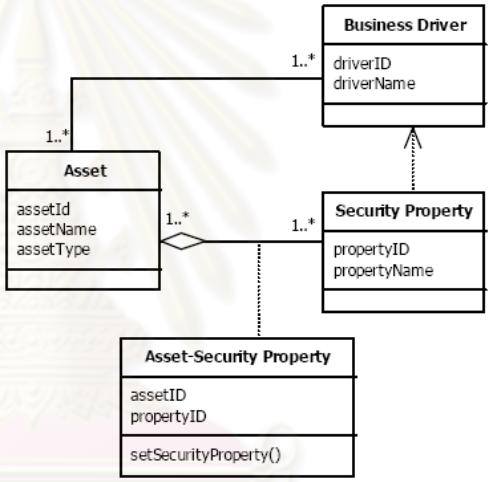
1) **การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง** (Enterprise Security and Risk Management) เป็นกลุ่มแบบรูปความมั่นคงที่เกี่ยวข้องกับการกำหนดและการจัดการซึ่งถือเป็นการกำหนดสำคัญที่จะต้องคำนึงถึง เนื่องจากเป็นการระบุข้อมูลพื้นฐานด้านความมั่นคงให้กับกลุ่มแบบรูปอื่นที่มีความเกี่ยวข้อง โดยแบบรูปในกลุ่มนี้ประกอบด้วย

1.1) **การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร** (Security Needs Identification for Enterprise Assets) เป็นแบบรูปเริ่มต้นสำหรับการพิจารณาความมั่นคงองค์กร ซึ่งจะช่วยให้เข้าใจถึงความต้องการด้านความมั่นคงที่จะเป็นต้องมีในองค์กร เพื่อนำคุณสมบัติด้านความมั่นคง ซึ่งได้แก่ การรักษาความลับ (Confidentiality) ความบูรณภาพ (Integrity) สภาพพร้อมใช้งาน (Availability) และภาระรับผิดชอบ (Accountability) มาประยุกต์ใช้ โดยรายละเอียดของแบบรูปดังตารางที่ 3.1

ตารางที่ 3.1 รายละเอียดแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

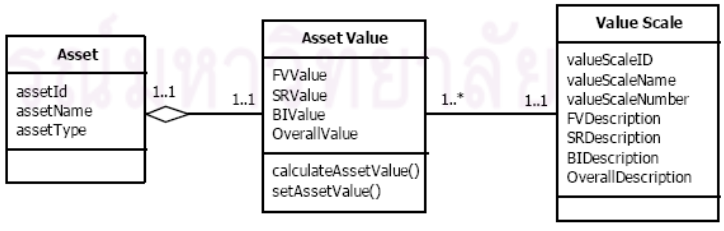
ชื่อแบบรูปความมั่นคง	การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	ไม่มี เนื่องจากเป็นแบบรูปเริ่มต้นของการดำเนินการสร้างความมั่นคงให้กับสินทรัพย์ขององค์กร
เงื่อนไขของการดำเนินการ	ไม่มี เนื่องจากเป็นแบบรูปเริ่มต้นของการดำเนินการสร้างความมั่นคงให้กับสินทรัพย์ขององค์กร
บริบท	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ แต่จะต้องทราบข้อมูลปัจจัยทางธุรกิจ (Business Factor) ของสินทรัพย์นั้นๆ ก่อน
ปัญหา	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ของตน

ตารางที่ 3.1 รายละเอียดแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (ต่อ)

ผลเฉลย	1. ระบุสินทรัพย์ทั้งหมดที่ต้องการสร้างความมั่นคง โดยจัดกลุ่มตามชนิดของสินทรัพย์ 2. ระบุปัจจัยทางธุรกิจขององค์กร 3. ระบุความสัมพันธ์ระหว่างสินทรัพย์และปัจจัยทางธุรกิจ 4. กำหนดคุณสมบัติด้านความมั่นคง ซึ่งโดยปกติแล้วจะประกอบไปด้วย 4 คุณสมบัติ ได้แก่ การรักษาความลับ, ความบูรณภาพ, สภาพพร้อมใช้งาน, และภาระรับผิดชอบ 5. ระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากปัจจัยทางธุรกิจ
โครงสร้าง	

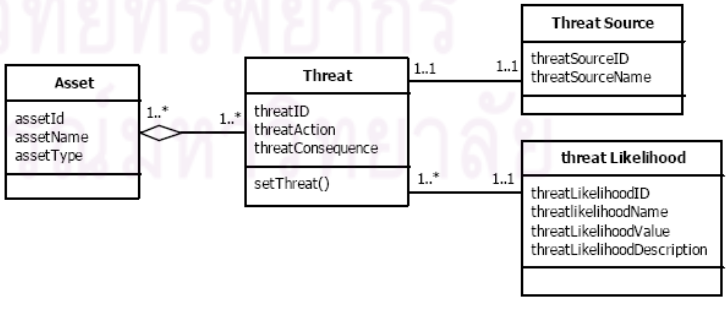
1.2) **การกำหนดมูลค่าสินทรัพย์** (Asset Valuation) การกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่ เพื่อระบุว่าเมื่อเกิดความสูญเสียหรือเกิดความเสียหายของสินทรัพย์จะกระทบต่อองค์กรในด้านใดบ้างและมีผลกระทบในระดับใด โดยมูลค่าสินทรัพย์ (Overall Value) จะได้จากการพิจารณาผลกระทบในด้านต่างๆ ซึ่งได้แก่ ด้านความต้องการความมั่นคง (Security Value) ด้านเศรษฐกิจ (Financial Value) และทางด้านธุรกิจ (Business Value) โดยรายละเอียดของแบบรูปดังตารางที่ 3.2

ตารางที่ 3.2 รายละเอียดแบบรูปการกำหนดมูลค่าสินทรัพย์

ชื่อแบบรูปความมั่นคง	การกำหนดมูลค่าสินทรัพย์
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขของการดำเนินการ	ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
บริบท	องค์กรต้องการทราบมูลค่าโดยรวมของสินทรัพย์ เพื่อใช้ในการประเมินค่าความเสี่ยง
ปัญหา	การกำหนดค่าความสำคัญของสินทรัพย์นั้นทำอย่างไร
ผลเฉลย	1. ระบุมูลค่าด้านความต้องการความมั่นคงของสินทรัพย์ 2. ระบุมูลค่าด้านเศรษฐกิจของสินทรัพย์ 3. ระบุมูลค่าทางด้านธุรกิจของสินทรัพย์ 4. สร้างตารางเพื่อรวมมูลค่าของสินทรัพย์ทั้งหมด โดยที่กำหนดให้ค่าที่มากที่สุดกลายเป็นมูลค่าโดยรวมของสินทรัพย์นั้น
โครงสร้าง	

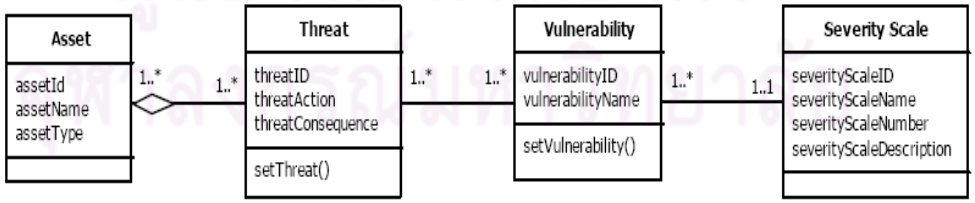
1.3) **การประเมินภัยคุกคาม** (Threat Assessment) ภัยคุกคามเป็นโอกาสของภัยอันตรายต่างๆ ที่อาจจะเกิดขึ้นและส่งผลกระทบต่อสินทรัพย์ขององค์กร แบบรูปนี้จึงมีวัตถุประสงค์เพื่อระบุภัยคุกคามที่จะเกิดขึ้นต่อสินทรัพย์ ความถี่ของภัยคุกคาม (Threat likelihood) และผลกระทบเมื่อสินทรัพย์นั้นถูกคุกคาม (Threat consequence) โดยรายละเอียดของแบบรูปดังตารางที่ 3.3

ตารางที่ 3.3 รายละเอียดแบบรูปการประเมินภัยคุกคาม

ชื่อแบบรูปความมั่นคง	การประเมินภัยคุกคาม
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขของการดำเนินการ	ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
บริบท	เมื่อทำการกำหนดสินทรัพย์ขององค์กรที่ต้องการความมั่นคงแล้ว จะต้องทำการระบุเหตุการณ์ซึ่งเป็นภัยคุกคามของสินทรัพย์นั้น
ปัญหา	จะทำการระบุภัยคุกคามที่เกิดขึ้นกับสินทรัพย์ขององค์กรได้อย่างไร
ผลเฉลย	1. การระบุภัยคุกคาม ซึ่งมีรายละเอียดที่ต้องระบุ ดังนี้ 1) ต้นเหตุที่ทำให้เกิดภัยคุกคาม 2) ภัยคุกคามที่เกิดขึ้น 3) ผลกระทบจากภัยคุกคามนั้น 2. ระบุระดับความถี่ที่เกิดขึ้นของภัยคุกคามนั้น 3. สร้างตารางของภัยคุกคาม โดยแยกตามชนิดของสินทรัพย์
โครงสร้าง	

1.4) **การประเมินจุดอ่อน** (Vulnerability Assessment) จุดอ่อนเป็นจุดที่จะถูกใช้โดยภัยคุกคาม เพื่อเป็นช่องทางในการสร้างภัยอันตรายให้กับสินทรัพย์ การประเมินจุดอ่อนคือการระบุจุดอ่อนของสินทรัพย์ในองค์กร รวมถึงระดับความรุนแรง (Severity scale) เมื่อถูกภัยคุกคามใดๆ โจมตีจุดอ่อนดังกล่าว โดยรายละเอียดของแบบรูปดังตารางที่ 3.4

ตารางที่ 3.4 รายละเอียดแบบรูปการประเมินจุดอ่อน

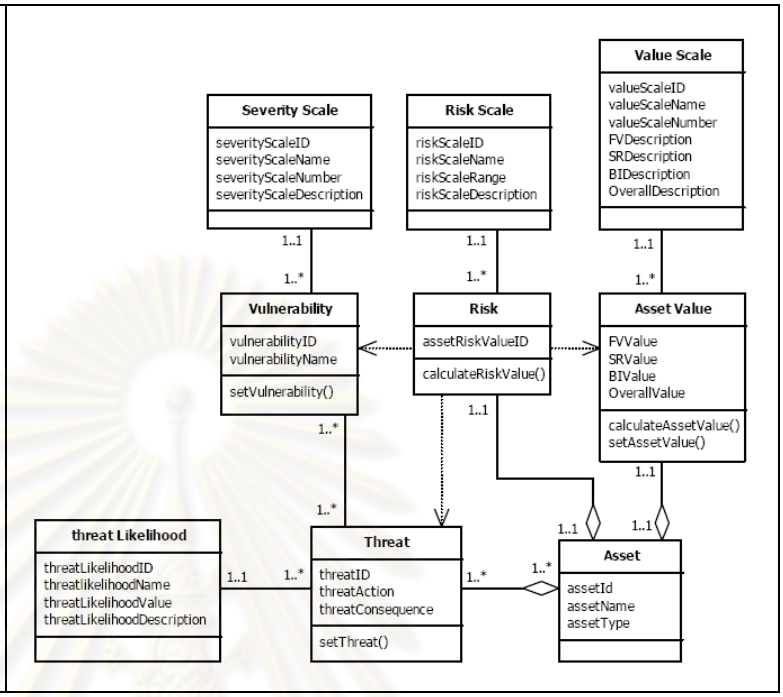
ชื่อแบบรูปความมั่นคง	การประเมินจุดอ่อน
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	1. แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 2. แบบรูปการประเมินภัยคุกคาม : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขของการดำเนินการ	1. ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร 2. ข้อมูลภัยคุกคามของสินทรัพย์จากแบบรูปการประเมินภัยคุกคาม
บริบท	องค์กรต้องการระบุจุดอ่อนของสินทรัพย์ซึ่งที่ภัยคุกคามใช้ในการโจมตี
ปัญหา	ทำอย่างไรองค์กรจึงจะระบุจุดอ่อนของสินทรัพย์ และระดับความรุนแรงเมื่อเกิดภัยคุกคามนั้นโจมตี
ผลเฉลย	1. รวบรวมข้อมูลภัยคุกคามของสินทรัพย์ใดๆ 2. ระบุจุดอ่อนที่อาจจะเกิดขึ้น 3. กำหนดระดับความรุนแรงของจุดอ่อนนั้น 4. สร้างตารางความสัมพันธ์ระหว่างจุดอ่อนและภัยคุกคาม
โครงสร้าง	

1.5) **การกำหนดความเสี่ยง** (Risk Determination) เป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง ใช้ร่วมกับผลการประเมินจุดอ่อน การประเมินภัยคุกคาม และการกำหนดมูลค่าสินทรัพย์ ซึ่งข้อมูลนำเข้าเหล่านี้ จะทำให้สามารถนำมาหาค่าความเสี่ยงที่เหมาะสมและจัดลำดับความสำคัญของสินทรัพย์ได้ โดยรายละเอียดของแบบรูปดังตารางที่ 3.5

ตารางที่ 3.5 รายละเอียดแบบรูปการกำหนดความเสี่ยง

ชื่อแบบรูปความมั่นคง	การกำหนดความเสี่ยง
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	1. แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 2. แบบรูปการกำหนดมูลค่าสินทรัพย์ : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 3. แบบรูปการประเมินภัยคุกคาม : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 4. แบบรูปการประเมินจุดอ่อน : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขของการดำเนินการ	1. ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร 2. ข้อมูลมูลค่าของสินทรัพย์จากแบบรูปการกำหนดมูลค่าสินทรัพย์ 3. ข้อมูลความถี่ของภัยคุกคามทั้งหมดจากแบบรูปการประเมินภัยคุกคาม 4. ข้อมูลระดับความรุนแรงของจุดอ่อนทั้งหมดจากแบบรูปการประเมินจุดอ่อน
บริบท	องค์กรต้องการที่จะกำหนดค่าความเสี่ยงให้กับสินทรัพย์ของตน
ปัญหา	จะทำการกำหนดค่าความเสี่ยงให้กับสินทรัพย์ขององค์กรได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลสำคัญจากการระบุทั้งในรูปแบบการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร แบบรูปการกำหนดมูลค่าสินทรัพย์ แบบรูปการประเมินภัยคุกคาม และแบบรูปการประเมินจุดอ่อน 2. เชื่อมโยงทั้งมูลค่าสินทรัพย์ ความถี่ภัยคุกคาม และระดับความรุนแรงของจุดอ่อนภายใต้สินทรัพย์ใดๆ เข้าด้วยกัน 3. คำนวนค่าความเสี่ยงตามสูตรดังนี้ ค่าความเสี่ยง = [ผลรวม (ความถี่ของภัยคุกคามใดๆ x ระดับความรุนแรงเมื่อภัยคุกคามนั้นโจมตีจุดอ่อนใดๆ)] x มูลค่าสินทรัพย์ 4. แสดงผลลัพท์ค่าความเสี่ยงของสินทรัพย์

ตารางที่ 3.5 รายละเอียดแบบรูปการกำหนดความเสี่ยง (ต่อ)

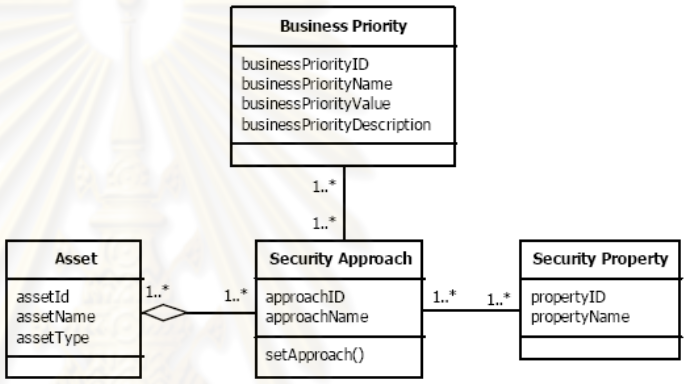
โครงสร้าง	

1.6) แนวคิดความมั่นคงขององค์กร (Enterprise Security Approaches) เป็นการแนะนำให้องค์กรเลือกแนวทางบริหารความเสี่ยง เช่น การป้องกัน (Prevention) การตรวจจับ (Detection) และการตอบสนอง (Response) เป็นต้น โดยพิจารณาตามคุณสมบัติความมั่นคงที่เหมาะสมและระดับความเสี่ยงของสินทรัพย์ ซึ่งแนวทางความมั่นคง นั้นจะมีผลต่อความต้องการความมั่งคงของสินทรัพย์ของตนที่ได้กำหนดไว้ก่อนหน้า โดยรายละเอียดของแบบรูปดังตารางที่ 3.6

ตารางที่ 3.6 รายละเอียดแบบรูปแนวคิดความมั่นคงขององค์กร

ชื่อแบบรูปความมั่นคง	แนวคิดความมั่นคงขององค์กร
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	1. แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 2. แบบรูปการกำหนดความเสี่ยง : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขของการดำเนินการ	1. ข้อมูลสินทรัพย์และคุณสมบัติความมั่นคงของสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร 2. ข้อมูลค่าความเสี่ยงของสินทรัพย์จากแบบรูปการกำหนดความเสี่ยง
บริบท	สินทรัพย์ต้องการการป้องกันและคุณสมบัติด้านความมั่นคงที่ต้องมี

ตารางที่ 3.6 รายละเอียดแบบรูปแนวคิดความมั่นคงขององค์กร (ต่อ)

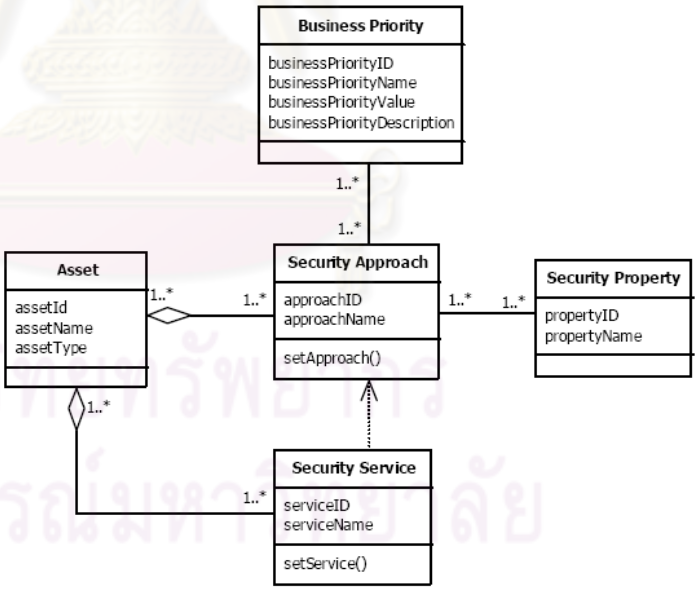
ปัญหา	จะทำการกำหนดแนวคิดความมั่นคงให้แก่สินทรัพย์ขององค์กรได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น ซึ่งได้แก่ สินทรัพย์องค์กรโดยแยกตามชนิด และคุณสมบัติความมั่นคงของสินทรัพย์นั้น 2. รวบรวมข้อมูลค่าความเสี่ยงของสินทรัพย์ 3. เลือกแนวคิดความมั่นคงที่เหมาะสมให้กับสินทรัพย์ ทั้งการป้องกัน การตรวจจับ และการตอบสนอง โดยพิจารณาจากข้อมูลที่รวบรวมได้จากข้อที่ 1 และ 2
โครงสร้าง	

1.7) **บริการความมั่นคงขององค์กร** (Enterprise Security Services) เป็นการแนะนำให้องค์กรเลือกบริการความมั่นคง (Security Services) ให้กับสินทรัพย์ของตน ซึ่งต้องสอดคล้องกับแนวทางความมั่นคงที่ได้กำหนดไว้ก่อนหน้า ตัวอย่างบริการด้านความมั่นคง เช่น การระบุและพิสูจน์ตัวตน การควบคุมการเข้าถึง เป็นต้น โดยรายละเอียดของแบบรูปดังตารางที่ 3.7

ตารางที่ 3.7 รายละเอียดแบบรูปบริการความมั่นคงขององค์กร

ชื่อแบบรูปความมั่นคง	บริการความมั่นคงขององค์กร
กลุ่มของแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
แบบรูปความมั่นคงที่เกี่ยวข้อง	1. แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 2. แบบรูปแนวคิดความมั่นคงขององค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง **หมายเหตุ** : แบบรูปบริการความมั่นคงขององค์กรเป็นส่วนขยายจากแบบรูปแนวคิดความมั่นคงขององค์กร

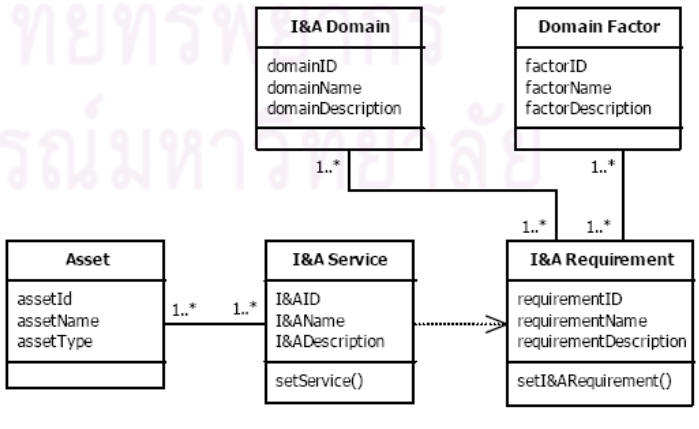
ตารางที่ 3.7 รายละเอียดแบบรูปบริการความมั่นคงขององค์กร (ต่อ)

เงื่อนไขของการดำเนินการ	1. ข้อมูลสินทรัพย์และคุณสมบัติความมั่นคงของสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร 2. ข้อมูลแนวคิดความมั่นคงของสินทรัพย์จากแบบรูปแนวคิดความมั่นคงขององค์กร
บริบท	สินทรัพย์ขององค์กรนั้นต้องการบริการด้านความมั่นคง โดยพิจารณาจากแนวคิดความมั่นคงที่ได้กำหนดไว้ก่อนหน้า
ปัญหา	จะทำการกำหนดบริการความมั่นคงของสินทรัพย์องค์กรได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น ซึ่งได้แก่ สินทรัพย์องค์กรโดยแยกตามชนิด คุณสมบัติความมั่นคงของสินทรัพย์นั้น และแนวคิดความมั่นคงขององค์กร 2. ระบุบริการความมั่นคงสำหรับสินทรัพย์องค์กร โดยต้องสอดคล้องตามแนวคิดความมั่นคง 3. ทวนสอบบริการความมั่นคงอย่างสม่ำเสมอ เมื่อมีสถานการณ์เปลี่ยนแปลงไป
โครงสร้าง	

2) **การระบุและการพิสูจน์ตัวตน** (Identification and Authentication) เป็นกลุ่มแบบรูปความมั่นคงที่มุ่งเน้นการตรวจสอบการเข้าถึงและเข้าใช้ทรัพยากรภายในระบบของผู้ใช้งาน โดยแบบรูปในกลุ่มนี้ประกอบด้วย

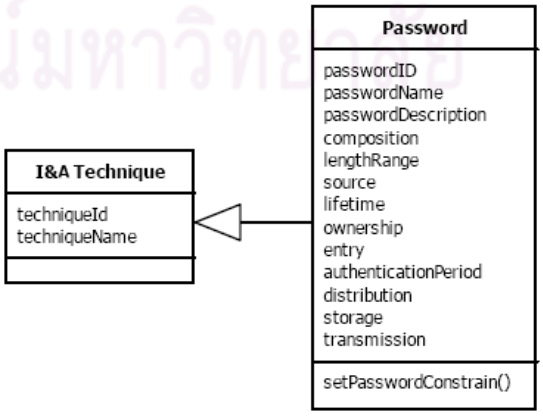
2.1) **ความต้องการด้านการระบุและการพิสูจน์ตัวตน** (Identification and Authentication Requirements) เป็นแบบรูปที่กำหนดความต้องการพื้นฐานด้านการระบุและพิสูจน์ตัวตน ซึ่งจะช่วยให้สามารถกำหนดความต้องการได้อย่างเหมาะสมกับสถานการณ์ใดๆ ที่อาจจะเกิดขึ้น โดยรายละเอียดของแบบรูปดังตารางที่ 3.8

ตารางที่ 3.8 รายละเอียดแบบรูปความต้องการด้านการระบุและพิสูจน์ตัวตน

ชื่อแบบรูปความมั่นคง	ความต้องการด้านการระบุและพิสูจน์ตัวตน
กลุ่มของแบบรูปความมั่นคง	การระบุและการพิสูจน์ตัวตน
แบบรูปความมั่นคงที่เกี่ยวข้อง	ไม่มี เนื่องจากเป็นแบบรูปเริ่มต้นของการดำเนินการสร้างการระบุและพิสูจน์ตัวตน ซึ่งจะต้องพิจารณาตามสภาวะแวดล้อมขององค์กรเป็นหลัก
เงื่อนไขของการดำเนินการ	ไม่มี เนื่องจากเป็นแบบรูปเริ่มต้นของการดำเนินการสร้างการระบุและพิสูจน์ตัวตน ซึ่งจะต้องพิจารณาตามสภาวะแวดล้อมขององค์กรเป็นหลัก
บริบท	องค์กรต้องการระบุความต้องการของบริการการระบุและพิสูจน์ตัวตน ทั้งนี้เพื่อกำหนดการเข้าถึงเพื่อใช้งานระบบ
ปัญหา	องค์กรนั้นจะทำการกำหนดความต้องการของบริการการระบุและพิสูจน์ตัวตนได้อย่างไร
ผลเฉลย	1. ระบุขอบเขตของการใช้บริการการระบุและพิสูจน์ตัวตน 2. ระบุปัจจัยที่มีผลต่อการกำหนดความต้องการของการใช้บริการการระบุและพิสูจน์ตัวตน 3. ระบุความต้องการของการใช้บริการการระบุและพิสูจน์ตัวตน ในแต่ละขอบเขตที่ระบุในข้อที่ 1 4. สร้างความสัมพันธ์ระหว่างปัจจัยในข้อ 2 และความต้องการในข้อ 3
โครงสร้าง	

2.2) **การออกแบบและใช้งานรหัสผ่าน** (Password Design and Use) แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและการพิสูจน์ตัวตน โดยรายละเอียดของแบบรูปดังตารางที่ 3.9

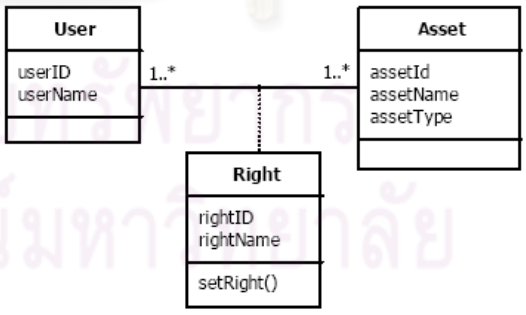
ตารางที่ 3.9 รายละเอียดแบบรูปการออกแบบและใช้งานรหัสผ่าน

ชื่อแบบรูปความมั่นคง	การออกแบบและใช้งานรหัสผ่าน
กลุ่มของแบบรูปความมั่นคง	การระบุและการพิสูจน์ตัวตน
แบบรูปความมั่นคงที่เกี่ยวข้อง	แบบรูปความต้องการด้านการระบุและพิสูจน์ตัวตน : กลุ่มแบบรูปการระบุและพิสูจน์ตัวตน
เงื่อนไขของการดำเนินการ	ข้อมูลขอบเขต ปัจจัย และความต้องการของการใช้บริการการระบุและพิสูจน์ตัวตนจากแบบรูปความต้องการด้านการระบุและพิสูจน์ตัวตน
บริบท	องค์กรต้องการที่จะกำหนดคุณลักษณะของรหัสผ่านที่ต้องการใช้บริการ
ปัญหา	ทำอย่างไรจึงจะสร้าง จัดการ และใช้งานรหัสผ่านได้อย่างมั่นคงและปลอดภัย
ผลเฉลย	1. กำหนดลักษณะตัวอักษรที่จะใช้ในรหัสผ่าน 2. กำหนดความยาวของรหัสผ่าน 3. กำหนดที่มาของรหัสผ่าน 4. กำหนดอายุการใช้งานของรหัสผ่าน 5. กำหนดบุคคลที่มีสิทธิในการใช้งานรหัสผ่าน 6. กำหนดวิธีการในการกรอกรหัสผ่าน 7. กำหนดระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน 8. กำหนดวิธีการในการส่งรหัสผ่านให้กับผู้ใช้งาน 9. กำหนดวิธีการในการจัดเก็บรหัสผ่าน 10. กำหนดวิธีการในการถ่ายโอนรหัสผ่าน เพื่อใช้ในการตรวจสอบ
โครงสร้าง	

3) **แบบจำลองควบคุมการเข้าถึง** (Access Control Models) เป็นกลุ่มแบบรูปความมั่นคงที่มุ่งเน้นการควบคุมการเข้าถึงทรัพยากรภายในระบบ โดยกำหนดเป็นเงื่อนไขข้อบังคับในระดับต่างๆ ทั้งระดับสถาปัตยกรรม ระดับโปรแกรมประยุกต์ และระดับล่างของการปฏิบัติงาน โดยแบบรูปในกลุ่มนี้ประกอบด้วย

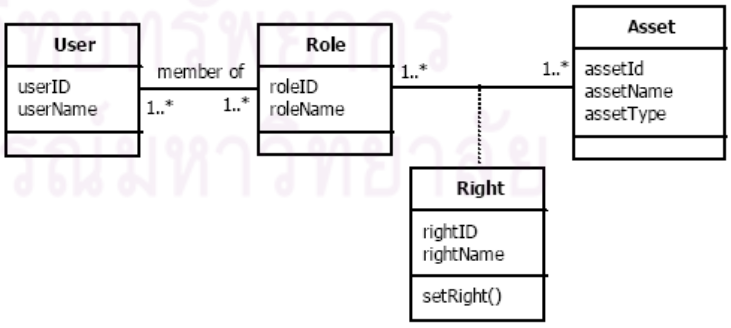
3.1) **การให้อำนาจ** (Authorization) แบบรูปนี้ช่วยในการกำหนดว่าใครที่จะได้สิทธิในการเข้าถึงทรัพยากรภายในระบบ ในสภาพแวดล้อมที่ต้องมีการควบคุมการเข้าถึงและเข้าใช้ทรัพยากรของระบบ โดยรายละเอียดของแบบรูปดังตารางที่ 3.10

ตารางที่ 3.10 รายละเอียดแบบรูปการให้อำนาจ

ชื่อแบบรูปความมั่นคง	การให้อำนาจ
กลุ่มของแบบรูปความมั่นคง	การระบุและการพิสูจน์ตัวตน
แบบรูปความมั่นคงที่เกี่ยวข้อง	แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขของการดำเนินการ	ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
บริบท	ระบบมีทรัพยากรที่จำเป็นต้องสร้างการควบคุมการเข้าถึง
ปัญหา	จะอธิบายว่าสิ่งกระตุ้นนั้นสามารถเข้าถึงทรัพยากรของระบบได้อย่างไร
ผลเฉลย	1. ระบุสิ่งกระตุ้นที่ต้องการเข้าถึงทรัพยากรของระบบ 2. ระบุทรัพยากรของระบบที่ถูกควบคุมการเข้าถึง 3. ระบุสิทธิที่ควบคุมการเข้าถึงเพื่อใช้งานทรัพยากรของระบบ
โครงสร้าง	

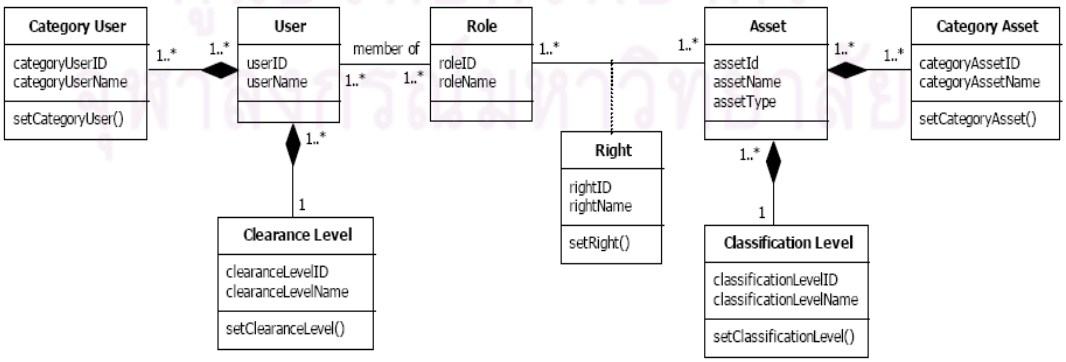
3.2) **การควบคุมการเข้าถึงเชิงบทบาท** (Role-Based Access Control) แบบรูปนี้เป็นการกำหนดสิทธิบนพื้นฐานของบทบาทที่บุคคลพึงจะได้รับ เพื่อใช้ในการควบคุมการเข้าถึงทรัพยากรที่มีในองค์กร โดยมีการนำเสนอกลุ่มบุคคล ประเภทข้อมูล และการดำเนินการที่บุคคลสามารถทำได้กับทรัพยากรที่ต้องการเข้าถึง โดยรายละเอียดของแบบรูปดังตารางที่ 3.11

ตารางที่ 3.11 รายละเอียดแบบรูปการควบคุมการเข้าถึงเชิงบทบาท

ชื่อแบบรูปความมั่นคง	การควบคุมการเข้าถึงเชิงบทบาท
กลุ่มของแบบรูปความมั่นคง	แบบจำลองควบคุมการเข้าถึง
แบบรูปความมั่นคงที่เกี่ยวข้อง	1. แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง 2. แบบรูปการให้อำนาจ : กลุ่มแบบรูปแบบจำลองควบคุมการเข้าถึง **<u>หมายเหตุ</u>** : แบบรูปการควบคุมการเข้าถึงเชิงบทบาทเป็นส่วนขยายจากแบบรูปการให้อำนาจ
เงื่อนไขก่อนดำเนินการ	ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
บริบท	องค์กรใดๆ ที่มีทรัพยากรซึ่งจำเป็นต้องควบคุมการเข้าถึง โดยต้องอยู่ในกรณีที่ผู้ใช้งานและทรัพยากรมีเป็นจำนวนมาก
ปัญหา	องค์กรจะทำการกำหนดสิทธิในการเข้าถึงทรัพยากรจากบทบาทของบุคคลได้อย่างไร
ผลเฉลย	กำหนดสิทธิในการเข้าถึงทรัพยากรขององค์กร โดยพิจารณาจากบทบาทและหน้าที่การทำงาน ซึ่งต้องมีความสอดคล้องตามนโยบายพื้นฐานด้านความมั่นคง
โครงสร้าง	

3.3) **ความมั่นคงหลายระดับ** (Multilevel Security) ในบางกรณีที่ทรัพยากรหรือผู้ใช้งานมีระดับความสำคัญที่แตกต่างกันออกไป แบบรูปนี้จะช่วยในการจัดกลุ่มหรือกำหนดระดับของทั้งทรัพยากรและผู้ใช้งาน รวมถึงกำหนดสิทธิในการเข้าถึงทรัพยากรดังกล่าว ทั้งนี้เพื่อใช้ในการตรวจสอบการเข้าถึงว่าผู้ใช้มีระดับสิทธิมากพอที่จะเข้าถึงทรัพยากรใดๆ ขององค์กรหรือไม่ โดยรายละเอียดของแบบรูปดังตารางที่ 3.12

ตารางที่ 3.12 รายละเอียดแบบรูปความมั่นคงหลายระบบ

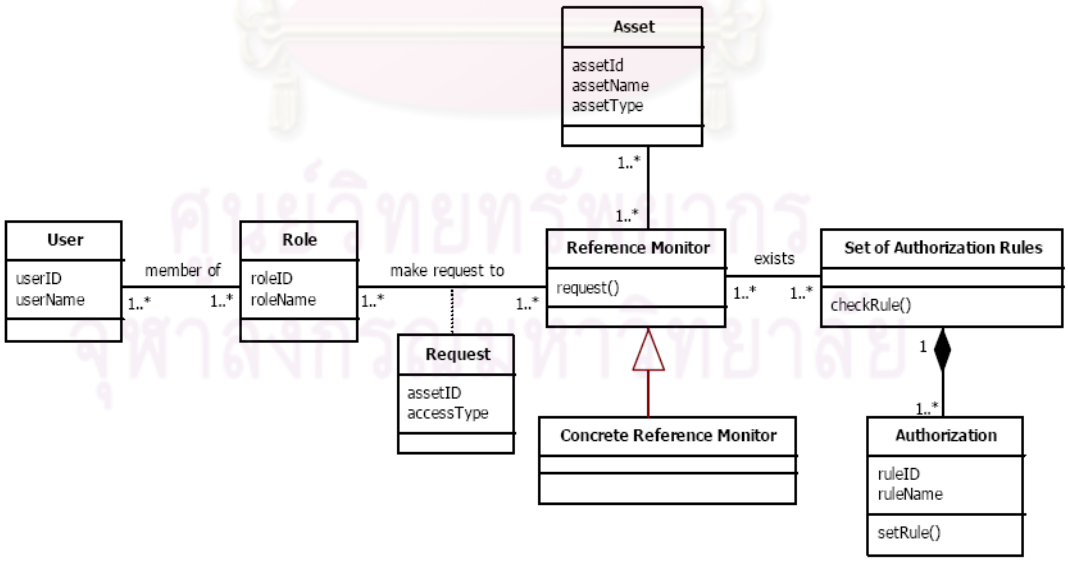
ชื่อแบบรูปความมั่นคง	ความมั่นคงหลายระบบ
กลุ่มของแบบรูปความมั่นคง	แบบจำลองควบคุมการเข้าถึง
แบบรูปความมั่นคงที่เกี่ยวข้อง	แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนดำเนินการ	ข้อมูลสินทรัพย์จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
บริบท	ระบบมีทรัพยากรเชิงวิกฤต ซึ่งจะมีปัญหาเกิดขึ้นเมื่อทรัพยากรนั้นถูกเปิดเผย
ปัญหา	จะสร้างการควบคุมการเข้าถึงของทรัพยากรที่มีความสำคัญนั้นได้อย่างไร โดยยึดจากตำแหน่งหน้าที่ในองค์กรเป็นหลัก รวมถึงสามารถกำหนดสิทธิของผู้ใช้งานตามระดับของทรัพยากรได้
ผลเฉลย	1. จัดแบ่งหมวดหมู่ของผู้ใช้งานตามตำแหน่งหน้าที่การทำงานภายในองค์กร 2. จัดแบ่งหมวดหมู่ของทรัพยากรตามระดับความสำคัญ เช่น ลับที่สุด, ลับ, เปิดเผย เป็นต้น
โครงสร้าง  	

3.4) **การตรวจสอบการเข้าถึง** (Reference Monitor) แบบรูปนี้เป็นข้อบังคับการเข้าถึงทรัพยากรเป้าหมาย โดยเพิ่มความเข้มงวดเมื่อมีการร้องขอการเข้าถึงทรัพยากรของระบบ โดยทั้งนี้จะทำการตรวจสอบกับเซตของบทบาทที่ได้รับอนุญาตและสิทธิสำหรับบทบาทดังกล่าว โดยรายละเอียดของแบบรูปดังตารางที่ 3.13

ตารางที่ 3.13 รายละเอียดแบบรูปการตรวจสอบการเข้าถึง

ชื่อแบบรูปความมั่นคง	การตรวจสอบการเข้าถึง
กลุ่มของแบบรูปความมั่นคง	แบบจำลองควบคุมการเข้าถึง
แบบรูปความมั่นคงที่เกี่ยวข้อง	แบบรูปการนิยามบทบาทและสิทธิ: กลุ่มแบบแบบจำลองควบคุมการเข้าถึง
เงื่อนไขก่อนดำเนินการ	ข้อมูลการดำเนินการสำหรับบทบาทจากแบบรูปการนิยามบทบาทและสิทธิ
บริบท	ระบบซึ่งมีผู้ใช้งานหรือการประมวลผลใดๆ ที่ร้องขอเข้าถึงทรัพยากรของระบบนั้น
ปัญหา	ทำอย่างไรจึงจะควบคุมคำร้องของของผู้ใช้งานหรือการประมวลผลใดๆ ในทุกๆ ระดับของระบบ
ผลเฉลย	ระบุข้อบังคับการเข้าถึงที่จะควบคุมและตรวจสอบคำร้องขอใช้ทรัพยากรของระบบ

โครงสร้าง



3.5) **การนิยามบทบาทและสิทธิ** (Role Rights Definition) แบบรูปนี้เป็นการนำเสนอแนวทางที่แน่นอนในการกำหนดสิทธิต่ำสุดให้กับบทบาทใดๆ สำหรับระบบที่ต้องการความมั่นคง ทั้งนี้เพื่อให้ทราบว่าบทบาทหนึ่งๆ มีสิทธิในการดำเนินการกับทรัพยากรใดได้บ้าง โดยรายละเอียดของแบบรูปดังตารางที่ 3.14

ตารางที่ 3.14 รายละเอียดแบบรูปการนิยามบทบาทและสิทธิ

ชื่อแบบรูปความมั่นคง	การนิยามบทบาทและสิทธิ
กลุ่มของแบบรูปความมั่นคง	แบบจำลองควบคุมการเข้าถึง
แบบรูปความมั่นคงที่เกี่ยวข้อง	ไม่มี เนื่องจากเป็นแบบรูปที่ช่วยเสนอแนวความคิดในการกำหนดสิทธิให้กับบทบาทใดๆ เท่านั้น
เงื่อนไขก่อนดำเนินการ	ไม่มี เนื่องจากเป็นแบบรูปที่ช่วยเสนอแนวความคิดในการกำหนดสิทธิให้กับบทบาทใดๆ เท่านั้น
บริบท	ระบบนั้นประกอบด้วยหลายบทบาท ดังนั้นการกำหนดบทบาทที่เหมาะสมจึงเป็นสิ่งสำคัญ
ปัญหา	จะกำหนดสิทธิให้กับบทบาทนั้นได้อย่างไร โดยคำนึงถึงสิทธิขั้นพื้นฐานของแต่ละบทบาท
ผลเฉลย	1. สร้างแผนภาพยูสเคสโดยผู้กระทำจะถูกแทนที่ด้วยบทบาท 2. สร้างแผนภาพซีเควนสำหรับในแต่ละยูสเคสนั้น 3. วิเคราะห์แผนภาพซีเควนเพื่อหาการดำเนินการในการกำหนดสิทธิของบทบาท 4. หาข้อยกเว้นในแผนภาพยูสเคสเพื่อหาการกระทำที่ละเมิดความมั่นคง 5. การเพิ่ม-ลบกฎการให้อำนาจจะกระทำก็ต่อเมื่อการเปลี่ยนแปลงของยูสเคสใดๆ
โครงสร้าง	เนื่องจากแบบรูปนี้กล่าวถึงขั้นตอนในการกำหนดสิทธิพื้นฐานให้กับบทบาท ดังนั้นจึงไม่มีแผนภาพโครงสร้างแสดงเพิ่มเติม

3.1.2 ศึกษาและวิเคราะห์มาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 27002:2005

มาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 27002:2005 ได้ถูกนำมาใช้เพื่อเป็นกรอบงานของการออกแบบกระบวนการ เนื่องจากมาตรฐานทั้ง 2 ได้มุ่งอธิบายถึงข้อกำหนดและข้อปฏิบัติสำหรับการสร้างระบบความมั่นคงให้กับสารสนเทศภายในองค์กรโดยเฉพาะ อีกทั้งมาตรฐานดังกล่าวได้บ่งชี้ถึงแนวทางปฏิบัติที่สำคัญ องค์ประกอบที่จำเป็นต้องใช้และที่ได้ออกมา

รวมถึงวัฏจักรของการดำเนินการภายใต้สภาวะแวดล้อมของความมั่นคงอย่างต่อเนื่อง การศึกษาและวิเคราะห์ในส่วนนี้จึงช่วยให้การออกแบบกระบวนการมีความถูกต้องและสมบูรณ์มากยิ่งขึ้น โดยรายละเอียดที่เกี่ยวข้องของแต่ละมาตรฐานมีดังต่อไปนี้

1) **มาตรฐาน** ISO/IEC 27001:2005 เป็นมาตรฐานที่มีการดำเนินการเกี่ยวข้องกับการจัดการความมั่นคงสารสนเทศ (Information Security Management System: ISMS) โดยตรง ซึ่งมีรูปแบบตามโมเดล PDCA ซึ่งเป็นระบบบริหารที่มีการจัดการเป็นวงรอบและต่อเนื่อง โดยเริ่มตั้งแต่การจัดตั้ง (Plan) การนำไปใช้และการดำเนินการ (Do) การเฝ้าสังเกตและทวนสอบ (Check) การบำรุงรักษาและการปรับปรุง (Act) โครงสร้างดังกล่าวได้ถูกนำมาศึกษาและวิเคราะห์เพื่อใช้เป็นแนวทางของการออกแบบการดำเนินการกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยรายละเอียดของโครงสร้างมีดังนี้

1.1) **การจัดตั้งระบบ** (Establish ISMS) มีรายละเอียดดังต่อไปนี้

1.1.1) กำหนดขอบเขตของการจัดตั้งระบบ โดยพิจารณาจากสภาพแวดล้อมโดยรวมขององค์กรเป็นสำคัญ ทั้งลักษณะทางธุรกิจ โครงสร้างขององค์กร สถานที่ตั้ง สินทรัพย์ประเภทสารสนเทศ และเทคโนโลยีที่ถูกนำมาใช้

1.1.2) กำหนดนโยบายของระบบ โดยอาจรวมถึงกรอบงาน กฎหรือข้อบังคับ และหลักการที่มีความเกี่ยวข้อง

1.1.3) กำหนดรูปแบบของการประเมินความเสี่ยง ในที่นี้คือ ระเบียบวิธีการประเมิน เกณฑ์และระดับของการยอมรับความเสี่ยง

1.1.4) กำหนดความเสี่ยง โดยระบุเป็นสินทรัพย์ที่ต้องการสร้างความมั่นคง ภัยคุกคามที่ก่อให้เกิดความเสี่ยงของสินทรัพย์นั้น จุดอ่อนที่จะถูกใช้โดยภัยคุกคาม รวมถึงผลกระทบต่อคุณสมบัติด้านความมั่นคงของสินทรัพย์

1.1.5) วิเคราะห์และประเมินความเสี่ยง โดยประเมินถึงผลกระทบที่องค์กรจะได้รับเมื่อมีความเสี่ยงใดๆ เกิดขึ้น ระดับของความเสี่ยง และสรุปถึงวิธีการยอมรับหรือป้องกันรักษาความเสี่ยงนั้น

1.1.6) ระบุและสรุปถึงวิธีการป้องกันรักษาความเสี่ยง โดยเลือกเป็นการควบคุมที่มีความเหมาะสม ซึ่งต้องพิจารณาจากผลการวิเคราะห์และประเมินความเสี่ยง

1.1.7) สรุปถึงการจัดการกับความเสี่ยงที่ผันแปรค่า

1.1.8) สรุปถึงการจัดการสิทธิการใช้งานระบบ รวมถึงการประยุกต์ใช้

1.1.9) จัดทำรายการความสามารถ (Statement of Applicable: SOA) ของการควบคุมที่ได้เลือกใช้ โดยรวมถึงการระบุเหตุผลของการเลือกใช้

1.2) **การนำไปใช้และการดำเนินการของระบบ** (Implement and Operate the ISMS) มีรายละเอียดดังต่อไปนี้

1.2.1) กำหนดแผนการลดความเสี่ยง โดยระบุถึงการจัดการที่เหมาะสม ทรัพยากรที่จำเป็นต้องใช้ รวมถึงบทบาทและหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง

1.2.2) ดำเนินการตามแผนการลดความเสี่ยงที่ได้กำหนดไว้

1.2.3) ดำเนินการตามการควบคุมที่ได้เลือกไว้ตามข้อที่ 1.1.6)

1.2.4) กำหนดวิธีการวัดประสิทธิภาพของการควบคุมที่ได้เลือกไว้ รวมถึงระบุตัวชี้วัดประสิทธภาพ

1.2.5) จัดทำรายการฝึกอบรมให้กับผู้ที่เกี่ยวข้องกับระบบ

1.2.6) จัดการการดำเนินการประยุกต์ใช้งานระบบ

1.2.7) จัดการสิ่งซึ่งเป็นทรัพยากรที่ได้นำมาประยุกต์ใช้ในการดำเนินการของระบบ

1.2.8) พัฒนาส่วนการทำงานหรือส่วนการควบคุมใดๆ ของระบบซึ่งเป็นส่วนที่ใช้ควบคุมป้องการความผิดพลาดที่อาจจะเกิดขึ้น

1.3) **การเฝ้าสังเกตและทวนสอบระบบ** (Monitor and Review ISMS) มีรายละเอียดดังต่อไปนี้

1.3.1) ดำเนินการเฝ้าสังเกตและทวนสอบระบบ เพื่อตรวจหาและป้องกันความผิดพลาดที่อาจจะเกิดขึ้น

1.3.2) ทบทวนประสิทธิภาพของระบบอย่างสม่ำเสมอ ทั้งนี้จะต้องเป็นไปตามวัตถุประสงค์ นโยบาย และการควบคุมที่ได้เลือกไว้

1.3.3) วัดประสิทธิภาพของระบบ ทั้งนี้เพื่อตรวจสอบว่าเป็นไปตามความต้องการด้านความมั่นคงหรือไม่

1.3.4) ทบทวนการประเมินความเสี่ยงตามแผนการลดความเสี่ยง รวมถึงความเสี่ยงที่ผันแปรโดยสม่ำเสมอตามรอบของระยะที่ได้กำหนดไว้

1.3.5) ดำเนินการตรวจติดตามภายในระบบ โดยให้เป็นไปตามแผนการณ์ที่ได้กำหนดไว้ ทั้งที่เป็นวัตถุประสงค์ของการควบคุม การควบคุมที่ได้เลือกไว้ และส่วนการทำงานของระบบ

1.3.6) รวบรวมและจัดทำการจัดการทวนสอบ ทั้งนี้เพื่อประเมินและสรุปผลว่า ควรมีการปรับปรุงระบบมาก-น้อยเพียงใด

1.3.7) ปรับปรุงแผนความมั่นคง ทั้งนี้เพื่อสามารถนำมาใช้ในการทวนสอบระบบครั้งถัดไป

1.3.8) บันทึกการกระทำและเหตุการณ์ที่มีผลกระทบต่อประสิทธิภาพและประสิทธิผลของระบบ

1.4) **การบำรุงรักษาและการปรับปรุงระบบ** (Maintain and Improve the ISMS) มีรายละเอียดดังต่อไปนี้

1.4.1) ระบุการปรับปรุงระบบ โดยพิจารณาและวิเคราะห์การประเมินและสรุปผลจากขั้นตอนการเฝ้าสังเกตและทวนสอบระบบ

1.4.2) ดำเนินการตามการกระทำและการป้องกันสำหรับการปรับปรุงระบบ ซึ่งอาจประยุกต์ใช้จากประสบการณ์ที่เคยเกิดขึ้นและมีความคล้ายคลึงกัน

1.4.3) ประกาศการกระทำและการป้องกันสำหรับการปรับปรุงระบบให้ผู้ที่เกี่ยวข้องกับระบบได้รับทราบ และเกิดความเข้าใจที่ตรงกัน

1.4.4) ทำให้แน่ใจว่า การกำหนดวิธีการปรับปรุงระบบนั้นได้บรรลุถึงวัตถุประสงค์ที่ได้วางไว้

2) **มาตรฐาน** ISO/IEC 27002:2005 มาตรฐานนี้ได้บ่งบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่จะเกิดจากจุดอ่อนของระบบการจัดการความมั่นคงสารสนเทศ ซึ่งจะต้องปฏิบัติควบคู่กับข้อกำหนดในมาตรฐาน ISO/IEC 27001:2005 วิธีปฏิบัติดังกล่าวได้แบ่งแยกหัวข้อสำคัญออกเป็น 11 หมวดหลัก โดยรายละเอียดในแต่ละหมวด มีดังต่อไปนี้

2.1) **นโยบายด้านความมั่นคง** (Security Policy) ซึ่งประกอบด้วยนโยบายความมั่นคงสำหรับสินทรัพย์ประเภทสารสนเทศ โดยมีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงสำหรับสินทรัพย์ประเภทสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎข้อบังคับและระเบียบการปฏิบัติที่เกี่ยวข้อง โดยจะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายดังกล่าวตามระยะเวลาที่กำหนด

2.2) **โครงสร้างด้านความมั่นคงสารสนเทศ** (Organization of Information Security) มีรายละเอียดดังต่อไปนี้

2.2.1) โครงสร้างทางด้านความมั่นคงภายในองค์กร เพื่อบริหารและจัดการความมั่นคงสำหรับสินทรัพย์ประเภทสารสนเทศขององค์กร

2.2.2) โครงสร้างทางด้านความมั่นคงที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงสำหรับสินทรัพย์ประเภทสารสนเทศและอุปกรณ์ประมวลผลสินทรัพย์ประเภทสารสนเทศขององค์กรที่ถูกเข้าถึงสำหรับติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

2.3) **การจัดการสินทรัพย์** (Asset Management) มีรายละเอียดดังต่อไปนี้

2.3.1) หน้าที่ความรับผิดชอบต่อสินทรัพย์ขององค์กร เพื่อป้องกันสินทรัพย์ขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

2.3.2) การจัดหมวดหมู่สินทรัพย์ประเภทสารสนเทศ เพื่อกำหนดระดับของการป้องกันสินทรัพย์ประเภทสารสนเทศขององค์กรอย่างเหมาะสม

2.4) **ความมั่นคงด้านบุคลากร** (Human Resources Security) มีรายละเอียดดังต่อไปนี้

2.4.1) การสร้างความมั่นคงก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดหรือเข้าใจผิดของพนักงานและผู้เกี่ยวข้องดังกล่าว

2.4.2) การสร้างความมั่นคงในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคง บทบาทและหน้าที่ความรับผิดชอบ รวมถึงความเข้าใจเกี่ยวกับนโยบายด้านความมั่นคง และเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

2.4.3) การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงบทบาทและหน้าที่ความรับผิดชอบของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

2.5) **ความมั่นคงด้านกายภาพและสภาวะแวดล้อม** (Physical and Environmental Security) มีรายละเอียดดังต่อไปนี้

2.5.1) สถานที่หรือบริเวณที่ต้องมีการรักษาความมั่นคง เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อสินทรัพย์ประเภทสารสนเทศขององค์กร

2.5.2) ความมั่นคงของอุปกรณ์ประมวลผลสินทรัพย์ประเภทสารสนเทศเพื่อป้องกันการสูญหาย การเกิดความเสียหาย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของสินทรัพย์ประเภทสารสนเทศขององค์กร และทำให้กิจกรรมการดำเนินการขององค์กรเกิดการติดขัดหรือหยุดชะงัก

2.6) **การจัดการการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communications and Operations Management)** มีรายละเอียดดังต่อไปนี้

2.6.1) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงานเพื่อให้การดำเนินการที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสินทรัพย์ประเภทสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

2.6.2) การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษาระดับความมั่นคงของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

2.6.3) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

2.6.4) การป้องกันซอฟต์แวร์ที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสินทรัพย์ประเภทสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

2.6.5) การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสินทรัพย์ประเภทสารสนเทศและอุปกรณ์ประมวลผลสินทรัพย์ประเภทสารสนเทศ

2.6.6) การบริหารจัดการทางด้านความมั่นคงสำหรับเครือข่ายขององค์กร เพื่อป้องกันสินทรัพย์ประเภทสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

2.6.7) การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือทำลายสินทรัพย์ประเภทสารสนเทศโดยไม่ได้รับอนุญาต

2.6.8) การแลกเปลี่ยนสินทรัพย์ประเภทสารสนเทศ เพื่อรักษาความมั่นคงของซอฟต์แวร์และสินทรัพย์ประเภทสารสนเทศที่มีการแลกเปลี่ยนภายในองค์กร และแลกเปลี่ยนกับหน่วยงานภายนอก

2.6.9) การสร้างความมั่นคงสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และการใช้งาน

2.6.10) การเฝ้าระวังทางด้านความมั่นคง เพื่อตรวจจับกิจกรรมการประมวลผลสินทรัพย์ประเภทสารสนเทศที่ไม่ได้รับอนุญาต

2.7) **การควบคุมการเข้าถึง** (Access Control) มีรายละเอียดดังต่อไปนี้

2.7.1) ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ เพื่อควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร

2.7.2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต

2.7.3) หน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสินทรัพย์ประเภทสารสนเทศและอุปกรณ์ประมวลผลสินทรัพย์ประเภทสารสนเทศ

2.7.4) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

2.7.5) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

2.7.6) การควบคุมการเข้าถึงซอฟต์แวร์และสินทรัพย์ประเภทสารสนเทศที่ไม่ได้รับอนุญาต

2.7.7) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก เพื่อสร้างความมั่นคงให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

2.8) **การจัดการการได้มาซึ่งการพัฒนาและการบำรุงรักษาระบบสารสนเทศ** (Information Systems Acquisition, Development and Maintenance) มีรายละเอียดดังต่อไปนี้

2.8.1) ข้อกำหนดด้านความมั่นคงสำหรับระบบสารสนเทศ เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงเป็นองค์ประกอบพื้นฐานที่สำคัญ

2.8.2) การประมวลผลสินทรัพย์ประเภทสารสนเทศในซอฟต์แวร์ เพื่อป้องกันความผิดพลาด การสูญหาย การเปลี่ยนแปลงแก้ไขสินทรัพย์ประเภทสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานที่ผิดวัตถุประสงค์

2.8.3) มาตรการการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูล โดยใช้วิธีการทางการเข้ารหัสข้อมูล

2.8.4) การสร้างความมั่นคงให้กับไฟล์ของระบบสารสนเทศที่ให้บริการ

2.8.5) การสร้างความมั่นคงสำหรับกระบวนการในการพัฒนาระบบสารสนเทศและกระบวนการสนับสนุน เพื่อรักษาความมั่นคงสำหรับซอฟต์แวร์และสินทรัพย์ประเภทสารสนเทศของระบบ

2.8.6) การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

2.9) **การจัดการเหตุการณ์ละเมิดความมั่นคงสารสนเทศ** (Information Security Incident Management) มีรายละเอียดดังต่อไปนี้

2.9.1) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคง เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงของระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

2.9.2) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงสำหรับสินทรัพย์ประเภทสารสนเทศขององค์กร

2.10) **การจัดการความต่อเนื่องในการดำเนินการ** (Business Continuity Management) โดยเกี่ยวกับพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้คืนระบบสารสนเทศกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

2.11) **การปฏิบัติตามข้อกำหนดทางกฎหมายและบทลงโทษ** (Compliance) มีรายละเอียดดังต่อไปนี้

2.11.1) การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงอื่นๆ

2.11.2) การปฏิบัติตามนโยบาย มาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงตามที่องค์กรกำหนดไว้

2.11.3) การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดเพื่อป้องกันการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

3.1.3 ศึกษาและวิเคราะห์หลักการ แนวทางปฏิบัติและงานวิจัยต่าง ๆ ที่เกี่ยวข้อง

การศึกษาหลักการ แนวทางปฏิบัติและงานวิจัยต่างๆ ที่มีความเกี่ยวข้องกับกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเพิ่มเติมนั้น จะช่วยให้กระบวนการที่ได้ออกแบบมีความละเอียดมากยิ่งขึ้นทั้งในด้านของหลักการความมั่นคง โดยเฉพาะการสร้างการควบคุมการเข้าถึง และด้านของหลักการออกแบบกระบวนการ ทั้งนี้ได้เกิดจากการรวบรวมเอาประเด็นสำคัญต่างๆ ของแต่ละงานมาประยุกต์ใช้ โดยข้อมูลที่นำมาใช้นั้น มีดังต่อไปนี้

1) **วิธีปฏิบัติ** (Practices) ส่วนของข้อมูลในหัวข้อนี้ เป็นแนวทางปฏิบัติซึ่งเป็นที่ยอมรับกันในทางสากล ทั้งแบบรูปซึ่งเป็นที่นิยมถูกนำมาใช้เป็นหลักการสำคัญในงานวิจัยต่างๆ วิธีปฏิบัติที่ดีของการสร้างการควบคุมการเข้าถึงที่หลายๆ องค์กรได้นำมาใช้ รวมถึงแนวทางที่ถูกต้องของการออกแบบกระบวนการ โดยวิธีปฏิบัตินั้นประกอบด้วย 2 ส่วนข้อมูลสำคัญ ดังนี้

1.1) **วิธีปฏิบัติซึ่งมักนิยมใช้** (Best Practices) เป็นวิธีปฏิบัติที่หลายๆ องค์กรได้ประยุกต์ใช้ โดยกล่าวถึงแนวทางการสร้างการควบคุมการเข้าถึงทรัพยากรภายในองค์กร คือการอธิบายถึงสิ่งซึ่งจำเป็นต้องสร้างการควบคุมการเข้าถึงและบุคคลหรือผู้ใช้งานที่มีสิทธิในการเข้าถึงนั้น รวมถึงกระบวนการในการบริหารจัดการที่ดีใดๆ เพื่อลดความเสี่ยงซึ่งอาจจะเกิดขึ้นในระหว่างการดำเนินการ

1.1.1) **หลักการควบคุมการเข้าถึง** (Access Control Approach) [12] เป็นหลักการในการกำหนดข้อจำกัดของการเข้าใช้งานระบบ การเข้าถึงข้อมูลหรือการสื่อสารต่างๆ ซึ่งโดยปกติแล้วผู้โจมตีระบบ (Attacker) จะไม่สามารถเข้าถึงแหล่งข้อมูลดังกล่าวและสร้างความเสียหายให้เกิดขึ้นได้ ดังนั้นวัตถุประสงค์หลักก็คือ การป้องกันและหยุดยั้งการโจมตีระบบในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งการเข้าถึงข้อมูลของระบบนั่นเอง โดยกระบวนการของการสร้างการควบคุมการเข้าถึง มีดังนี้

(1) **การแจกแจงทรัพยากร** (Enumeration of Resources) คือการแจกแจงรายละเอียดสำคัญของระบบให้มีความชัดเจน เช่น ฐานข้อมูลบุคคล ข้อมูลสำคัญทางธุรกิจ เป็นต้น

(2) **ความอ่อนไหวของแต่ละทรัพยากร** (Sensitivity of Each Resource) คือการวิเคราะห์ถึงความสำคัญและความอ่อนไหว (Sensitivity) ของแหล่งข้อมูล กล่าวคือ แหล่งข้อมูลใดๆ ซึ่งเมื่อถูกทำลายหรือเกิดความเสียหาย อาจส่งผลกระทบอย่างมากต่อการประกอบการขององค์กร ดังนั้นจึงถือว่าแหล่งข้อมูลนั้นสำคัญและอ่อนไหวสูง

(3) **การกำหนดบทบาทของการเข้าถึง** (Role Determination) คือการกำหนดบทบาทและหน้าที่ (Role) ของการเข้าถึงข้อมูลใดๆ เช่น บางข้อมูล

อาจกำหนดให้ผู้ใช้ทุกคนภายในระบบสามารถเข้าถึงได้ และในบางข้อมูลที่มีความสำคัญมากอาจกำหนดให้ผู้ที่มีหน้าที่เกี่ยวข้องเฉพาะจึงจะสามารถเข้าถึงได้ เป็นต้น

(4) **การกำหนดสิทธิในการเข้าถึง** (Access Permission) คือ การกำหนดสิทธิในการเข้าถึงข้อมูล กล่าวคือเป็นการอนุญาตให้สามารถใช้งานข้อมูลได้ (Authorization) โดยระบุว่าแต่ละกลุ่มหรือแต่ละบุคคลนั้นมีสิทธิในการกระทำกับข้อมูลได้เพียงใด เช่น ผู้ใช้สามารถอ่านข้อมูลได้เพียงอย่างเดียวแต่ไม่มีสิทธิในการแก้ไข ในขณะที่ผู้จัดการระบบมีสิทธิในการเข้าถึงข้อมูลได้ทุกไฟล์ และสามารถกระทำกับข้อมูลได้ทุกอย่าง เป็นต้น

(5) **การจัดสร้างระบบการควบคุมการเข้าถึง** (Access Control Construction) เป็นขั้นตอนสุดท้ายของระบบการควบคุมการเข้าถึง โดยเป็นการตัดสินใจว่า จะกำหนดขอบเขตในการป้องกันการเข้าถึงให้แก่แต่ละแหล่งข้อมูล (Resources) อย่างไร เช่น การกำหนดให้การติดต่อกับเครื่องแม่ข่ายจะต้องผ่านระบบไฟล์วอลล์ เป็นต้น ภายหลังจากการที่มีการตัดสินใจเรียบร้อยแล้ว จะต้องนำไปประกาศไว้สำหรับเป็นข้อกำหนดการป้องกันการเข้าถึง (Access Protection Policy)

1.1.2) **กระบวนการ** (Process) กระบวนการของเรชันแนลหรืออาร์ยูพี (Rational Unified Process: RUP) [13] ถือเป็นวิธีปฏิบัติหนึ่งทางด้านกระบวนการทางวิศวกรรมซอฟต์แวร์ซึ่งเป็นที่ยอมรับกันอย่างแพร่หลายในองค์กร โดยมีรูปแบบของการบริหารจัดการทั้งการกำหนดภารกิจสิ่งที่ต้องกระทำและหน้าที่ความรับผิดชอบของบุคคลภายใต้ภารกิจนั้นๆ ซึ่งองค์กรทั่วไปสามารถที่จะนำไปประยุกต์ใช้ในงานหรือโครงการต่างๆ ขององค์กรได้เป็นอย่างดี และสำหรับในงานวิจัยนี้ก็เช่นกัน ได้นำเอาโครงสร้างกระบวนการเชิงสถิต (Static Structure) ซึ่งเป็นระเบียบวิธีการต่างๆ ที่จะต้องกระทำในแต่ละขั้นตอน และรูปแบบของเอกสารแผ่นแบบมาประยุกต์ใช้ โดยจะทำให้กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ออกแบบนั้นมีการดำเนินการที่ถูกต้อง เป็นไปตามหลักการของกระบวนการที่เป็นสากล

1.2) **งานที่เกี่ยวข้อง** (Related Works) เป็นงานวิจัยที่มีความเกี่ยวข้องกับการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยได้พิจารณาถึงประเด็นสำคัญต่างๆ ของแต่ละงานวิจัย สามารถสรุปได้ดังตารางที่ 3.15

ตารางที่ 3.15 สรุปประเด็นสำคัญของงานวิจัยที่เกี่ยวข้องกับการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	งานวิจัย	ประเด็นสำคัญที่นำมาใช้
1	การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง (Defining Security Requirements Using Grammar of Security Patterns) : งานวิจัยที่ 2.2.1	การวิเคราะห์รายละเอียดโครงสร้างของแบบรูปความมั่นคง และแบบรูปความมั่นคงที่สัมพันธ์กัน รวมถึงไวยากรณ์ความมั่นคงที่ใช้ในการกำหนดความต้องการความมั่นคง ทำให้พิจารณาถึงข้อมูลนำเข้าที่สำคัญ เงื่อนไขและลำดับการทำงานที่เป็นไปได้
2	การศึกษาสถาปัตยกรรมของแบบรูปความมั่นคง (A Study of Security Architectural Patterns) : งานวิจัยที่ 2.2.2	การศึกษาในรายละเอียดหัวข้อย่อยของแต่ละแบบรูปความมั่นคง โดยเฉพาะแบบรูปที่เกี่ยวข้องกับการควบคุมการเข้าถึง ซึ่งจะทำให้เกิดความเข้าใจในบริบทของแต่ละแบบรูปมากยิ่งขึ้น
3	การวิเคราะห์การควบคุมการเข้าถึงในกระบวนการพัฒนาซอฟต์แวร์ (Formal Access Control Analysis in the Software Development Process) : งานวิจัยที่ 2.2.3	แนวคิดของการนำโมเดลความมั่นคงภายใต้การควบคุมการเข้าถึงมาใช้ในการออกแบบและพัฒนาซอฟต์แวร์ ทำให้มองเห็นภาพรวมของวัตถุที่เกิดขึ้น รวมถึงการปฏิสัมพันธ์ระหว่างกันภายใต้ข้อกำหนดของวิธีการดังกล่าว
4	การออกแบบและพัฒนากระบวนการการคัดเลือกผลิตภัณฑ์ซอฟต์แวร์เชิงพาณิชย์ที่ใช้แบบจำลองวุฒิภาวะความสามารถแบบบูรณาการเป็นฐาน (CMMI-Based Process Model Design and Development for COTS Software Product Selection Process) : งานวิจัยที่ 2.2.4	แนวคิดในการออกแบบและพัฒนา กระบวนการโดยจะทำให้ทราบว่าควรปฏิบัติหรือดำเนินการอย่างไรตั้งแต่เริ่มต้นจนถึงสิ้นสุด

2) **สิ่งสำคัญที่เกี่ยวข้องเฉพาะ** (Specific Concerns) ส่วนของข้อมูลนี้จะเป็นส่วนที่มีความเฉพาะในแต่ละองค์กรใดองค์กรหนึ่ง ซึ่งได้ถูกกำหนดขึ้นภายใต้องค์กรนั้น เช่น นโยบายองค์กร (Organization Policy) ข้อบังคับทางธุรกิจ (Business Rule) องค์ความรู้ (Domain Knowledge) เป็นต้น โดยที่การจัดตั้งโครงการหรือการดำเนินการใดๆ จำเป็นที่จะต้องคำนึงถึงข้อมูลข้างต้นเป็นสำคัญ ทั้งนี้เพื่อให้เป็นไปตามเป้าหมายหรือข้อบังคับที่องค์กรนั้นได้กำหนดไว้

และในการจัดตั้งกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศก็เช่นกัน โดยเฉพาะข้อมูลที่เกี่ยวข้องกับความมั่นคงขององค์กร เช่น นโยบายองค์กรด้านความมั่นคง (Organization's Security Policies) ซึ่งถือเป็นตัวที่กำหนดถึงแนวทางปฏิบัติสำคัญของกระบวนการ หรือข้อมูลทั่วไปที่มีความเกี่ยวข้องกับการควบคุมการเข้าถึง (Access Control Domain Information) อย่างเช่น ข้อมูลบันทึกการเข้าใช้งานทรัพยากรขององค์กร เป็นต้น

3.1.4 กำหนดและผสานเชื่อมต่อกิจกรรมและเอกสารที่เกี่ยวข้องกับกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

เมื่อทำการศึกษาและวิเคราะห์ทั้งแบบรูปความมั่นคง มาตราฐาน ISO/IEC 27001:2005 และ 27002:2005 แนวทางปฏิบัติ หลักการและงานวิจัยที่เกี่ยวข้องแล้ว นำสิ่งที่ได้จากการศึกษามากำหนดเป็นกิจกรรมและเอกสารที่เกี่ยวข้องกับกระบวนการ จากนั้นสร้างเป็นกระแสงาน (Workflow) โดยทำการผสานเชื่อมต่อกิจกรรมและเอกสารที่ได้เป็นลำดับก่อน-หลังให้มีความต่อเนื่องและสอดคล้องต้องกัน โดยในแต่ละกิจกรรมที่กำหนดขึ้นนั้นจะต้องนำมาอธิบายเป็นรายละเอียดแยกย่อยขึ้นอีก ทั้งนี้ได้ประยุกต์ใช้การอธิบายพื้นฐานมาจาก SCAMPI [14] ที่ซึ่งแสดงถึงขั้นตอนการทำงานภายใต้กิจกรรม เงื่อนไขก่อนและหลังของการดำเนินกิจกรรม เอกสารนำเข้าเอกสารแผ่นแบบ อาร์ทิแฟกที่เกี่ยวข้อง รวมถึงผู้ที่รับผิดชอบของแต่ละกิจกรรม สำหรับรายละเอียดการอธิบายกิจกรรมนั้นประกอบด้วย 8 องค์ประกอบหลัก ดังแสดงในตารางที่ 3.16

ตารางที่ 3.16 รายละเอียดการอธิบายกิจกรรมทั้ง 8 องค์ประกอบหลัก

ลำดับ	หัวข้อ	คำอธิบาย
1	ชื่อกิจกรรม	บ่งบอกชื่อของกิจกรรม
2	จุดประสงค์ของกิจกรรม	อธิบายถึงการบรรลุผลของกิจกรรม
3	เงื่อนไขก่อนการดำเนินกิจกรรม	อธิบายถึงเงื่อนไขก่อนเริ่มกิจกรรม
4	ส่วนนำเข้า	บ่งบอกถึงเอกสารสนับสนุนและเอกสารแผ่นแบบที่นำมาใช้ในกิจกรรม
5	ขั้นตอนการทำงาน	อธิบายถึงกลุ่มของงานซึ่งเป็นขั้นตอนภายใต้กิจกรรม
6	ส่วนนำออก	บ่งบอกถึงอาร์ทิแฟกผลลัพธ์ที่ได้จากกิจกรรม
7	เงื่อนไขการออกจากกิจกรรม	อธิบายถึงเงื่อนไขหลังจากจบกิจกรรม
8	ผู้รับผิดชอบกิจกรรม	บ่งบอกถึงผู้ที่มีหน้าที่รับผิดชอบกิจกรรม

3.1.5 ทวนสอบและสร้างวัฏจักรการดำเนินการของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภายหลังจากการกำหนดและอธิบายรายละเอียดของกิจกรรมดังกล่าว ให้ทำการทวนสอบการดำเนินการของกระบวนการที่ได้กับสิ่งที่ศึกษามา โดยในที่นี้จะใช้รายการตรวจสอบ (Checklists) ในการทวนสอบว่าถูกต้องและครบถ้วน มีความสอดคล้องเป็นไปตาม โดยเฉพาะแบบรูปความมั่นคง มาตรฐาน ISO/IEC 27001:2005 และ 27002:2005 หรือไม่ ทั้งกิจกรรมที่เกิดขึ้นและเอกสารต่างๆ ที่เกี่ยวข้อง รวมถึงการเรียงลำดับก่อน-หลังของกลุ่มกิจกรมดังกล่าว หากไม่เป็นไปตามให้เพิ่มหรือลดกิจกรรมหรือเอกสารที่เกี่ยวข้องเข้าไปในกระบวนการ

เมื่อทวนสอบเสร็จสิ้นให้ทำการสร้างวัฏจักรของการดำเนินการกระบวนการ และเนื่องจากการดำเนินการกระบวนการนั้นมีแนวทางตามแบบรูปความมั่นคงและมาตรฐานข้างต้น ซึ่งจากการศึกษาวิเคราะห์สามารถแบ่งออกเป็นช่วงของการดำเนินการ กล่าวคือ เป็นการแบ่งลำดับขั้นตอนของกิจกรรมออกเป็นขั้นตอนหลักๆ (Phase) และมีการกำหนดผู้ที่จะต้องรับผิดชอบการดำเนินการนั้น โดยในที่นี้ได้แบ่งออกเป็น 9 ขั้นตอนหลัก ได้แก่ 1) การริเริ่มกระบวนการ (Initiation Phase) 2) การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Risk Determination Phase) 3) การเลือกและกำหนดวิธีการการควบคุมการเข้าถึง (Access Control Selecting and Definition Phase) 4) การกำหนดวิธีการระบุและพิสูจน์ตัวตน (Identification and Authentication Definition Phase) 5) การตรวจสอบข้อกำหนดของกระบวนการ (Verification Phase) 6) การวางแผนปฏิบัติการ (Planning Phase) 7) การพัฒนาระบบและการใช้งาน (Implementation and Operation Phase) 8) การเฝ้าสังเกตและทวนสอบระบบ (Monitoring and Reviewing Phase) และ 9) การปรับปรุงระบบ (Improvement Phase) สำหรับรายละเอียดของแต่ละขั้นตอนได้อธิบายภายใต้แบบจำลองกระบวนการเชิงกระแสงานในบทที่ 4 ต่อไป

3.1.6 ออกแบบเอกสารแผ่นแบบที่เกี่ยวข้องกับกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ขั้นตอนนี้เป็นขั้นตอนสุดท้ายของการวิเคราะห์และออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยเมื่อได้กระบวนการที่มีการสร้างวัฏจักรการดำเนินการเรียบร้อยแล้ว จะเป็นการออกแบบเอกสารแผ่นแบบที่มีความเกี่ยวข้องกับกระบวนการ ทั้งนี้เอกสารแผ่นแบบที่ได้สามารถแบ่งแยกออกเป็นประเภทเอกสาร ฟอร์ม และรายการตรวจสอบ ซึ่งจะเป็นแนวทางให้องค์กรสามารถนำเอากระบวนการไปประยุกต์ใช้ได้อย่างชัดเจนมากยิ่งขึ้น

เอกสารแผ่นแบบดังกล่าวจะสนับสนุนในแต่ละกิจกรรมของการดำเนินการกระบวนการ โดยสามารถแสดงได้ในภาคผนวก ค.

3.2 การพัฒนาเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หลังจากเสร็จสิ้นขั้นตอนการวิเคราะห์และออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศทั้ง 8 ขั้นตอนหลักแล้วนั้น ขั้นตอนต่อไปจะเป็นขั้นตอนของการพัฒนาเครื่องมือสนับสนุนกระบวนการ ซึ่งผู้วิจัยได้ใช้กระบวนการทางวิศวกรรมซอฟต์แวร์ที่เรียกว่าแบบจำลองวอเตอร์ฟอลล์ (Waterfall Model) เข้ามาใช้ในการพัฒนา โดยขั้นตอนจะเริ่มจากการวิเคราะห์ความต้องการของเครื่องมือทั้งเชิงหน้าที่และไม่ใช่หน้าที่ จากนั้นทำการออกแบบหน้าที่การทำงานของเครื่องมือ ฐานข้อมูลเชิงสัมพันธ์ สถาปัตยกรรมเครื่องมือ และส่วนต่อประสานกับผู้ใช้ ผลลัพธ์ที่ได้จากการวิเคราะห์และออกแบบจะถูกนำมาใช้ในการพัฒนาเครื่องมือ เมื่อได้เป็นเครื่องมือสนับสนุนกระบวนการแล้วนั้นจะถูกนำมาทดสอบและประเมินผล ทั้งนี้เพื่อทำให้แน่ใจว่าเครื่องมือดังกล่าวสามารถสนับสนุนกระบวนการได้อย่างถูกต้องและมีประสิทธิภาพ สำหรับขั้นตอนของการพัฒนาเครื่องมือสามารถแสดงได้ดังรูปที่ 3.3 และผลของการวิเคราะห์และออกแบบเครื่องมือดังกล่าวจะนำเสนอในบทที่ 5 และ 6 ถัดไป

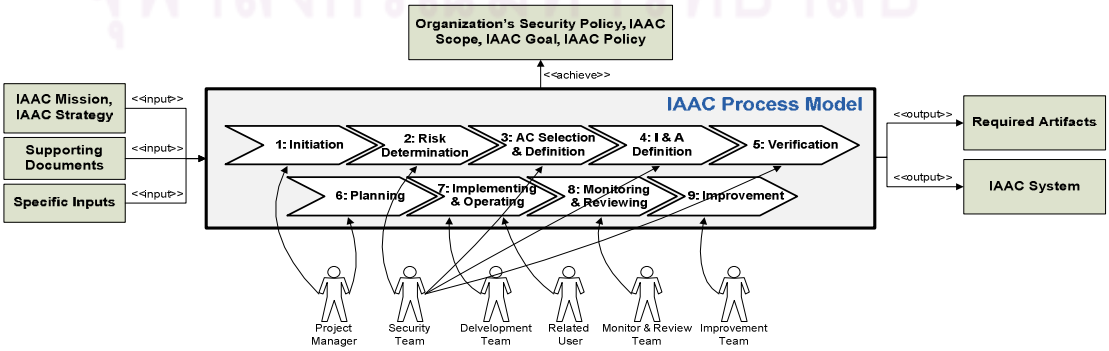
รูปที่ 3.3 ขั้นตอนการพัฒนาเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

บทที่ 4
กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

บทนี้จะเป็นการนำเสนอกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยเป็นผลจากการวิเคราะห์และออกแบบกระบวนการในขั้นตอนที่หนึ่ง ซึ่งมีรายละเอียดของขั้นตอนที่กล่าวมาแล้วในบทที่ 3 กระบวนการที่ได้มานั้นสามารถอธิบายรายละเอียดโดยใช้ชั้นของแบบจำลอง ซึ่งมีมุมมองเริ่มจากภาพรวมของกระบวนการที่ซึ่งอธิบายถึงส่วนนำเข้าและส่วนนำออกที่จำเป็นต่อการดำเนินการของกระบวนการ รวมถึงบทบาทและหน้าที่ของผู้ที่เกี่ยวข้องตลอดจนลำดับขั้นตอนและรายละเอียดของกิจกรรมที่เกิดขึ้น แบบจำลองของกระบวนการดังกล่าวสามารถแบ่งออกเป็น 3 ชั้นหลัก ได้แก่ ชั้นแบบจำลองกระบวนการเชิงภาพรวม ชั้นแบบจำลองกระบวนการเชิงกระแสงาน และชั้นแบบจำลองกระบวนการเชิงนิยาม ดังแสดงไว้ในรูปที่ 3.1 นอกจากนี้ยังนำเสนอการประเมินกระบวนการ โดยเป็นการเปรียบเทียบกับความต้องการของสิ่งที่ได้ศึกษามา ทั้งนี้เพื่อเป็นการทวนสอบกระบวนการว่ามีการดำเนินการสอดคล้องและเป็นไปตามหรือไม่

4.1 ชั้นแบบจำลองกระบวนการเชิงภาพรวม (Overview Process Model Layer)

แบบจำลองกระบวนการเชิงภาพรวมนั้นได้อธิบายถึงองค์ประกอบพื้นฐานของการดำเนินการกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งจะทำให้องค์กรที่นำไปประยุกต์ใช้มองเห็นภาพรวมและเข้าใจถึงสภาวะแวดล้อมของกระบวนการได้อย่างชัดเจนมากยิ่งขึ้น โดยโครงสร้างของแบบจำลองนี้ประกอบด้วยองค์ประกอบหลัก 4 องค์ประกอบ ได้แก่ 1) เป้าหมายและนโยบายหลักที่การดำเนินการกระบวนการจะต้องบรรลุถึง 2) ส่วนนำเข้าและออกของกระบวนการ 3) กระบวนการที่เกิดขึ้นซึ่งแบ่งออกเป็น 9 ขั้นตอนหลัก รวมถึง 4) บทบาทและหน้าที่รับผิดชอบของผู้ที่มีส่วนเกี่ยวข้อง โดยแบบจำลองนี้สามารถแสดงได้ดังรูปที่ 4.1



รูปที่ 4.1 ชั้นแบบจำลองเชิงภาพรวมของกระบวนการการควบคุมการเข้าถึงสินทรัพย์สารสนเทศ

จากรูปที่ 4.1 อธิบายรายละเอียดขององค์ประกอบหลักทั้ง 4 องค์ประกอบ ได้ดังต่อไปนี้

1) **เป้าหมายและนโยบายหลักที่จะต้องบรรลุถึง** (Goal and Policy) การดำเนินการกระบวนการใดๆ จำเป็นที่จะต้องให้บรรลุถึงเป้าหมายที่กำหนดไว้ตั้งแต่แรกเริ่ม และต้องเป็นไปตามนโยบายที่ได้ตั้งไว้ ทั้งนี้เพื่อแสดงว่ากระบวนการนั้นสามารถดำเนินการได้อย่างสัมฤทธิ์ผล สำหรับกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนี้ก็เช่นกัน สิ่งที่จะต้องบรรลุถึง ได้แก่ นโยบายองค์กรด้านความมั่นคง (Organization's Security Policy) ขอบเขตและเป้าหมายที่ได้กำหนดไว้ รวมถึงนโยบายของกระบวนการ

2) **ส่วนนำเข้าและออกของกระบวนการ** (Inputs and Outputs)

2.1) **ส่วนนำเข้า** เป็นสิ่งสำคัญในการขับเคลื่อนกระบวนการให้สามารถดำเนินการได้ โดยในที่นี้ประกอบไปด้วย 3 ส่วนหลัก ดังนี้

2.1.1) **พันธกิจและกลยุทธ์ของกระบวนการ** (IAAC Mission and Strategy) เป็นการกำหนดถึงงานหรือแนวทางที่จะปฏิบัติตามของการดำเนินการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร ทั้งนี้เพื่อให้การดำเนินการนั้นสามารถสำเร็จลุล่วงไปได้

2.1.2) **เอกสารสนับสนุน** (Supporting Documents) ประกอบด้วยเอกสารสำคัญทั้ง 4 ประเภท ดังนี้

(1) **เอกสารที่เกี่ยวข้อง** (Related Documents) เป็นเอกสารขององค์กรที่เกี่ยวข้องกับการสร้างความมั่นคงให้กับสินทรัพย์ของตน โดยเฉพาะสินทรัพย์ประเภทสารสนเทศ ทั้งนี้เอกสารดังกล่าวอาจถูกกำหนดขึ้นตั้งแต่แรกเริ่มของการจัดตั้งองค์กร เช่น เอกสารนโยบายองค์กรด้านความมั่นคง เป็นต้น

(2) **เอกสารแผ่นแบบของกระบวนการ** (IAAC Template Documents) เป็นเอกสารแผ่นแบบที่ได้ทำการออกแบบไว้เพื่อสนับสนุนกระบวนการ โดยภายในจะระบุหัวข้อสำคัญต่างๆ ที่จำเป็นต้องคำนึงถึง ซึ่งจะช่วยให้องค์กรมีแนวทางในการประยุกต์ใช้ได้อย่างชัดเจนมากยิ่งขึ้น เช่น แผ่นแบบนโยบายกระบวนการ แผ่นแบบแผนการเฝ้าสังเกตและทวนสอบระบบ เป็นต้น

(3) **ฟอร์ม** (Forms) เป็นเอกสารแผ่นแบบในลักษณะของแบบฟอร์มที่นำมาใช้เพื่อเก็บข้อมูลสำคัญของกระบวนการ ทั้งนี้ข้อมูลดังกล่าวจะถูกนำมาศึกษาวิเคราะห์เพื่อใช้เป็นข้อมูลนำเข้าสำคัญสำหรับใช้ดำเนินการกระบวนการต่อไป เช่น ฟอร์มรายการคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ ฟอร์มรายการกระทำสำหรับการปรับปรุงระบบ เป็นต้น

(4) **รายการตรวจสอบ** (Checklists) เป็นเอกสารแผ่นแบบในลักษณะรายการตรวจสอบ โดยระบุถึงข้อกำหนดหรืองานใดๆ ที่ต้องมีหรือกระทำภายใต้กิจกรรมนั้นๆ เพื่อให้ผู้ดำเนินการสามารถตรวจสอบกิจกรรมได้ว่า ได้กระทำครบถ้วนตามที่ระบุหรือไม่ เช่น รายการตรวจสอบข้อกำหนดของกระบวนการ รายการตรวจสอบความครบถ้วนของการพัฒนาระบบ เป็นต้น

2.1.3) **ส่วนนำเข้าเฉพาะ** (Specific Inputs) คือ ข้อมูลนำเข้าสำคัญต่างๆ ของกระบวนการที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ เช่น ข้อมูลบทบาทของผู้ใช้ภายในองค์กร ข้อมูลการจัดแบ่งระดับของสินทรัพย์ประเภทสารสนเทศ เป็นต้น ทั้งนี้ข้อมูลดังกล่าวต้องอยู่ภายใต้สภาวะแวดล้อมขององค์กรเป็นสำคัญ

2.2) **ส่วนนำออก** (Outputs) เป็นสิ่งที่ได้ภายหลังจากการดำเนินการกระบวนการเสร็จสิ้น ซึ่งได้แบ่งออกเป็น 2 ส่วนหลัก ดังนี้

2.2.1) **อาร์ทิแฟกที่จำเป็น** (Required Artifacts) โดยหมายรวมถึงเอกสารข้อกำหนดต่างๆ แผนงาน บันทึกผลหรือรายงานสรุป เป็นต้น ทั้งนี้เอกสารดังกล่าวอาจมีรูปแบบที่เป็นไปตามเอกสารแผ่นแบบที่ได้ออกแบบมาสำหรับสนับสนุนกระบวนการนี้

2.2.2) **ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ** (IAAC System) เป็นระบบที่พัฒนาขึ้นสำหรับใช้ในการควบคุมการเข้าถึงและเข้าใช้งานสินทรัพย์ประเภทสารสนเทศขององค์กร โดยอาจเป็นการพิจารณาจากสิทธิของผู้ใช้งานหรืออาจเป็นการพิจารณาจากบทบาท ทั้งนี้จะเป็นไปตามความเหมาะสมของแต่ละองค์กร

3) **กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ** (IAAC process model) เป็นกระบวนการที่มุ่งเน้นเกี่ยวกับการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศขององค์กร โดยวิธีการควบคุมการเข้าถึง ซึ่งในการดำเนินการกระบวนการนั้นจะเป็นไปตาม 9 ขั้นตอนหลักดังแสดงในรูปที่ 4.1 โดยเริ่มจากการจัดตั้งกระบวนการซึ่งจะต้องทำการกำหนดขอบเขตและเป้าหมาย รวมถึงการจัดตั้งนโยบาย เรื่อยไปจนถึงการประเมินและสรุปผลการปรับปรุงกระบวนการ ทั้งนี้เพื่อให้กระบวนการดังกล่าวมีประสิทธิภาพในการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ สำหรับรายละเอียดของแต่ละขั้นตอนสามารถอธิบายได้ในหัวข้อที่ 4.2 ต่อไป

4) **บทบาทและหน้าที่รับผิดชอบของผู้ที่เกี่ยวข้อง** (Role and Responsibility) เพื่อให้กระบวนการสามารถดำเนินการได้ จำเป็นที่จะต้องมีผู้ที่เกี่ยวข้องเข้ามารับผิดชอบในแต่ละขั้นตอนของการดำเนินการ โดยบทบาทและหน้าที่สามารถแบ่งแยกออกเป็น 5 กลุ่มบุคคล ดังนี้

4.1) **ผู้จัดการโครงการ** (Project Manager) มีหน้าที่โดยตรงในการกำหนดขอบเขตและเป้าหมายของกระบวนการ จัดตั้งนโยบายและกลยุทธ์การดำเนินการ ทวนสอบข้อกำหนดของกระบวนการโดยเปรียบกับนโยบายและกลยุทธ์ รวมถึงการวางแผนการปฏิบัติการต่างๆ ซึ่งในการกำหนดนั้นจะบ่งบอกถึงทิศทางโดยรวมของการดำเนินการกระบวนการ ดังนั้นผู้จัดการโครงการจึงจำเป็นต้องเป็นผู้ที่มีความเชี่ยวชาญด้านความมั่นคงอย่างสูง

4.2) **ทีมความมั่นคง** (Security Team) มีหน้าที่ในการกำหนดข้อมูลนำเข้าสำคัญต่างๆ เข้าสู่กระบวนการ ทั้งในขั้นตอนการระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ การกำหนดวิธีการควบคุมการเข้าถึง และการกำหนดวิธีการระบุและพิสูจน์ตัวตน หน้าที่ในการตรวจสอบสิ่งที่ได้จากการกำหนดดังกล่าว ทั้งนี้เพื่อให้การสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศนั้นมีความถูกต้อง รวมถึงหน้าที่ในการฝึกอบรมทีมปฏิบัติการให้รับทราบถึงข้อกำหนดต่างๆ ที่ตรงกัน โดยจะทำให้การดำเนินกระบวนการนั้นสำเร็จลุล่วงไปได้ด้วยดี

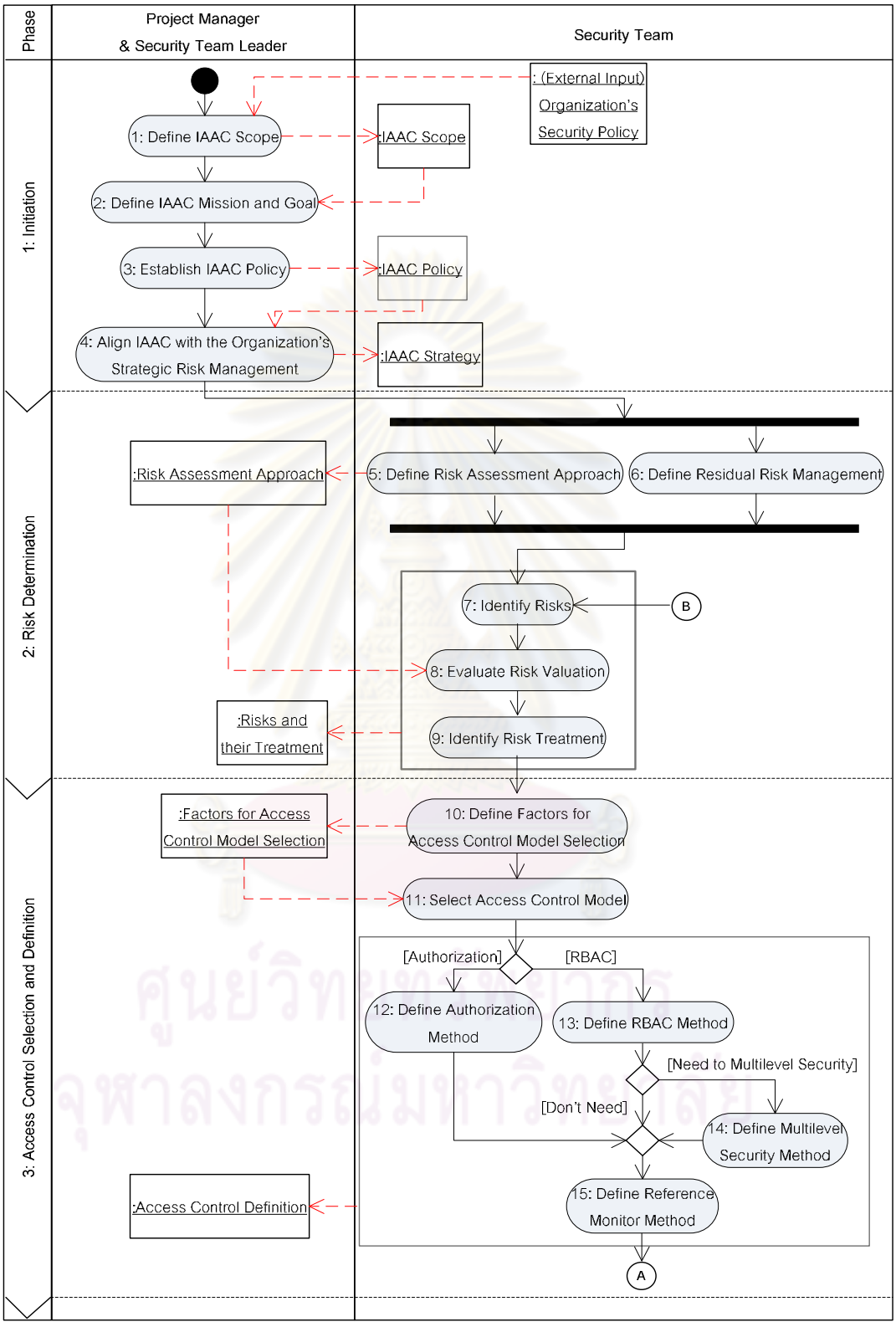
4.3) **ทีมการพัฒนาและผู้ใช้งานที่เกี่ยวข้อง** (Delvelopment Team and Related User) มีหน้าที่ในการพัฒนาระบบที่ซึ่งควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร รวมถึงหน้าที่ในการฝึกอบรมผู้ใช้งานให้สามารถใช้งานระบบที่พัฒนาขึ้นให้เป็นไปตามทิศทางที่ถูกต้องและอยู่ในขอบเขตของสิทธิของแต่ละบุคคลที่สามารถเข้าถึงได้

4.4) **ทีมการเฝ้าสังเกตและทวนสอบ** (Monitoring and Reviewing Team) มีหน้าที่ในการเฝ้าสังเกตการณ์และทวนสอบระบบที่พัฒนาขึ้นในด้านของประสิทธิภาพเมื่อผ่านการใช้งานจากผู้ใช้ในช่วงระยะเวลาหนึ่ง นอกจากนี้ยังรวมถึงการปรับปรุงแผนการเฝ้าสังเกตและทวนสอบระบบให้มีข้อมูลที่สามารถนำมาใช้ในการเฝ้าสังเกตและทวนสอบระบบในครั้งถัดไปได้

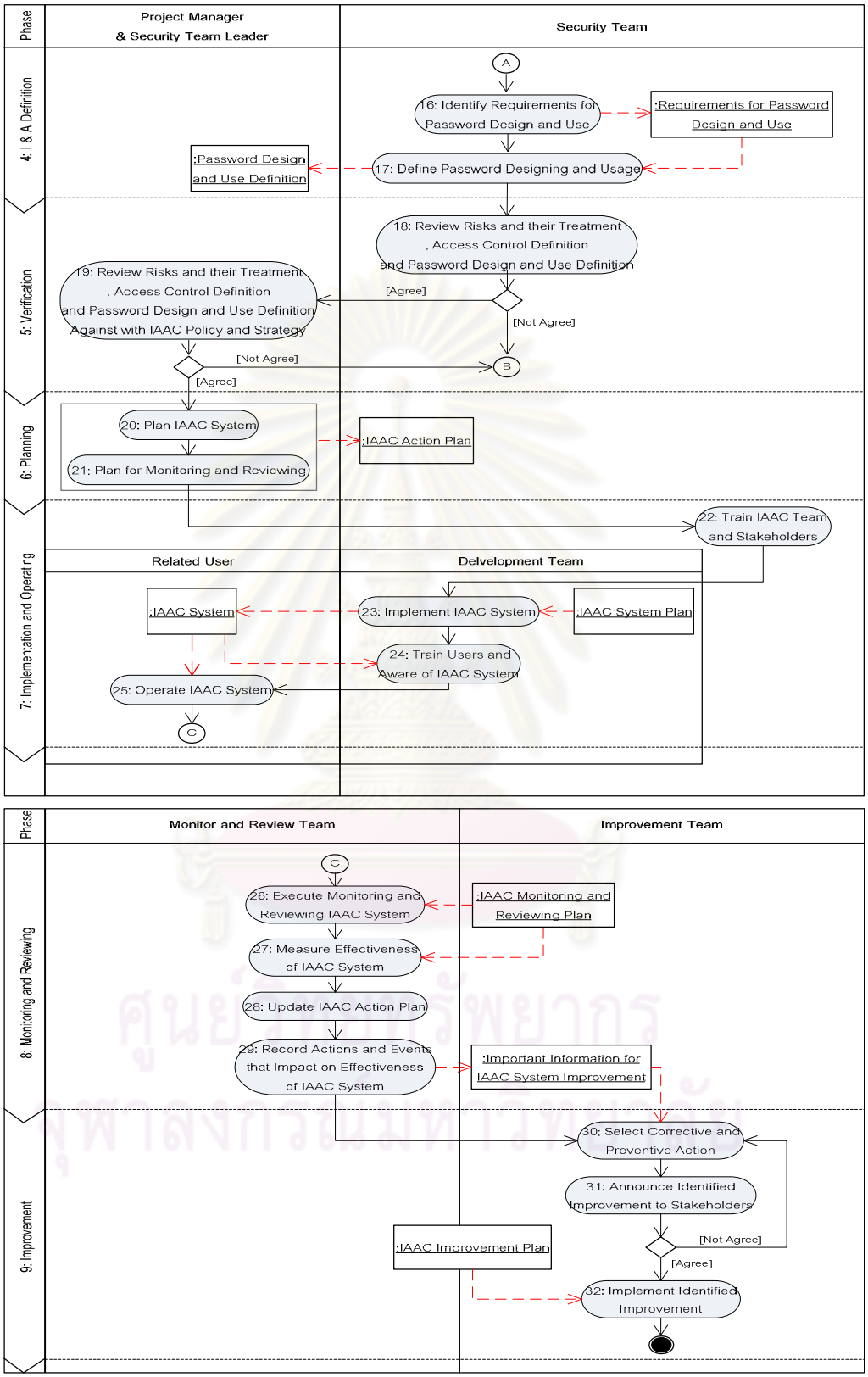
4.5) **ทีมการปรับปรุง** (Improvement Team) มีหน้าที่ในการปรับปรุงระบบให้มีประสิทธิภาพเพิ่มมากขึ้นภายหลังจากการเฝ้าสังเกตและทวนสอบ รวมถึงดำเนินการประกาศการกระทำของการปรับปรุงให้กับผู้ที่เกี่ยวข้องกับกระบวนการได้รับทราบและมีความเข้าใจตรงกัน

4.2 ชั้นแบบจำลองกระบวนการเชิงกระแสงาน (Workflow Process Model Layer)

ชั้นแบบจำลองนี้ได้อธิบายถึงลำดับขั้นตอนของกิจกรรมภายใต้การดำเนินการกระบวนการ นอกจากนี้ยังอธิบายถึงส่วนนำเข้าและออกเพื่อใช้ขับเคลื่อนการดำเนินกิจกรรมนั้นๆ สำหรับส่วนนำออกของกิจกรรมใดๆ อาจกลายเป็นส่วนนำเข้าสำคัญของอีกกิจกรรมหนึ่ง แบบจำลองกระบวนการเชิงกระแสงานแบ่งได้เป็น 9 ขั้นตอนหลัก ซึ่งนำเสนอด้วยแผนภาพกิจกรรมของยูเอ็มแอลดังรูปที่ 4.2



รูปที่ 4.2 ชั้นแบบจำลองเชิงกระแสงานของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ



รูปที่ 4.2 ชั้นแบบจำลองเชิงกระแสงานของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

จากรูปที่ 5.2 สามารถอธิบายรายละเอียดของขั้นตอนหลักทั้ง 9 ขั้นตอน ได้ดังต่อไปนี้

1) **การริเริ่มกระบวนการ** (Initiation Phase) ขั้นตอนแรกควรเริ่มตั้งแต่การกำหนดขอบเขตและเป้าหมายของกระบวนการ รวมถึงการกำหนดนโยบายและกลยุทธ์การดำเนินการ ทั้งนี้เพื่อใช้เป็นแนวทางหรือจุดมุ่งหมายสำหรับการกำหนดการดำเนินการที่จะเกิดขึ้น ดังนั้นขั้นตอนนี้จึงถือเป็นขั้นตอนที่สำคัญที่สุด โดยในการจัดตั้งในที่นี้สิ่งที่นำมาพิจารณาเป็นสำคัญ คือ นโยบายองค์กรด้านความมั่นคง

2) **การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ** (Risk Determination Phase) ขั้นตอนนี้เป็นขั้นตอนการระบุความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศภายในองค์กร ซึ่งก่อนการระบุนั้นจะต้องกำหนดกลยุทธ์ของการประเมินความเสี่ยง (Risk Assessment Approach) เพื่อใช้กำหนดวิธีการประเมินและระดับของความเสี่ยง นอกจากนี้ยังรวมถึงการกำหนดการจัดการความเสี่ยงที่คงเหลือ (Residual Risk Management) เพื่อใช้จัดการกับความเสี่ยงที่อาจเกิดขึ้นในภายหลัง การวิเคราะห์และประเมินค่าความเสี่ยงของสินทรัพย์นั้นจะทำให้ทราบถึงแนวทางในการกำหนดวิธีการป้องกันความเสี่ยง กล่าวคือวิธิการควบคุมการเข้าถึงและการระบุและพิสูจน์ตัวตนในขั้นตอนต่อไป

3) **การเลือกและกำหนดวิธีการการควบคุมการเข้าถึง** (Access Control Selecting and Definition Phase) รายละเอียดความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศจากขั้นตอนก่อนหน้า ทำให้สามารถนำมาใช้เป็นแนวทางในการเลือกและกำหนดวิธีการของการควบคุมการเข้าถึงที่เหมาะสม ทั้งการให้อำนาจ (Authorization) การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control) ความมั่นคงหลายระดับ (Multilevel Security) และการตรวจสอบการเข้าถึง (Reference Monitor) ทั้งนี้ควรคำนึงถึงสภาวะแวดล้อมขององค์กรด้วย อย่างเช่น จำนวนผู้ใช้งาน บทบาทที่มีภายในองค์กร หรือการแบ่งแยกประเภทของสินทรัพย์ประเภทสารสนเทศ เป็นต้น การกำหนดปัจจัยสำหรับพิจารณาเลือกใช้โมเดลนั้น ถือเป็นขั้นตอนสำคัญที่จะช่วยให้การเลือกมีความถูกต้องและเหมาะสมกับองค์กรมากที่สุด

4) **การกำหนดวิธีการระบุและพิสูจน์ตัวตน** (Identification and Authentication Definition Phase) วิธีการระบุและพิสูจน์ตัวตนในที่นี้จะมุ่งเน้นไปที่การออกแบบและใช้งานรหัสผ่าน (Password Design and Use) ซึ่งเป็นเทคนิคที่ได้รับความนิยมอย่างแพร่หลาย อีกทั้งยังง่ายต่อการใช้งานของผู้ใช้ โดยขั้นตอนนี้จะมีการกำหนดความต้องการเพื่อใช้เป็นแนวทางในการออกแบบและกำหนดการใช้งานรหัสผ่าน

5) **การตรวจสอบข้อกำหนดของกระบวนการ** (Verification Phase) ขั้นตอนนี้เป็นขั้นตอนของการตรวจสอบความถูกต้องของการระบุความเสี่ยง วิธีการควบคุมการเข้าถึงและ

วิธีการออกแบบและใช้งานรหัสผ่าน โดยดูว่าเป็นไปตามสิทธิการเข้าถึงและเข้าใช้งานสินทรัพย์ของผู้ใช้หรือไม่ และเป็นไปตามนโยบายและกลยุทธ์ที่กำหนดไว้ตั้งแต่แรกเริ่มของโครงการหรือไม่

6) **การวางแผนปฏิบัติการ** (Planning Phase) ทำการวางแผนการปฏิบัติการต่างๆ ของกระบวนการ ทั้งแผนการพัฒนาระบบ แผนการสังเกตการณ์และทวนสอบระบบ และแผนการประเมินและปรับปรุงระบบ ทั้งนี้เพื่อให้ทราบถึงกำหนดการที่แน่ชัด โดยรวมถึงระยะเวลาที่ใช้ ทีมปฏิบัติการที่จะต้องมารับผิดชอบ งบประมาณและทรัพยากรที่จำเป็นต้องใช้

7) **การพัฒนาระบบและการใช้งาน** (Implementation and Operation Phase) ขั้นตอนนี้เป็นขั้นตอนของการพัฒนาระบบเพื่อใช้ควบคุมการเข้าถึงและเข้าใช้งานสินทรัพย์ประเภทสารสนเทศของผู้ใช้ ซึ่งจะต้องพัฒนาให้เป็นไปตามแผนการพัฒนาระบบที่ได้กำหนดไว้ โดยก่อนการพัฒนาจะต้องทำการอบรมทีมปฏิบัติการที่เกี่ยวข้องให้เข้าใจถึงข้อกำหนดต่างๆ ที่ได้กำหนดไว้แต่เริ่มแรก ทั้งนี้เพื่อให้เกิดความเข้าใจที่ถูกต้องและตรงกัน ในส่วนของการใช้งานระบบจำเป็นต้องมีการอบรมการใช้งานให้กับผู้ใช้ เพื่อให้สามารถใช้งานระบบได้อย่างถูกต้องและเป็นประโยชน์มากที่สุด

8) **การเฝ้าสังเกตและทวนสอบระบบ** (Monitoring and Reviewing Phase) ขั้นตอนนี้จะต้องทำการเฝ้าสังเกตและทวนสอบระบบภายหลังจากที่มีการใช้งานมาในช่วงระยะเวลาหนึ่ง ซึ่งกำหนดการและการปฏิบัติจะเป็นไปตามแผนการสังเกตการณ์และทวนสอบระบบที่ได้กำหนดไว้ โดยในที่นี้จะรวมถึงการวัดประสิทธิภาพของระบบ ข้อมูลที่ได้จากขั้นตอนนี้จะถูกบันทึกไว้เพื่อบ่งชี้ถึงการปรับปรุงระบบต่อไป

9) **การปรับปรุงระบบ** (Improvement Phase) ข้อมูลสำคัญทั้งการกระทำและเหตุการณ์ที่กระทบต่อประสิทธิภาพของระบบจากขั้นตอนก่อนหน้า จะถูกนำมาวิเคราะห์เพื่อหาทางแก้ไขและปรับปรุง ซึ่งก่อนทำการปรับปรุงนั้นจะต้องแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบ ทั้งนี้เพื่อขอความเห็นจึงจะสามารถกำหนดเป็นการปรับปรุงระบบที่เหมาะสมต่อไป

4.3 **ชั้นแบบจำลองกระบวนการเชิงนิยาม** (Definition Process Model Layer)

รายละเอียดของแต่ละกิจกรรมที่เกิดขึ้นภายใต้การดำเนินการกระบวนการได้ถูกอธิบายในแบบจำลองเชิงนิยามนี้ ซึ่งถือว่าเป็นการนิยามพื้นฐานที่จะช่วยให้องค์กรเกิดความเข้าใจได้อย่างเป็นรูปธรรม ซึ่งเป็นประโยชน์อย่างมากต่อการนำไปประยุกต์ใช้ อีกทั้งยังช่วยลดเวลาในการจัดเตรียมการประเมินผลของแต่ละกิจกรรม เนื่องจากว่ามีการกำหนดตัวบ่งชี้อย่างชัดเจนนั่นเอง โดยองค์ประกอบของการอธิบายประกอบด้วย 8 องค์ประกอบหลักที่ได้กำหนดไว้ในบทที่ 3 หัวข้อที่

3.1.4 สำหรับรายละเอียดของการอธิบายกิจกรรมของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศสามารถแสดงได้ดังภาคผนวก ข.

4.4 การประเมินกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Process Model Evaluation)

ภายหลังที่ได้แบบจำลองซึ่งอธิบายรายละเอียดของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ แบบจำลองดังกล่าวจะต้องถูกนำมาประเมินผลเพื่อเปรียบเทียบกับรายละเอียดของสิ่งที่ได้ศึกษามา โดยเฉพาะแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้อง โดยในที่นี้จะประยุกต์ใช้วิธีการทวนสอบแบบตรวจตลอด (Walkthroughs Verification) ซึ่งได้ใช้รายการตรวจสอบ (Checklists) เป็นเครื่องมือในการทวนสอบถึงความถูกต้องและความครบถ้วนของทั้งวิธีปฏิบัติหลักและข้อปฏิบัติย่อยที่เกิดขึ้นภายใต้การดำเนินการกระบวนการ ทั้งนี้การทวนสอบในระดับข้อปฏิบัติย่อยนั้นจะทำให้แน่ใจว่า ทั้งกิจกรรมการทำงานและสิ่งที่ได้มานั้นเป็นไปตามการวิเคราะห์รายละเอียดของสิ่งที่ได้ศึกษามาหรือไม่ ผลของการประเมินซึ่งนำเสนอความสอดคล้องกันระหว่างกระบวนการกับแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้องนั้นสามารถแสดงได้ดังตารางที่ 4.1 และการอธิบายสัญลักษณ์ภายใต้ตารางที่ 4.1 สามารถแสดงได้ดังตารางที่ 4.2

ตารางที่ 4.1 เปรียบเทียบการดำเนินการของกระบวนการกับรายละเอียดของแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้อง

Information Assets Access Control Process	Security Patterns	ISO/IEC 27001:2005	ISO/IEC 27002:2005
Phase I: Initiation	☒	☑	☑
1. Define IAAC Scope	SP	Establish the ISMS a), b) & Management Commitment a) - d)	Security Policy & Organization of Information Security & Access Control (11.1)
2. Define IAAC Mission & Goal			
3. Establish IAAC Policy			
4. Align with the Organization's Strategic Risk Management			
Phase II: Risk Determination	☑	☑	☑
1. Define Risk Assessment Approach	SP	Establish the ISMS c), h)	Risk Assessment and Treatment & Asset Management
2. Define Residual Risk Management			
3. Identify Risks	Enterprise Security and Risk Management (6.1 - 6.7)	Establish the ISMS d) - g), j) & Management Commitment f)	
4. Evaluate Risk Valuation			
5. Identify Risk Treatment			
Phase III: Access Control Selection & Definition	☑	☒	☑
1. Identify Factors for Access Control Model Selection	Access Control Model	27001	Access Control (11.1, 11.2)
2. Select & Define Access Control Model			
Phase IV: I & A Definition	☑	☒	☑
1. Identify Requirements for Password Designing and Usage	Identification and Authentication (7.1 - 7.3)	27001	Access Control (11.2, 11.3)
2. Define Password Designing And Usage			

ตารางที่ 4.1 เปรียบเทียบการดำเนินการของกระบวนการกับรายละเอียดของแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้อง (ต่อ)

Information Assets Access Control Process	Security Patterns	ISO/IEC 27001:2005		ISO/IEC 27002:2005
Phase V: Verification	☒	☑		☒
1. Review All Definition	SP	Documentation Requirements (General & Control of Doc.)		27002(1)
2. Review All Definition Against with IAAC and Strategy				
Phase VI: Planning	☒	☑		☑
1. Plan for IAAC System Development	SP	Resource Management (Provision of Resource)	Implement and Operate the ISMS a)	System Planning and Acceptance
2. Plan for Monitoring and Reviewing			Management Commitment g), h)	Information Security Incident Management
Phase VII: Implementing & Operating	☒	☑		☑
1. Train IAAC Team and Stakeholders	SP	Resource Management (Training, awareness and Competence)		Human Resource Security (8.1, 8.2)
2. Implement IAAC System		Implement and Operate the ISMS b), c)		Information Systems Acquisition, Development and Management (12.1, 12.2)
3. Train Users and Aware of IAAC System		Resource Management (Training, awareness and Competence)		Human Resource Security (8.1, 8.2)
4. Operate IAAC System		Implement and Operate the ISMS f)		27002(2)

ตารางที่ 4.1 เปรียบเทียบการดำเนินการของกระบวนการกับรายละเอียดของแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้อง (ต่อ)

Information Assets Access Control Process	Security Patterns	ISO/IEC 27001:2005	ISO/IEC 27002:2005
Phase VIII: Monitoring & Reviewing	☒	☑	☑
1. Execute Monitoring and Reviewing IAAC System	SP	Monitor and Review the ISMS & Internal ISMS Audits & Management Review of the ISMS	Information Security Incident Management
2. Measure Effectiveness of IAAC System			
3. Update Monitoring and Reviewing Plan			
4. Record Actions and Events that Impact on Effectiveness of IAAC System			
Phase IX: Improvement	☒	☑	☑
1. Define Corrective and Preventive Action	SP	Maintain and Improve the ISMS & ISMS Improvement	Business Continuity Management
2. Announce Identified Improvement to Stakeholders			
3. Implement Identified Improvement			

ตารางที่ 4.2 การอธิบายสัญลักษณ์ภายใต้การเปรียบเทียบการดำเนินการของกระบวนการกับรายละเอียดของแบบรูปความมั่นคงและมาตรฐานที่เกี่ยวข้องดังตารางที่ 4.1

สัญลักษณ์	คำอธิบาย
☑	กิจกรรมของขั้นตอนหลัก (Phase) มีแนวทางตามแบบรูปความมั่นคงและ/หรือมาตรฐานที่เกี่ยวข้อง
☒	กิจกรรมของขั้นตอนหลักไม่ได้มีแนวทางตามแบบรูปความมั่นคงและ/หรือมาตรฐานที่เกี่ยวข้อง
SP	เนื่องจากแบบรูปความมั่นคง [3] ที่นำมาใช้ในงานวิจัยนี้ เป็นการอธิบายถึงผลเฉลยของเทคนิคและวิธีการทางด้านความมั่นคงโดยเฉพาะ โดยมีกลุ่มแบบรูปที่เกี่ยวข้องทั้งหมด 3 กลุ่มแบบรูป คือ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management) โมเดลการควบคุมการเข้าถึง (Access Control Models) การระบุและพิสูจน์ตัวตน (Identification and Authentication) และเพื่อให้กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศมีการดำเนินการเป็นไปอย่างมีประสิทธิภาพ จำเป็นต้องผนวกรวมทั้งการจัดตั้งกระบวนการ (Initiation Phase) การวางแผนปฏิบัติการ (Planning Phase) การพัฒนาและดำเนินการใช้งานระบบ (Implementing & Operating Phase) การเฝ้าสังเกตและทวนสอบระบบ (Monitoring & Reviewing Phase) การปรับปรุงระบบ (Improvement Phase) เข้ากับวิธีการทางด้านความมั่นคงดังกล่าว ทั้งนี้ขั้นตอนข้างต้นยังยึดตามแนวทางของข้อกำหนดและข้อปฏิบัติภายใต้มาตรฐาน ISO/IEC 27001:2005 และ 27002:2005 ซึ่งมีแนวคิดของโมเดล PDCA โดยถือเป็นโมเดลระบบการบริหารที่เป็นสากล
27001	วิธีการการควบคุมการเข้าถึง (Access Control Definition Phase) และวิธีการระบุและพิสูจน์ตัวตน (Identification & Authentication Definition Phase) ถือเป็นข้อปฏิบัติที่อธิบายไว้ภายใต้แบบรูปความมั่นคงและมาตรฐาน ISO/IEC 27002:2005 ซึ่งไม่ได้มีการอธิบายไว้เป็นข้อกำหนดภายใต้มาตรฐาน ISO/IEC 27001:2005 อย่างชัดเจน อย่างไรก็ตาม ข้อกำหนดที่เกี่ยวข้องกับข้อปฏิบัติดังกล่าว ได้อธิบายเป็นการระบุการป้องกันรักษาความเสี่ยง หัวข้อ Establish the ISMS g)
27002(1)	การทวนสอบข้อกำหนดของกระบวนการ (Verification Phase) เป็นการจัดการเอกสารที่เกิดขึ้นภายใต้การดำเนินการกระบวนการ ซึ่งไม่ได้อธิบายเป็นข้อปฏิบัติของมาตรฐาน ISO/IEC 27002:2005 แต่มีการอธิบายไว้ในข้อกำหนดของมาตรฐาน ISO/IEC 27001:2005 หัวข้อ Documentation Requirements
27002(2)	กิจกรรมการดำเนินการใช้งานระบบควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Operate IAAC System) ภายใต้การพัฒนาและดำเนินการใช้งานระบบ (Implementing & Operating Phase) เป็นการดำเนินการใช้งานระบบของผู้ใช้งานทั่วไป ซึ่งถือเป็นกิจกรรมที่นอกเหนือข้อปฏิบัติของมาตรฐาน ISO/IEC 27002:2005 แต่มีการอธิบายไว้ในข้อกำหนดของมาตรฐาน ISO/IEC 27001:2005 หัวข้อ Implement and Operate the ISMS f)

บทที่ 5
การวิเคราะห์และออกแบบเครื่องมือสนับสนุนกระบวนการ

ภายหลังจากที่ได้วิเคราะห์และออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศแล้วนั้น ขั้นตอนต่อไป คือ การวิเคราะห์และออกแบบหน้าที่การทำงานของเครื่องมือสนับสนุนกระบวนการดังกล่าว โดยมีรายละเอียดของกระบวนการเป็นส่วนนำเข้าของขั้นตอนนี้ สิ่งที่ได้จากการวิเคราะห์และออกแบบเครื่องมือสนับสนุน ได้แก่ ความต้องการของเครื่องมือเชิงหน้าที่และไม่ใช่หน้าที่ หน้าที่การทำงานของเครื่องมือ ฐานข้อมูลเชิงสัมพันธ์ สถาปัตยกรรมระบบ และส่วนต่อประสานกับผู้ใช้ ซึ่งสิ่งเหล่านี้จะถูกนำมาประกอบรวมกันเพื่อใช้ในการพัฒนาเครื่องมือสนับสนุนต่อไป

เครื่องมือสนับสนุนกระบวนการนั้นได้ช่วยให้ผู้ที่เกี่ยวข้องสามารถจัดการ เฝ้าสังเกต และควบคุมกระบวนการได้ ตั้งแต่ขั้นตอนการจัดตั้งโครงการ เรื่อยไปจนถึงการดูแลและปรับปรุงระบบที่พัฒนาขึ้นเพื่อควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร นอกจากนี้ผลจากการใช้งานเครื่องมือยังสามารถนำมาประเมินเพื่อนำไปสู่การปรับปรุงกระบวนการและเครื่องมือนั่นเอง

5.1 การวิเคราะห์ความต้องการของเครื่องมือสนับสนุนกระบวนการ

จากการนำเอากระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศมาศึกษาและวิเคราะห์ พบว่า สามารถสรุปถึงความต้องการของเครื่องมือสนับสนุนกระบวนการ โดยแบ่งออกเป็น 2 ส่วนหลัก ได้แก่ ความต้องการเชิงหน้าที่และความต้องการที่ไม่ใช่เชิงหน้าที่ โดยรายละเอียดมีดังต่อไปนี้

5.1.1 **ความต้องการเชิงหน้าที่** (Functional Requirements) เครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้แบ่งฟังก์ชันการทำงานออกเป็น 2 ระบบหลัก ได้แก่ ระบบการทำงานหลักและระบบสนับสนุนการทำงาน และในแต่ละระบบสามารถแยกย่อยตามจุดประสงค์ของการใช้งาน ได้ดังต่อไปนี้

1) **ระบบการทำงานหลัก** (Main Functionalities) โดยระบบการทำงานหลักสามารถแยกออกเป็น 9 ระบบย่อย ได้ดังนี้

1.1) **ระบบสนับสนุนการจัดตั้งกระบวนการ** (Project Initiation) สามารถแบ่งหน้าที่การทำงานออกเป็น 3 ส่วน ดังนี้

1.1.1) บันทึก แก้ไขและเรียกดูข้อมูลการจัดตั้งกระบวนการ

1.1.2) บันทึก แก้ไขและเรียกดูข้อมูลนโยบายกระบวนการ

1.1.3) บันทึก แก้ไขและเรียกดูข้อมูลกลยุทธ์กระบวนการ

1.2) **ระบบสนับสนุนการระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ** (Risk Determination) สามารถแบ่งหน้าที่การทำงานออกเป็น 10 ส่วน ดังนี้

1.2.1) บันทึก แก้ไขและเรียกดูข้อมูลกลยุทธ์ของการประเมินความเสี่ยง

1.2.2) บันทึก แก้ไขและเรียกดูข้อมูลการจัดการความเสี่ยงที่คงเหลือ

1.2.3) บันทึก แก้ไขและเรียกดูข้อมูลปัจจัยทางธุรกิจ

1.2.4) บันทึก แก้ไขและเรียกดูข้อมูลสินทรัพย์ประเภทสารสนเทศที่ต้องการการควบคุมการเข้าถึง

1.2.5) บันทึก แก้ไขและเรียกดูข้อมูลปัจจัยทางธุรกิจของสินทรัพย์ประเภทสารสนเทศ

1.2.6) บันทึก แก้ไขและเรียกดูข้อมูลคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ

1.2.7) บันทึก แก้ไขและเรียกดูข้อมูลภัยคุกคามของสินทรัพย์ประเภทสารสนเทศ

1.2.8) บันทึก แก้ไขและเรียกดูข้อมูลจุดอ่อนที่จะใช้โดยภัยคุกคาม

1.2.9) บันทึก แก้ไขและเรียกดูข้อมูลการประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

1.2.10) บันทึก แก้ไขและเรียกดูข้อมูลการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

1.3) **ระบบสนับสนุนการเลือกและกำหนดวิธีการควบคุมการเข้าถึง** (Access Control Selection and Definition) สามารถแบ่งหน้าที่การทำงานออกเป็น 6 ส่วน ดังนี้

1.3.1) บันทึก แก้ไขและเรียกดูข้อมูลผู้ใช้งานหรือกลุ่มผู้ใช้งานที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1.3.2) บันทึก แก้ไขและเรียกดูข้อมูลบทบาทของการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1.3.3) บันทึก แก้ไขและเรียกดูข้อมูลสิทธิของการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1.3.4) บันทึก แก้ไขและเรียกดูข้อมูลปัจจัยการเลือกใช้โมเดลการควบคุมการเข้าถึง

1.3.5) บันทึก แก้ไขและเรียกดูข้อมูลการเลือกใช้โมเดลการควบคุมการเข้าถึง

1.3.6) บันทึก แก้ไขและเรียกดูข้อมูลวิธีการของการควบคุมการเข้าถึง คือ วิธีการของการให้อำนาจ วิธีการเข้าถึงเชิงบทบาท วิธีการของความมั่นคงหลายระดับ และวิธีการของการตรวจสอบการเข้าถึง

1.4) **ระบบสนับสนุนการกำหนดวิธีการระบุและพิสูจน์ตัวตน (Identification and Authentication Definition)** สามารถแบ่งหน้าที่การทำงานออกเป็น 2 ส่วน ดังนี้

1.4.1) บันทึก แก้ไขและเรียกดูข้อมูลความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน

1.4.2) บันทึก แก้ไขและเรียกดูข้อมูลการออกแบบและใช้งานรหัสผ่าน

1.5) **ระบบสนับสนุนการตรวจสอบข้อกำหนดกระบวนการ (Project Information Verification)** สามารถแบ่งหน้าที่การทำงานออกเป็น 2 ส่วน ดังนี้

1.5.1) บันทึก แก้ไขและเรียกดูข้อมูลการทวนสอบข้อกำหนดกระบวนการ

1.5.2) บันทึก แก้ไขและเรียกดูข้อมูลการทวนสอบข้อกำหนดกระบวนการเมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ

1.6) **ระบบสนับสนุนการวางแผนปฏิบัติการ** (Project Planning Management) สามารถแบ่งหน้าที่การทำงานออกเป็น 5 ส่วน ดังนี้

1.6.1) บันทึก แก้ไขและเรียกดูข้อมูลการวางแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร

1.6.2) บันทึก แก้ไขและเรียกดูข้อมูลการจัดการความเสี่ยงของการพัฒนาระบบ

1.6.3) บันทึก แก้ไขและเรียกดูข้อมูลการวางแผนการทดสอบระบบ

1.6.4) บันทึก แก้ไขและเรียกดูข้อมูลการวางแผนการเฝ้าสังเกตและตรวจสอบระบบ

1.6.5) บันทึก แก้ไขและเรียกดูข้อมูลการวางแผนการปรับปรุงระบบ

1.7) **ระบบสนับสนุนการพัฒนาระบบและการใช้งาน** (System Implementation Management) สามารถแบ่งหน้าที่การทำงานออกเป็น 7 ส่วน ดังนี้

1.7.1) บันทึก แก้ไขและเรียกดูข้อมูลการวางแผนการอบรมทีมการทำงานผู้ที่เกี่ยวข้อง และผู้ใช้งานระบบ

1.7.2) บันทึก แก้ไขและเรียกดูข้อมูลการประเมินผลการอบรม

1.7.3) บันทึก แก้ไขและเรียกดูข้อมูลรายงานความก้าวหน้าของการพัฒนาระบบ

1.7.4) บันทึก แก้ไขและเรียกดูข้อมูลการจัดการกับการเปลี่ยนแปลงที่อาจเกิดขึ้นระหว่างการพัฒนาระบบ

1.7.5) บันทึก แก้ไขและเรียกดูข้อมูลรายการตรวจสอบของการพัฒนาระบบ

1.7.6) บันทึก แก้ไขและเรียกดูข้อมูลรายการกรณีทดสอบ

1.7.7) บันทึก แก้ไขและเรียกดูข้อมูลผลการทดสอบระบบ

1.8) **ระบบสนับสนุนการเฝ้าสังเกตและทวนสอบระบบ** (System Monitoring and Reviewing Management) สามารถแบ่งหน้าที่การทำงานออกเป็น 5 ส่วน ดังนี้

1.8.1) บันทึก แก้ไขและเรียกดูข้อมูลวิธีการประเมินประสิทธิภาพของระบบ

1.8.2) บันทึก แก้ไขและเรียกดูข้อมูลรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบ

1.8.3) บันทึก แก้ไขและเรียกดูข้อมูลรายงานบันทึกผลการประเมินประสิทธิภาพของระบบ

1.8.4) บันทึก แก้ไขและเรียกดูข้อมูลรายงานบันทึกผลการปรับแผนการเฝ้าสังเกตและตรวจสอบระบบ

1.8.5) บันทึก แก้ไขและเรียกดูข้อมูลรายงานบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบ

1.9) **ระบบสนับสนุนการปรับปรุงระบบ** (System Improvement Management) สามารถแบ่งหน้าที่การทำงานออกเป็น 3 ส่วน ดังนี้

1.9.1) บันทึก แก้ไขและเรียกดูข้อมูลรายงานบันทึกผลการวิเคราะห์การยอมรับการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบ

1.9.2) บันทึก แก้ไขและเรียกดูข้อมูลความคิดเห็นของผู้ที่เกี่ยวข้องต่อการ ปรับปรุงระบบ

1.9.3) บันทึก แก้ไขและเรียกดูข้อมูลการกระทำและการป้องกันสำหรับการปรับปรุงระบบ

2 **ระบบสนับสนุนการทำงาน** (Supporting Functionalities) โดยระบบสนับสนุนการทำงานสามารถแยกออกเป็น 2 ระบบย่อย ได้ดังนี้

2.1) **ระบบสนับสนุนข้อมูลการดำเนินการ** (Information Supporting Management) สามารถแบ่งหน้าที่การทำงานออกเป็น 3 ส่วน ดังนี้

2.1.1) เรียกดูข้อมูลส่วนการดำเนินการของกระบวนการ

2.1.2) ดาวน์โหลดเอกสารการดำเนินการของกระบวนการ

2.1.3) เรียกดูและจัดพิมพ์เอกสารการดำเนินการของกระบวนการ

2.2) **ระบบสนับสนุนสิทธิการเข้าใช้งานระบบ** (Authorization Management) สามารถแบ่งหน้าที่การทำงานออกเป็น 4 ส่วน ดังนี้

2.2.1) แก้ไขและเรียกดูข้อมูลส่วนบุคคลของผู้ใช้งานระบบ

2.2.2) แก้ไขรหัสผ่านของผู้ใช้งานระบบ

2.2.3) บันทึก เรียกดูและลบข้อมูลผู้ใช้งานระบบ

2.2.4) จัดการข้อมูลสิทธิการเข้าถึงระบบของผู้ใช้งาน

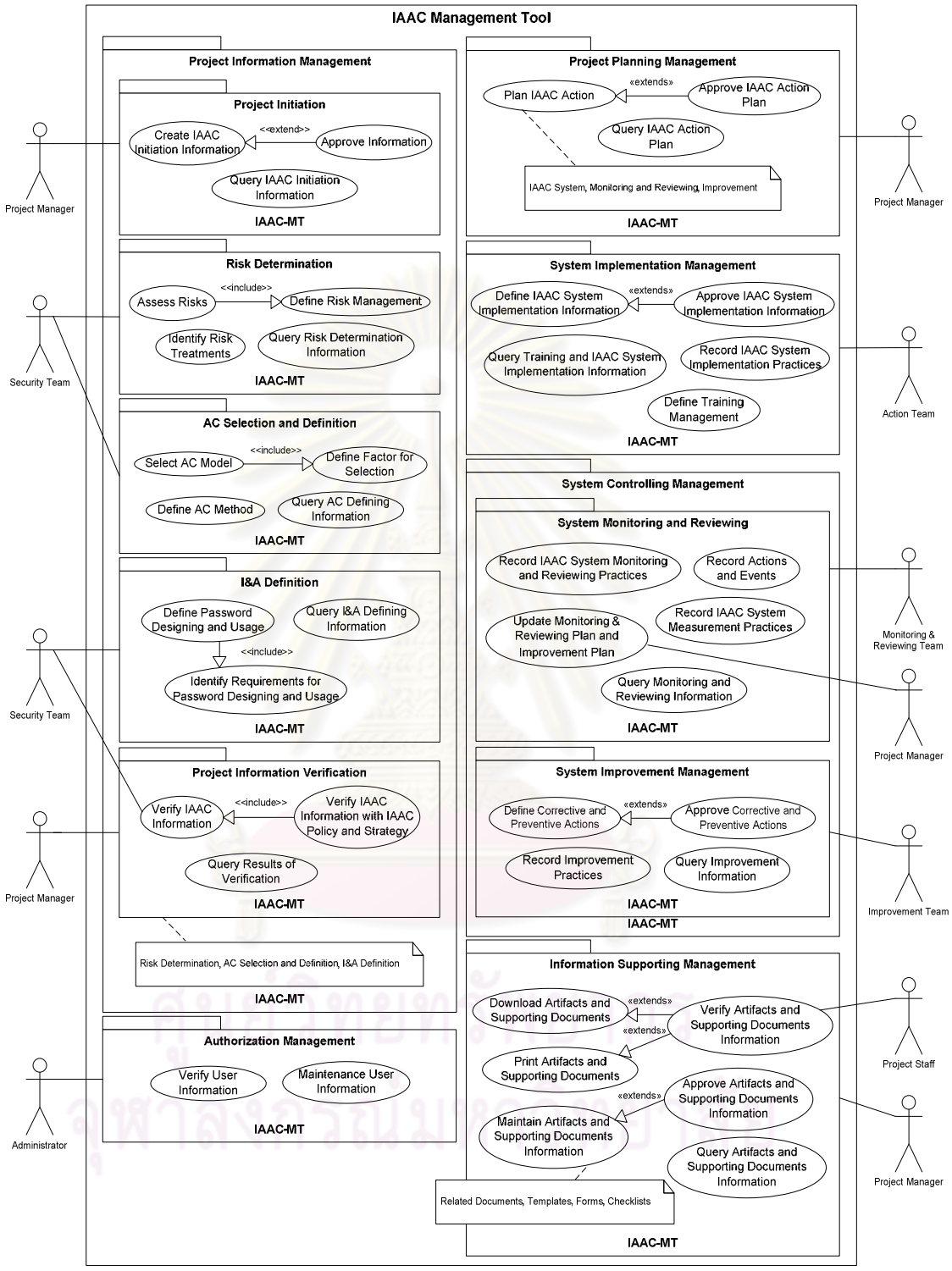
5.1.2 **ความต้องการที่ไม่ใช่เชิงหน้าที่** (Non-Functional Requirements) เป็นความต้องการที่สนับสนุนการทำงานของเครื่องมือให้มีประสิทธิภาพมากยิ่งขึ้น โดยมองปัจจัยที่เกี่ยวข้องในหลายๆ ด้าน โดยมีรายละเอียดของความต้องการที่ไม่ใช่หน้าที่แสดงดังตารางที่ 5.1

ตารางที่ 5.1 ความต้องการที่ไม่ใช่หน้าที่ของเครื่องมือสนับสนุนกระบวนการ

ความต้องการที่ไม่ใช่หน้าที่	คำอธิบาย
ความมั่นคงของระบบ (Security)	ระบบควรมีส่วนการทำงานในการกำหนดการเข้าใช้งานระบบในแต่ละบทบาทของผู้ใช้
ความสามารถของการใช้งานระบบ (Usability)	ระบบควรมีการออกแบบที่ง่ายต่อการใช้ง่าย แยกส่วนการทำงานออกอย่างชัดเจน พร้อมคำอธิบายในแต่ละการทำงานนั้น
ความต้องการด้านการเคลื่อนย้ายระบบ (Portability Requirements)	ระบบควรมีรูปแบบการติดตั้งที่ไม่ซับซ้อน โดยใช้สถาปัตยกรรมแบบเว็บเบสแอปพลิเคชัน ซึ่งผู้ใช้งานสามารถติดต่อผ่านเครือข่ายอินทราเน็ตเข้ามาใช้งานระบบได้
การบำรุงรักษาได้ของระบบ (Maintainability)	รหัสต้นฉบับ (Source Code) ของระบบควรมีการเขียนหมายเหตุ (Comment) และแบ่งแยกส่วนการทำงานอย่างชัดเจน ทั้งนี้เพื่อให้ง่ายต่อผู้ดูแลและบำรุงรักษาระบบต่อไปในภายหลัง

5.2 การออกแบบหน้าที่การทำงานของเครื่องมือสนับสนุนกระบวนการ

หน้าที่การทำงานของเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้แบ่งออกเป็น 2 ระบบงานหลัก 11 ระบบงานย่อย ซึ่งสามารถแสดงได้ด้วยแผนภาพยูสเคสดังรูปที่ 5.1



รูปที่ 5.1 แผนภาพยูสเคสแสดงหน้าที่การทำงานของเครื่องมือสนับสนุนกระบวนการ

จากรูปที่ 5.1 สามารถอธิบายรายละเอียดของระบบงานย่อยทั้ง 11 ระบบและผู้ที่เกี่ยวข้องได้ดังต่อไปนี้

5.2.1 **ส่วนการทำงานหลักของครื่องมือสนับสนุนกระบวนการ** ประกอบด้วยระบบงานย่อย 9 ระบบ ดังนี้

1) **การริเริ่มกระบวนการ** (Project Initiation) ก่อนการดำเนินการกระบวนการจำเป็นที่จะต้องกำหนดข้อมูลพื้นฐานเบื้องต้น เช่น ขอบเขต เป้าหมาย พันธกิจ นโยบายและกลยุทธ์ของกระบวนการ เป็นต้น ข้อมูลเหล่านี้จะถูกนำมาใช้เพื่อเป็นแนวทางของการปฏิบัติต่อไป นอกจากนี้ข้อมูลดังกล่าวจะเป็นตัวบ่งชี้หรือประเมินผลว่าการดำเนินการนั้นบรรลุผลสำเร็จหรือไม่ และเนื่องจากเป็นข้อมูลที่สำคัญของกระบวนการจึงถูกกำหนดโดยผู้จัดการโครงการ (Project Manager)

2) **การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ** (Risk Determination) การสร้างการควบคุมการเข้าถึงให้กับสินทรัพย์ประเภทสารสนเทศนั้นจำเป็นที่จะต้องระบุถึงสินทรัพย์ที่มีทั้งหมด รวมถึงการประเมินความเสี่ยงที่จะเกิดขึ้นกับสินทรัพย์เหล่านั้น ทั้งนี้เพื่อดูว่ามีความเสี่ยงมาก-น้อยเพียงใด ซึ่งผลที่ได้จะถูกนำมาเป็นแนวทางของการระบุการรักษาความเสี่ยง ในที่นี้จะมุ่งเน้นไปที่การกำหนดวิธีการควบคุมการเข้าถึงและวิธีการระบุและพิสูจน์ตัวตนแบบรหัสผ่าน การปฏิบัติในระบบงานนี้จะต้องปฏิบัติโดยทีมที่มีความเชี่ยวชาญทางด้านความมั่นคงเป็นอย่างสูง

3) **การเลือกและกำหนดวิธีการการควบคุมการเข้าถึง** (Access Control Selection and Definition) ระบบงานนี้สนับสนุนการกำหนดวิธีการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยก่อนการกำหนดจะต้องทำการเลือกโมเดลการควบคุมที่เหมาะสม ซึ่งต้องพิจารณาจากปัจจัยแวดล้อมขององค์กรเป็นสำคัญ

4) **การกำหนดวิธีการระบุและพิสูจน์ตัวตน** (Identification and Authentication Definition) ระบบงานนี้สนับสนุนการกำหนดวิธีการของการออกแบบและใช้งานรหัสผ่าน โดยรวมถึงการกำหนดความต้องการและปัจจัยต่างๆ ที่มีความเกี่ยวข้อง

5) **การตรวจสอบข้อกำหนดของกระบวนการ** (Project Information Verification) การตรวจสอบความถูกต้องของข้อมูลต่างๆ ที่เกี่ยวข้องกับความมั่นคงของสินทรัพย์ประเภทสารสนเทศขององค์กรถือว่าเป็นขั้นตอนที่มีความสำคัญอย่างมาก เนื่องจากข้อมูลเหล่านั้นจะถูกนำมาใช้เป็นกรอบของการสร้างความมั่นคงนั่นเอง การตรวจสอบข้อมูลจะต้องผ่านการตรวจสอบด้านความถูกต้องตามหลักการของความมั่นคง และด้านความสอดคล้องหรือเป็นไป

ตามนโยบายหรือกลยุทธ์ของกระบวนการที่ได้กำหนดไว้ตั้งแต่แรกเริ่มโครงการ ทั้งทีมความมั่นคง (Security Team) และผู้จัดการโครงการจะเข้ามารับผิดชอบการทำงานในระบบงานนี้

6) **การวางแผนปฏิบัติการ** (Project Planning Management) ผู้จัดการโครงการจะทำการสร้างแผนการดำเนินการเพื่อให้บรรลุผลตามวัตถุประสงค์ที่ได้ตั้งไว้ แผนการในที่นี้จะรวมถึงแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ แผนการเฝ้าสังเกตและทวนสอบระบบ และแผนการปรับปรุงระบบ ทั้งนี้ในการสร้างแผนนั้นจะต้องมีการกำหนดข้อมูลสำคัญ เช่น หลักการด้านความมั่นคงที่นำมาประยุกต์ใช้ ผู้ดำเนินการรับผิดชอบ ทรัพยากรที่จำเป็นต้องใช้ ระยะเวลาของการปฏิบัติการ เป็นต้น

7) **การพัฒนาระบบ** (System Implementation Management) ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศถูกพัฒนาขึ้นเพื่อใช้ควบคุมการเข้าถึงและเข้าใช้งานสินทรัพย์ประเภทสารสนเทศของผู้ใช้ภายในองค์กร ความต้องการของระบบและแผนภาพการออกแบบ รวมถึงการบันทึกความก้าวหน้าของการปฏิบัติการพัฒนาระบบจะถูกระบุในระบบงานนี้ นอกจากนี้แล้วการกำหนดการจัดการการอบรมเพื่อให้เกิดความเข้าใจรับรู้ในกระบวนการและความสามารถในการใช้งานระบบได้อย่างถูกต้อง สำหรับทั้งเจ้าหน้าที่โครงการ (Project Staff) และผู้ใช้งานระบบได้ถูกระบุในระบบงานนี้ด้วย และทีมการพัฒนา (Development Team) จะมีหน้าที่รับผิดชอบโดยตรง

8) **การเฝ้าสังเกตและทวนสอบระบบ** (System Monitoring and Reviewing Management) เมื่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกใช้งานไปในระยะหนึ่ง การเฝ้าสังเกตและทวนสอบระบบจะถูกปฏิบัติเพื่อวัดประสิทธิภาพของการรองรับการใช้งานของผู้ใช้ ผลจากการปฏิบัติจะต้องมีการบันทึกเอาไว้ และตัวชี้วัดได้ถูกกำหนดขึ้นเพื่อใช้เป็นเกณฑ์ของการวัด เมื่อเสร็จสิ้นการ เฝ้าสังเกตและทวนสอบระบบ ทีมการเฝ้าสังเกตและทวนสอบ (Monitoring and Reviewing Team) จะต้องทำการบันทึกการกระทำและเหตุการณ์ที่ซึ่งกระทบประสิทธิภาพของระบบ นอกจากนี้ผู้จัดการโครงการจะต้องทำการปรับปรุงแผนการเฝ้าสังเกตและทวนสอบระบบและแผนการปรับปรุงระบบเพื่อใช้ในการปฏิบัติครั้งต่อไป

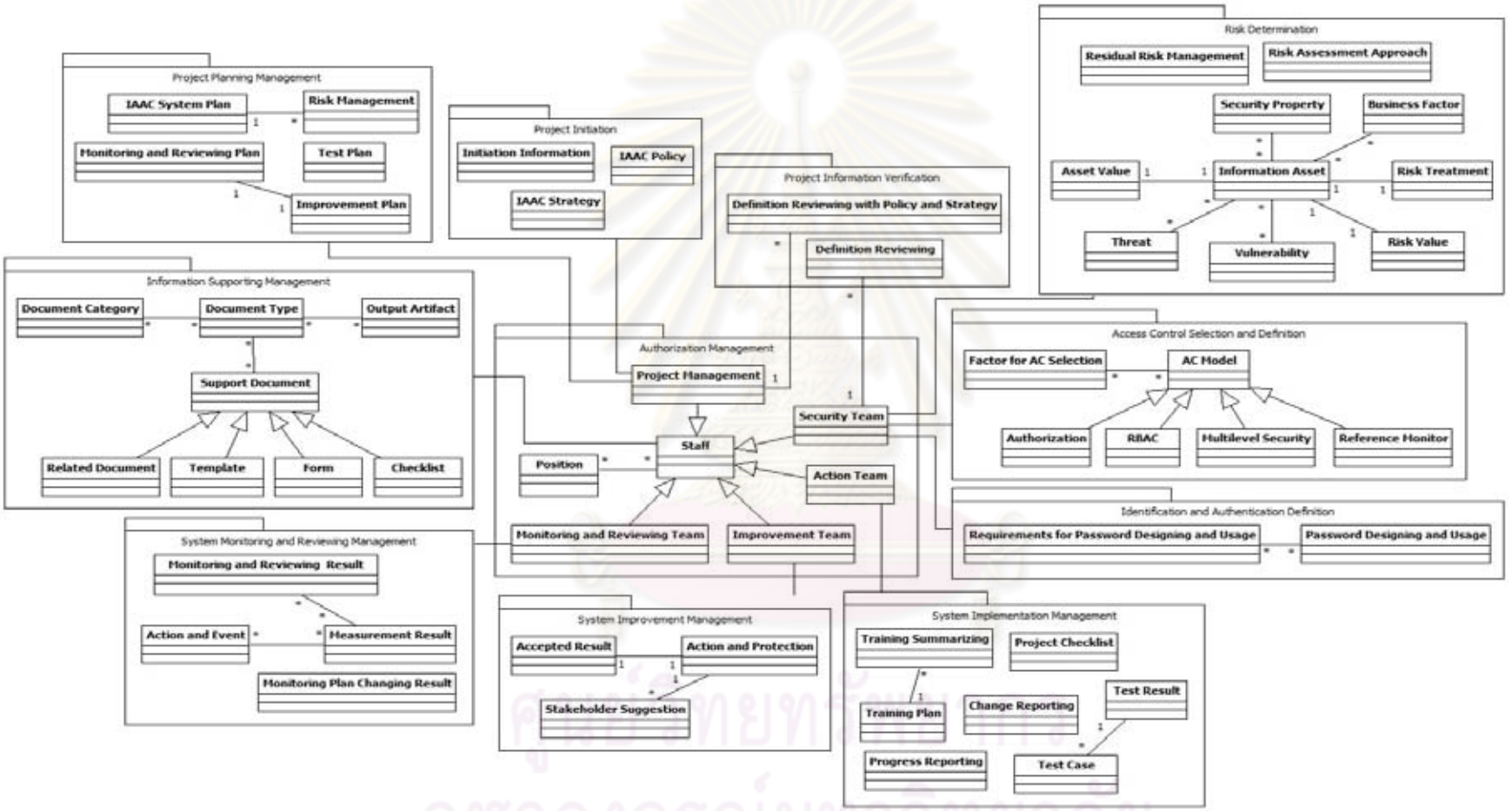
9) **การปรับปรุงระบบ** (System Improvement Management) ทีมการปรับปรุง (Improvement Team) จะต้องวิเคราะห์และพิจารณาผลลัพธ์จากการเฝ้าสังเกตและทวนสอบระบบ ทั้งนี้เพื่อกำหนดเป็นการกระทำและการป้องกันสำหรับการปรับปรุงระบบ

5.2.2 **ส่วนการทำงานสนับสนุนของเครื่องมือสนับสนุนกระบวนการ** ประกอบด้วยระบบงานย่อย 2 ระบบ ดังนี้

1) **การสนับสนุนระบบ** (Information Supporting Management) การดำเนินการตามกระบวนการก่อให้เกิดหรือเกี่ยวข้องกับเอกสารต่างๆ มากมาย เช่น เอกสารแนะนำ เอกสารแผ่นแบบ แบบฟอร์ม รายการตรวจสอบ เป็นต้น ดังนั้นเจ้าหน้าที่โครงการสามารถที่จะดาวน์โหลดและพิมพ์เอกสารเหล่านั้นเพื่อใช้ประกอบการปฏิบัติงานหรือกิจกรรมใดๆ ส่วนการบำรุงรักษาและการตรวจสอบเอกสารจะปฏิบัติโดยผู้จัดการโครงการ

(2) **การจำกัดสิทธิการใช้งานระบบ** (Authorization Management) การตรวจสอบสิทธิในการเข้าใช้งานในแต่ละระบบงานใดๆ รวมถึงการบำรุงรักษาข้อมูลส่วนบุคคลได้ถูกปฏิบัติในระบบงานนี้โดยผู้ดูแลระบบ (Administrator)

นอกจากนี้แผ่นภาพคลาสยังถูกนำมาใช้ในการออกแบบเครื่องมือสนับสนุนกระบวนการทั้งนี้เพื่อแสดงให้เห็นถึงวัตถุที่เกิดขึ้น องค์ประกอบสำคัญ รวมถึงความสัมพันธ์ของแต่ละวัตถุ โดยสามารถแสดงได้ดังรูปที่ 5.2 และคำอธิบายแผนภาพคลาสสามารถแสดงได้ดังตารางที่ 5.2



รูปที่ 5.2 แผนภาพคลาสแสดงวัตถุและความสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการ

ตารางที่ 5.2 คำอธิบายแผนภาพคลาสของเครื่องมือสนับสนุนกระบวนการ

ชื่อคลาส	คำอธิบาย
ส่วนการจัดตั้งโครงการ (Project Initiation)	
Initiation Information	ข้อมูลการจัดตั้งกระบวนการ
IAAC Policy	ข้อมูลนโยบายกระบวนการ
IAAC Strategy	ข้อมูลกลยุทธ์ของกระบวนการ
ส่วนการระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Risk Determination)	
Risk Assessment Approach	ข้อมูลกลยุทธ์ของการประเมินความเสี่ยง
Residual Risk Management	ข้อมูลการจัดการความเสี่ยงที่ผันแปร
Information Asset	ข้อมูลสินทรัพย์ประเภทสารสนเทศที่ต้องการการควบคุมการเข้าถึง
Business Factor	ข้อมูลปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ
Security Property	ข้อมูลคุณสมบัติด้านความมั่นคง
Asset Value	ข้อมูลมูลค่าของสินทรัพย์ประเภทสารสนเทศ
Threat	ข้อมูลภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ
Vulnerability	ข้อมูลจุดอ่อนที่ถูกใช้โดยภัยคุกคามของสินทรัพย์ประเภทสารสนเทศ
Risk Value	ข้อมูลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
Risk Treatment	ข้อมูลการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
ส่วนการเลือกและกำหนดวิธีการการควบคุมการเข้าถึง (Access Control Selection and Definition)	
Factor for AC Selection	ข้อมูลของปัจจัยในการเลือกใช้โมเดลวิธีการควบคุมการเข้าถึง
AC Model	ข้อมูลของโมเดลวิธีการควบคุมการเข้าถึง
Authorization	ข้อมูลของโมเดลวิธีการของการให้อำนาจ
RBAC	ข้อมูลของโมเดลวิธีการเข้าถึงเชิงบทบาท
ส่วนการเลือกและกำหนดวิธีการการควบคุมการเข้าถึง (Access Control Selection and Definition)	
Multilevel Security	ข้อมูลของโมเดลวิธีการของความมั่นคงหลายระดับ
Reference Monitor	ข้อมูลของโมเดลวิธีการตรวจสอบการเข้าถึง
ส่วนการกำหนดวิธีการระบุและพิสูจน์ตัวตน (Identification and Authentication Definition)	
Requirements for Password Designing and Usage	ข้อมูลความต้องการสำหรับการออกแบบรและการใช้งานหัสผ่าน
Password Designing and Usage	ข้อมูลวิธีการออกแบบและการใช้งานรหัสผ่าน

ตารางที่ 5.2 คำอธิบายแผนภาพคลาสของเครื่องมือสนับสนุนกระบวนการ (ต่อ)

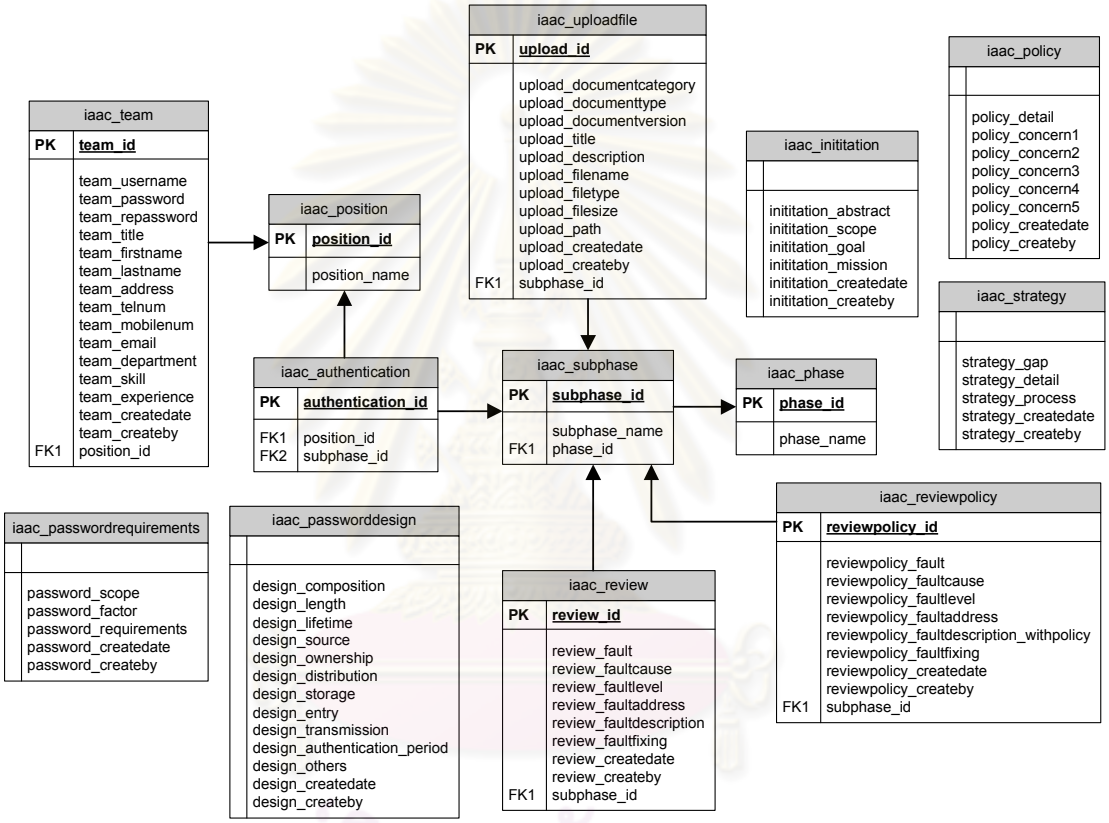
ชื่อคลาส	คำอธิบาย
ส่วนการตรวจสอบข้อกำหนดของกระบวนการ (Project Information Verification)	
Definition Reviewing	ข้อมูลการตรวจสอบข้อกำหนดของกระบวนการ
Definition Reviewing with Policy and Strategy	ข้อมูลการตรวจสอบข้อกำหนดของกระบวนการ เมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ
ส่วนการวางแผนปฏิบัติการ (Project Planning Management)	
IAAC System Plan	ข้อมูลแผนการพัฒนาระบบ
Risk Management	ข้อมูลการจัดการความเสี่ยงของการพัฒนาระบบ
Test Plan	ข้อมูลแผนการทดสอบระบบ
Monitoring and Reviewing Plan	ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ
Improvement Plan	ข้อมูลแผนการปรับปรุงระบบ
ส่วนการพัฒนาระบบ (System Implementation Management)	
Training Plan	ข้อมูลแผนการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง
Training Summarizing	ข้อมูลผลการประเมินการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง
Progress Reporting	ข้อมูลความก้าวหน้าของการพัฒนาระบบ
Change Reporting	ข้อมูลการเปลี่ยนแปลงของการพัฒนาระบบ
ส่วนการพัฒนาระบบ (System Implementation Management)	
Project Checklist	ข้อมูลรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ
Test Case	ข้อมูลกรณีทดสอบสำหรับใช้ทดสอบระบบ
Test Result	ข้อมูลผลการทดสอบระบบ
ส่วนการเฝ้าสังเกตและทวนสอบระบบ (System Monitoring and Reviewing Management)	
Monitoring and Reviewing Result	ข้อมูลผลการเฝ้าสังเกตและทวนสอบระบบ
Measurement Result	ข้อมูลผลการประเมินประสิทธิภาพของระบบ
Monitoring Plan Changing Result	ข้อมูลผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบ
Action and Event	ข้อมูลการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ

ตารางที่ 5.2 คำอธิบายแผนภาพคลาสของเครื่องมือสนับสนุนกระบวนการ (ต่อ)

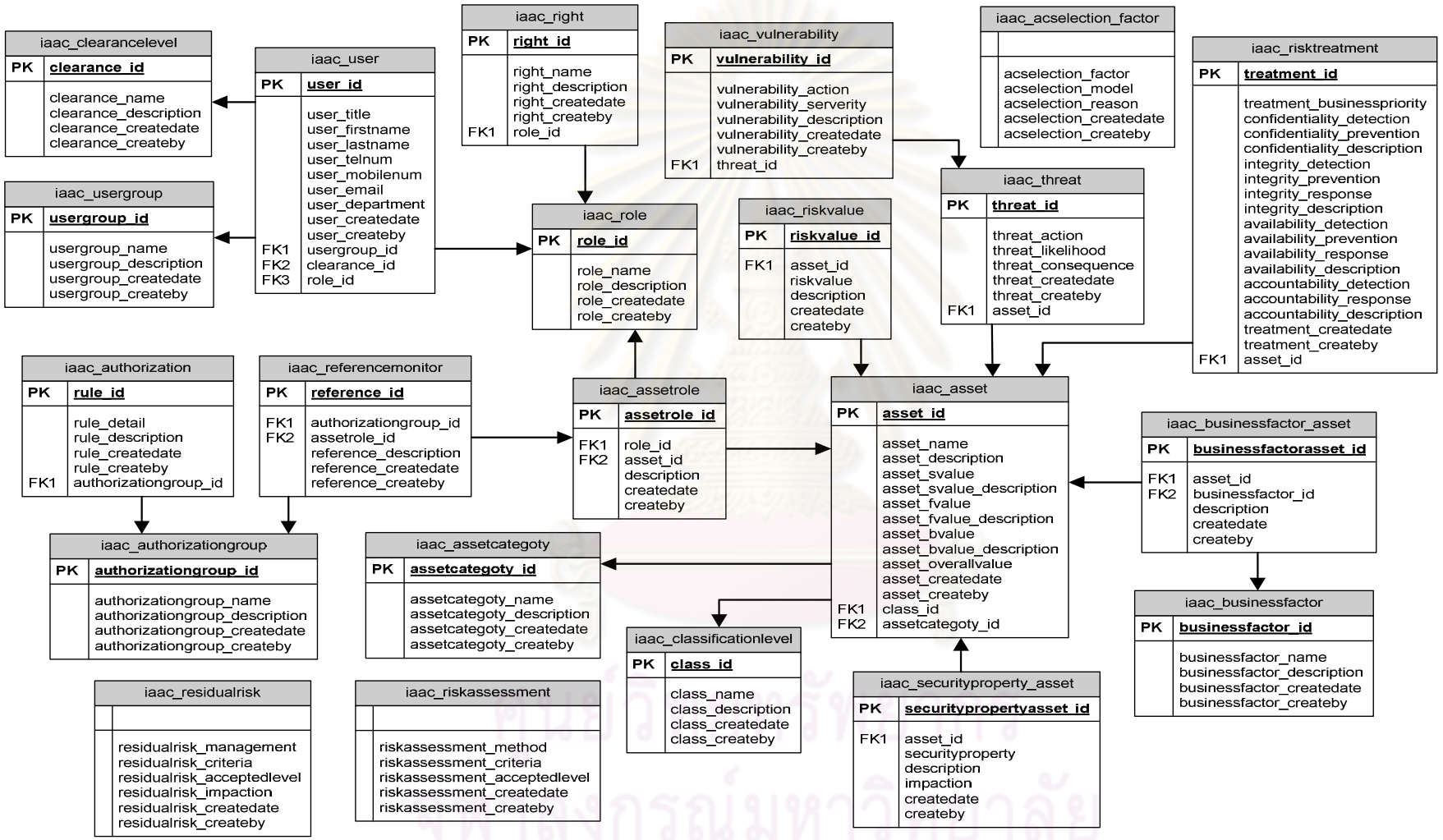
ชื่อคลาส	คำอธิบาย
ส่วนการปรับปรุงระบบ (System Improvement Management)	
Accepted Result	ข้อมูลผลการวิเคราะห์การยอมรับของการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
Action and Protection	ข้อมูลการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
Stakeholder Suggestion	ข้อมูลข้อเสนอแนะต่อการกระทำและการป้องกันสำหรับการปรับปรุงระบบของผู้ที่เกี่ยวข้องกับกระบวนการ
ส่วนการสนับสนุนระบบ (Information Supporting Management)	
Document Type	ข้อมูลประเภทของเอกสารสนับสนุนการ
Document Category	ข้อมูลหมวดหมู่ของเอกสารสนับสนุนการ
Support Document	ข้อมูลของเอกสารสนับสนุนกระบวนการ
Related Document	ข้อมูลของเอกสารที่เกี่ยวข้องกับกระบวนการ
Template	ข้อมูลของเอกสารแผ่นแบบ
ส่วนการสนับสนุนระบบ (Information Supporting Management)	
Form	ข้อมูลของฟอร์ม
Checklist	ข้อมูลของรายการตรวจสอบ
Output Artifact	ข้อมูลของอาร์ทิแฟกผลลัพธ์จากการดำเนินการกระบวนการ
ส่วนการจำกัดสิทธิการใช้งานระบบ (Authorization Management)	
Position	ข้อมูลตำแหน่งของเจ้าหน้าที่ดำเนินการกระบวนการ
Staff	ข้อมูลของเจ้าหน้าที่ผู้ซึ่งดำเนินการกระบวนการ
Project Management	ข้อมูลของผู้จัดการโครงการ
Security Team	ข้อมูลของทีมความมั่นคง
Action Team	ข้อมูลของทีมพัฒนาระบบ
Monitoring and Reviewing Team	ข้อมูลของทีมการเฝ้าสังเกตและทวนสอบระบบ
Improvement Team	ข้อมูลของทีมการปรับปรุงระบบ

5.3 การออกแบบฐานข้อมูลสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการ

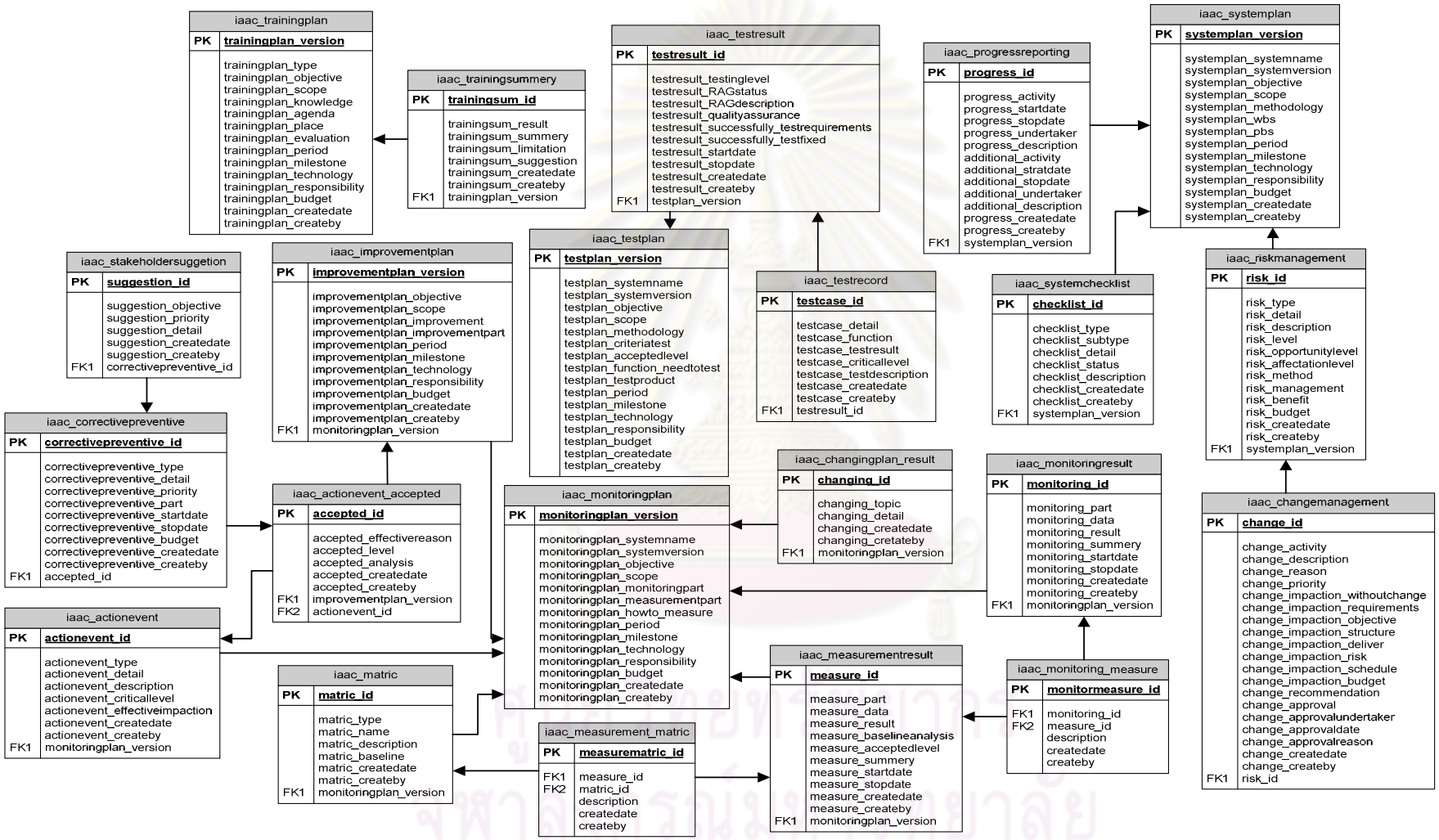
การออกแบบฐานข้อมูลสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ได้พิจารณาตามแผนภาพคลาสที่ได้ออกแบบไว้ก่อนหน้า โดยมีลักษณะเป็นฐานข้อมูลเชิงกายภาพที่ซึ่งแสดงให้เห็นตารางข้อมูลและความสัมพันธ์ระหว่างตารางข้อมูล ดังรูปที่ 5.3 สำหรับรายละเอียดของตารางข้อมูลสามารถแสดงได้ในภาคผนวก ง.



รูปที่ 5.3 โครงสร้างฐานข้อมูลเชิงสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการ



รูปที่ 5.3 โครงสร้างฐานข้อมูลเชิงสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการ (ต่อ)



รูปที่ 5.3 โครงสร้างฐานข้อมูลเชิงสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการ (ต่อ)

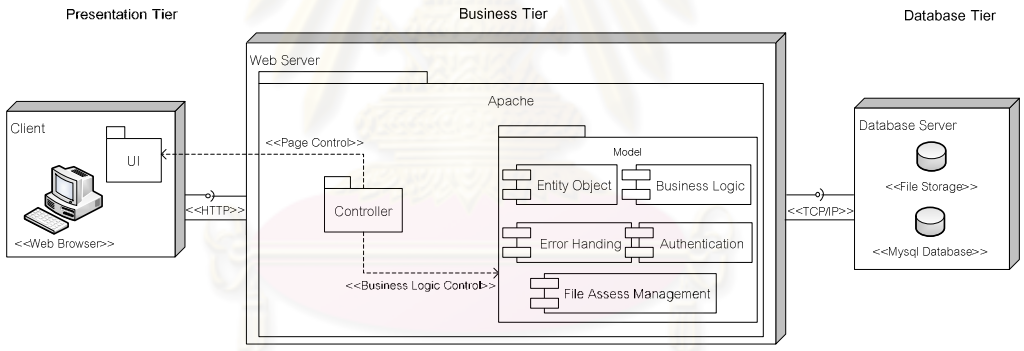
5.4 การออกแบบสถาปัตยกรรมของเครื่องมือสนับสนุนกระบวนการ

การออกแบบสถาปัตยกรรมระบบจะแสดงให้เห็นถึงโครงสร้างเทคโนโลยีของเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่สร้างขึ้น โดยสถาปัตยกรรมที่ใช้นั้นเป็นการเชื่อมต่อผ่านโพรโทคอลทีซีพีไอพี (TCP/IP) และระบบที่พัฒนาขึ้นมีฐานข้อมูลแบบรวมศูนย์ (Centralized Database) และส่วนงานสนับสนุนที่มีลักษณะโครงสร้างสถาปัตยกรรมแบบเว็บเบสแอพพลิเคชัน (Web Based Application) โดยที่สถาปัตยกรรมเทคโนโลยีนี้มีโครงสร้างเป็นแบบหลายชั้น (Multi-Tier) สามารถแสดงได้ในรูปที่ 5.4 ซึ่งมีรายละเอียดดังต่อไปนี้

1) **ชั้นการนำเสนอ** (Presentation Tier) ทำหน้าที่เป็นส่วนต่อประสานกับผู้ใช้งานระบบ

2) **ชั้นตรรกะทางธุรกิจ** (Business Logic Tier) ทำหน้าที่ให้บริการข้อมูลและประมวลการผลการทำงานให้แก่เครื่องลูกข่าย

3) **ชั้นหน่วยข้อมูล** (Data Tier) ทำหน้าที่เก็บข้อมูลของระบบทั้งหมด



รูปที่ 5.4 แผนภาพสถาปัตยกรรมของเครื่องมือสนับสนุนกระบวนการ

จากรูปที่ 5.4 เป็นสถาปัตยกรรมระบบแบบเว็บเบสแอพพลิเคชัน มีการออกแบบสถาปัตยกรรมซอฟต์แวร์ในชั้นตรรกะทางธุรกิจ ผู้วิจัยได้แบ่งแยกการออกแบบเป็น 4 ส่วนหลัก ดังนี้

1) **ส่วนการแสดงผล** (User Interface) เป็นส่วนที่รับข้อมูลจากผู้ใช้งานและส่งต่อไปยังส่วนควบคุมการไหลของการแสดงผล รวมถึงการแสดงผลการทำงานตามผลของส่วนการควบคุมด้านตรรกะธุรกิจ

2) **ส่วนควบคุม** (Controller) ประกอบด้วย 2 ส่วนการทำงาน ดังนี้

2.1) **ส่วนการควบคุมการไหลของการแสดงผล** (Page Control) เป็นส่วนควบคุมการแสดงผลตามผลที่เกิดขึ้นจากการทำงานของส่วนตรรกะธุรกิจ เช่น เมื่อผู้ใช้กรอกข้อมูลผิดพลาด ระบบต้องเรียกส่วนการแสดงผลผิดพลาดมาแสดง

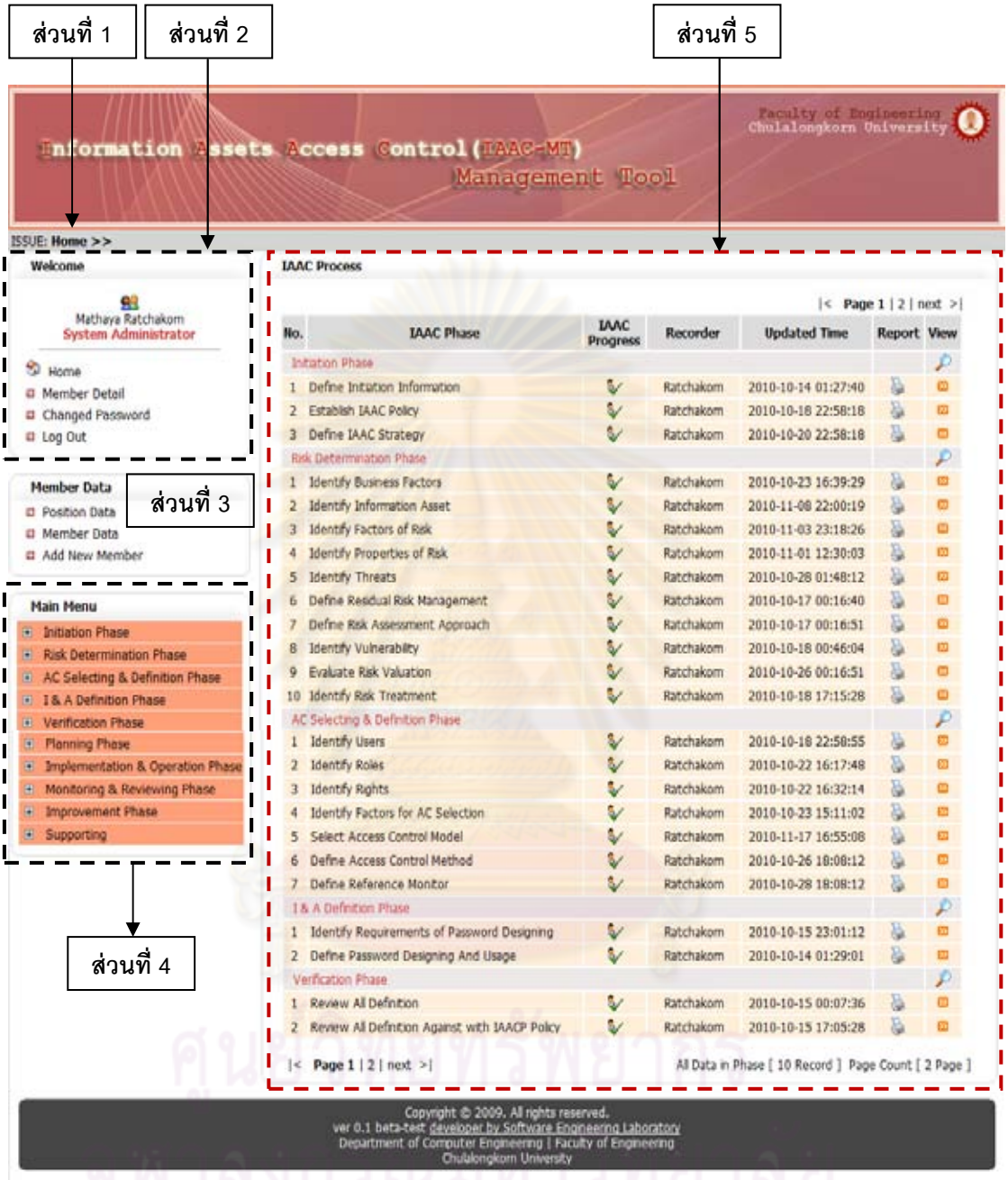
2.2) **ส่วนการควบคุมด้านตรรกะธุรกิจ** (Business Logic Control) เป็นส่วนควบคุมการทำงานของระบบให้เป็นไปตามตรรกะทางธุรกิจที่ได้ออกแบบไว้ เช่น ในการบันทึกข้อมูล ระบบต้องบังคับให้ผู้ใช้กรอกข้อมูลสำคัญอะไรบ้าง เป็นต้น

3) **ส่วนตรรกะธุรกิจ** (Model) เป็นส่วนการทำงานทางตรรกะธุรกิจให้เป็นไปตามหน้าที่การทำงานของระบบที่ได้ออกแบบไว้ ซึ่งมีส่วนประกอบได้แก่ Entity Object เป็นส่วนการเชื่อมต่อกับตารางในฐานข้อมูล Business Object เป็นส่วนการทำงานตามตรรกะธุรกิจ Error Handling เป็นส่วนการจัดการความผิดพลาดที่เกิดขึ้น Authentication เป็นส่วนการจัดการสิทธิการเข้าใช้งาน และ File Assess Management เป็นส่วนการบริหารจัดการการเข้าถึงแฟ้มข้อมูล

ประโยชน์ของการออกแบบสถาปัตยกรรมระบบนี้ คือ ในลักษณะของสถาปัตยกรรมเว็บเบสแอปพลิเคชัน ผู้ใช้งานระบบสามารถเข้าใช้งานจากเครื่องลูกข่ายในสถานที่ใดๆ ผ่านทางเว็บเบราว์เซอร์ ทำให้เกิดความคล่องตัวในการทำงาน สะดวกและง่ายต่อการบำรุงรักษาระบบ และในลักษณะของสถาปัตยกรรมซอฟต์แวร์ ระบบมีคุณลักษณะของการนำกลับไปใช้งานใหม่ หรือสามารถเพิ่มและแก้ไขเปลี่ยนแปลงระบบได้ง่ายขึ้น เช่น เมื่อองค์กรต้องการเปลี่ยนระบบฐานข้อมูล องค์กรเพียงแก้ไขส่วนการทำงานด้านข้อมูลที่ติดต่อไปยังโครงสร้างฐานข้อมูลตัวใหม่เท่านั้น ซึ่งจะทำให้ไม่กระทบต่อส่วนการทำงานหลักอื่นๆ

5.5 การออกแบบส่วนต่อประสานกับผู้ใช้ของเครื่องมือสนับสนุนกระบวนการ

การออกแบบส่วนต่อประสานกับผู้ใช้นั้น ผู้จัยได้พิจารณาโครงสร้างหน้าหลักของเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยแยกออกเป็น 5 ส่วน ดังรูปที่ 5.5



รูปที่ 5.5 โครงสร้างหน้าหลักของเครื่องมือสนับสนุนกระบวนการ

ส่วนที่ 1 เป็นส่วนที่แสดงเส้นทางที่ผู้ใช้กำลังใช้งานระบบ ซึ่งเริ่มต้นแสดงจากหน้าหลัก แล้วเรียงลำดับไปยังส่วนของโปรแกรมต่างๆ ที่ผู้ใช้กำลังใช้งานอยู่

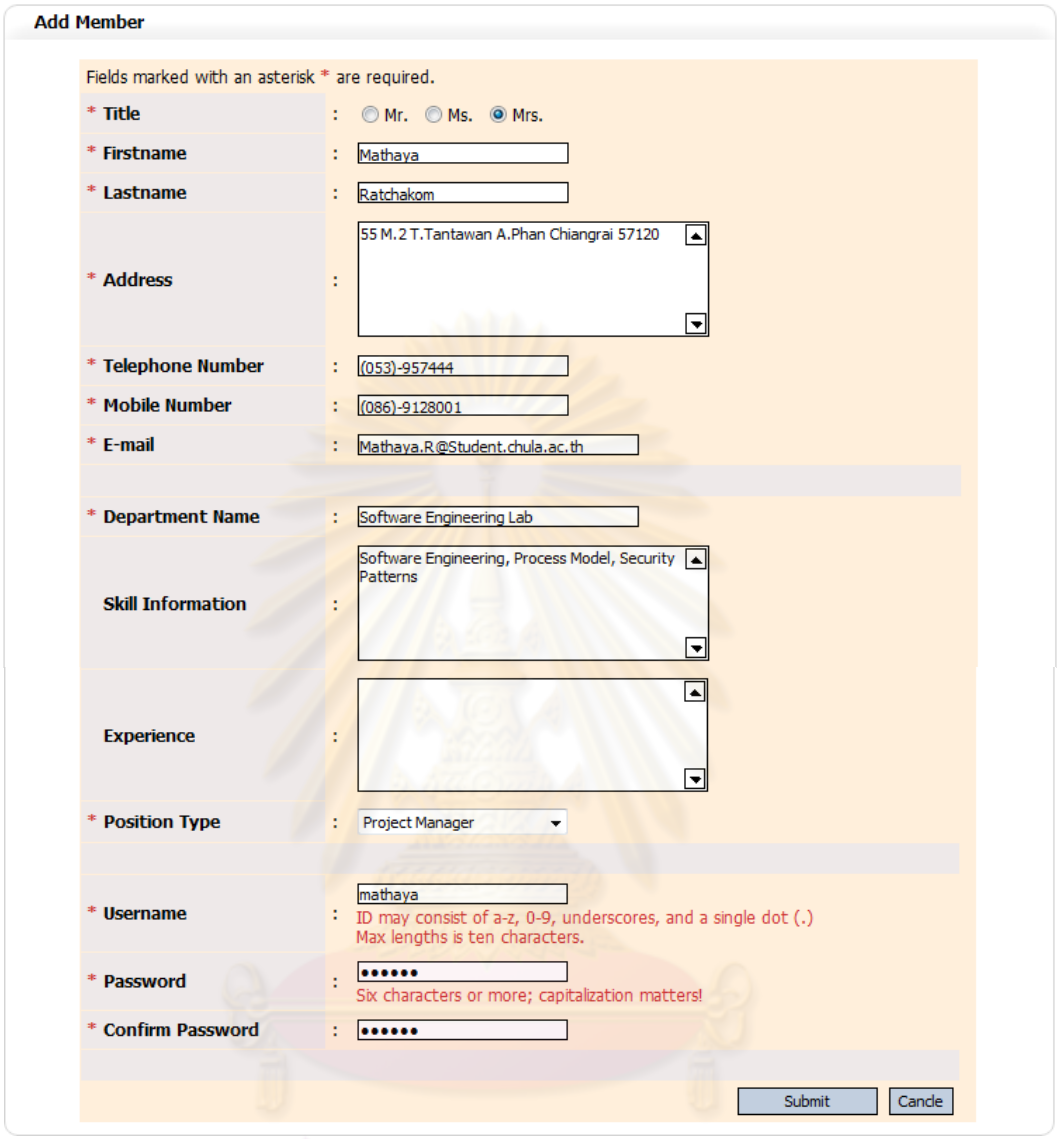
ส่วนที่ 2 เป็นส่วนที่แสดงชื่อ-นามสกุลและบทบาทของผู้ใช้ที่กำลังเข้าใช้งานระบบ รวมถึงเมนูข้อมูลส่วนบุคคลและการแก้ไขรหัสผ่าน

ส่วนที่ 3 เป็นส่วนที่แสดงเมนูของการจัดการบทบาทของผู้ใช้งานระบบ โดยสามารถกำหนดได้ว่าบทบาทใดสามารถเข้าใช้งานเมนูหลักและย่อยใดได้บ้าง ทั้งนี้ยังรวมถึงเมนูข้อมูลผู้ใช้งานทั้งหมดของระบบและการเพิ่มผู้ใช้งานใหม่

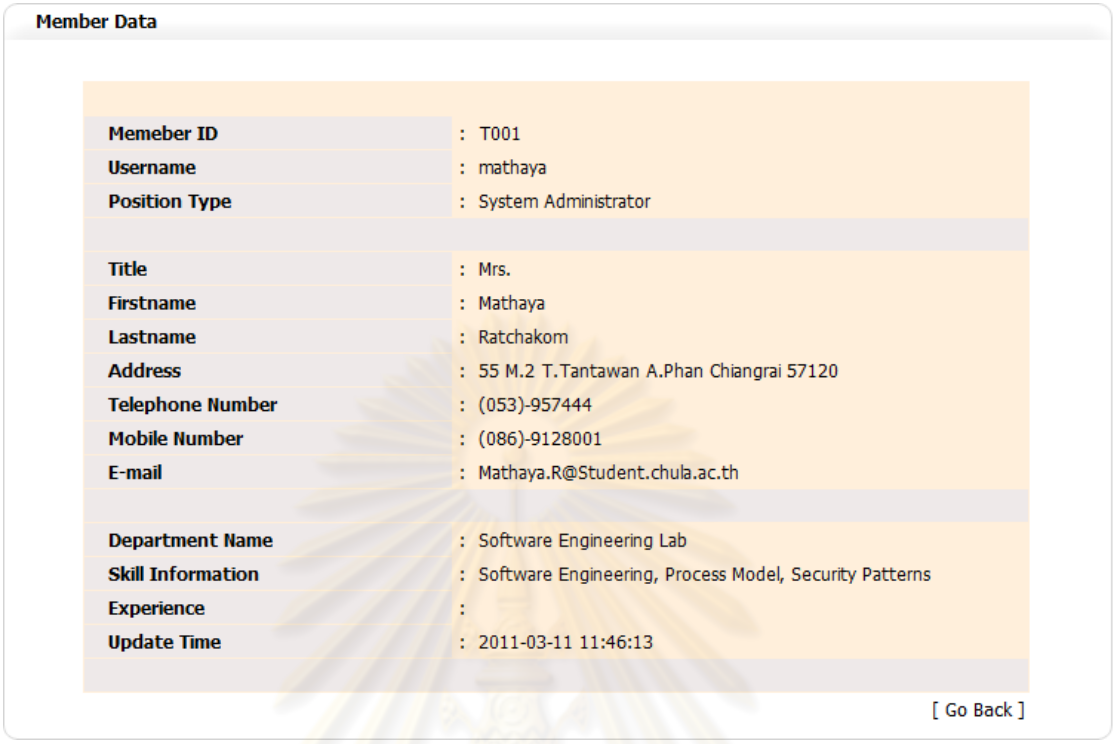
ส่วนที่ 4 เป็นส่วนที่แสดงเมนูหลักและภายในจะประกอบด้วยเมนูย่อยตามลำดับ โดยระบบจะเปิดการใช้งานเมนูตามลำดับขั้นตอนของการดำเนินงานกระบวนการ

ส่วนที่ 5 เป็นส่วนที่แสดงเนื้อหาหรือผลจากการทำงานของระบบ เช่น จากรูปที่ 5.7 แสดงถึงขั้นตอนการทำงานใดๆ ที่มีการจัดการข้อมูลเกิดขึ้น โดยแสดงด้วยนามสกุลผู้ใช้งานและวันเวลาของการทำงานนั้น

การแสดงข้อความเตือนให้ผู้ใช้งานได้ทราบถึงผลของการทำงานนั้น ผู้วิจัยได้พิจารณาส่วนต่อประสานกับผู้ใช้ โดยได้แบ่งการแสดงข้อความเตือนออกเป็น 2 กรณี คือ กรณีการทำงานปกติ และกรณีที่ผิดพลาด ในกรณีที่เครื่องมือทำงานได้ตามปกตินั้นระบบจะแสดงผลลัพธ์ภายหลังจากการทำงาน ดังแสดงได้ดังรูปที่ 5.6 และ 5.7

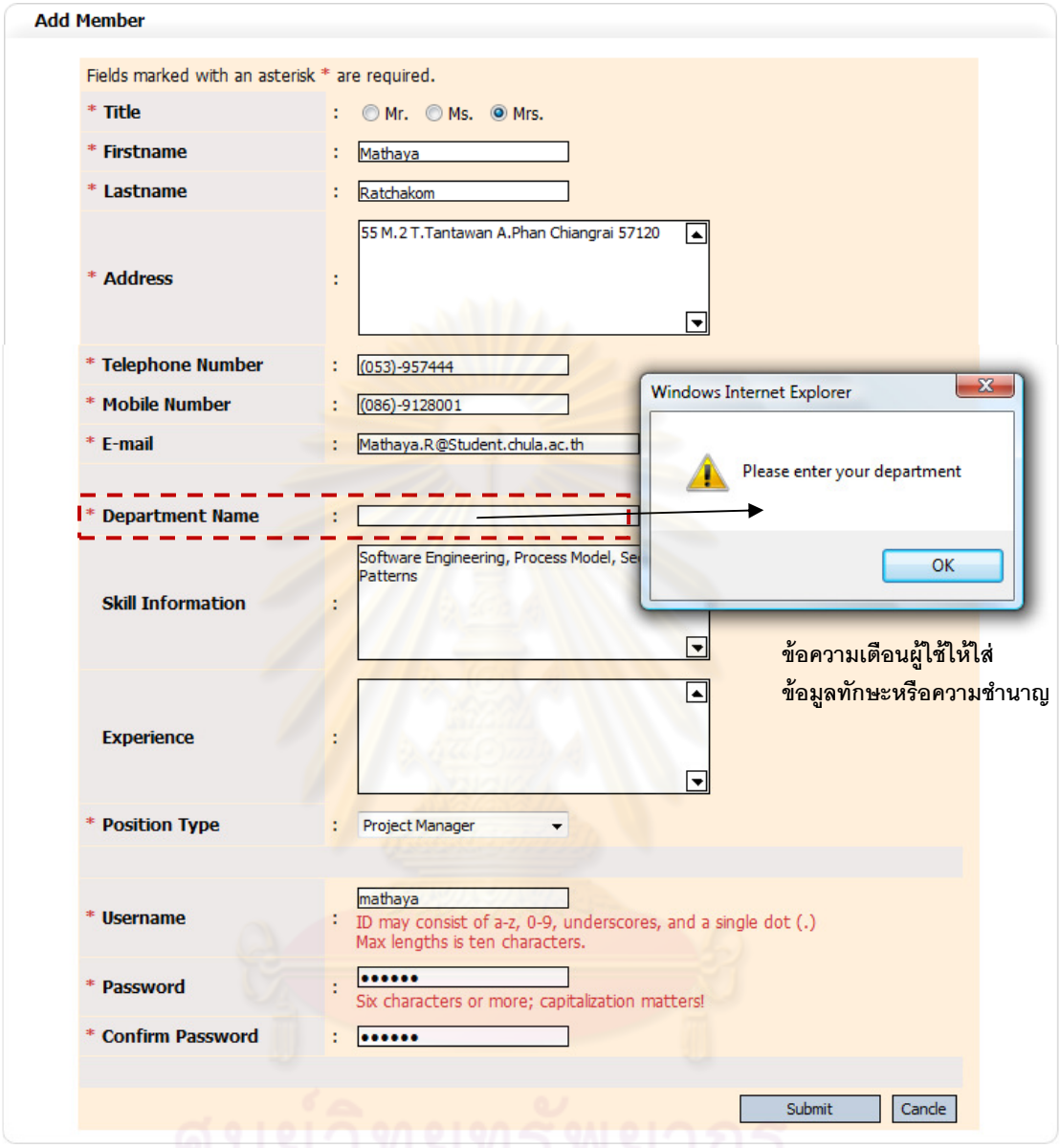


รูปที่ 5.6 หน้าจอการทำงานในกรณีปกติ



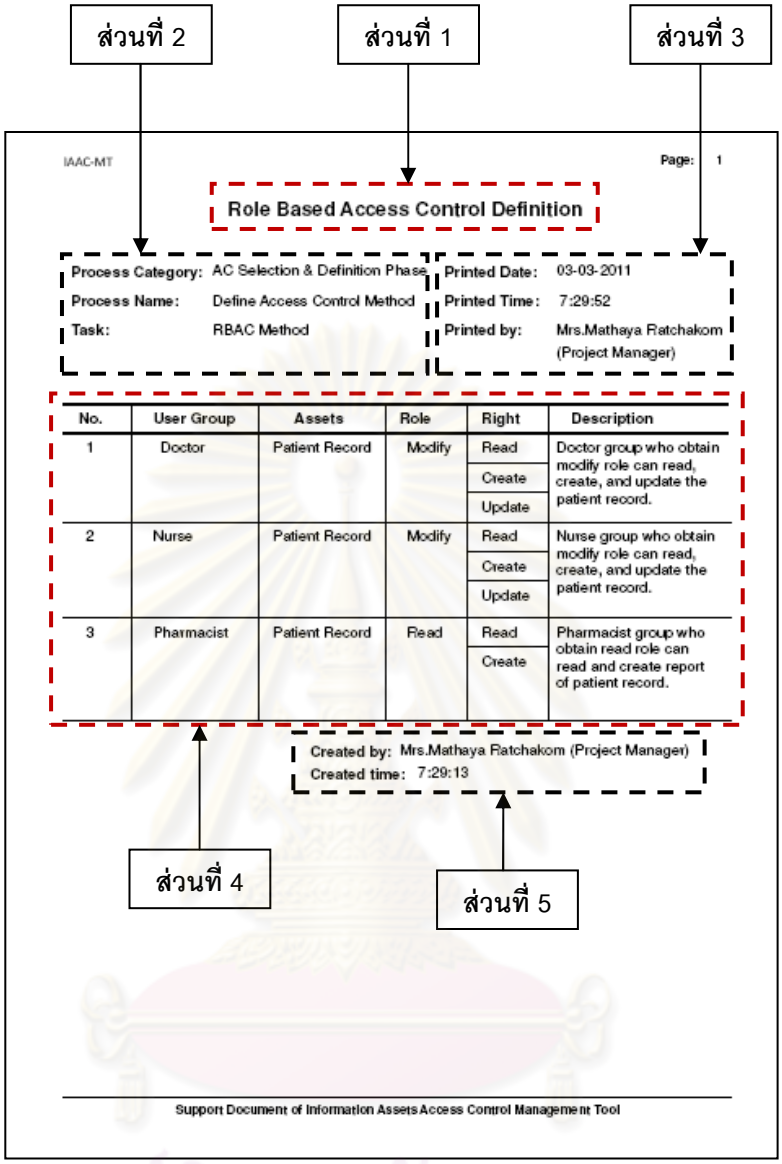
รูปที่ 5.7 หน้าจอผลลัพธ์ของการทำงานในกรณีปกติ

สำหรับกรณีที่การทำงานผิดพลาด เครื่องมือจะแสดงหน้าต่างข้อความเตือนของตำแหน่งที่ผิดพลาด โดยไม่อนุญาตให้มีการทำงานต่อไป เช่น กรณีที่ผู้ใช้งานไม่ได้กรอกข้อมูลทักษะ แล้วผู้ใช้ไม่ได้กรอกข้อมูล เครื่องมือจะแสดงข้อความเตือนตรงตำแหน่งที่ผู้ใช้ต้องกรอกข้อมูล เป็นต้น ดังแสดงได้ดังรูปที่ 5.8



รูปที่ 5.8 หน้าจอแสดงหน้าต่างข้อความเตือนในกรณีที่ผิดพลาด

นอกจากการออกแบบส่วนต่อประสานกับผู้ใช้ในส่วนของการเรียกดู บันทึก และปรับปรุงข้อมูลแล้วนั้น ผู้วิจัยยังได้ออกแบบส่วนต่อประสานกับผู้ใช้ในส่วนของการออกรายงานอีกด้วย เนื่องจากเครื่องมือสนับสนุนกระบวนการที่ได้พัฒนาขึ้นมานั้นมีการเก็บข้อมูลที่จำเป็นต่อการดำเนินการกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ และเพื่อเป็นประโยชน์ต่อโครงการอื่นๆ ที่ซึ่งมีความคล้ายคลึงกัน โดยโครงสร้างของการออกรายงานแบ่งออกเป็น 5 ส่วน สามารถแสดงได้ดังรูปที่ 5.9



รูปที่ 5.9 โครงสร้างส่วนต่อประสานกับผู้ใช้ในส่วนการออกรายงาน

ส่วนที่ 1 เป็นส่วนที่แสดงชื่อของรายงาน

ส่วนที่ 2 เป็นส่วนที่แสดงชื่อขั้นตอนการทำงานหลัก การทำงานย่อย และ/หรืองานที่ทำ

ส่วนที่ 3 เป็นส่วนที่แสดงชื่อของผู้ออกรายงาน วันที่และเวลาที่พิมพ์รายงาน

ส่วนที่ 4 เป็นส่วนที่แสดงรายละเอียดข้อมูลของรายงาน

ส่วนที่ 5 เป็นส่วนที่แสดงชื่อของผู้ที่บันทึกข้อมูล วันที่และเวลาที่บันทึกข้อมูลนั้น

บทที่ 6
การพัฒนาและทดสอบเครื่องมือสนับสนุนกระบวนการ

เมื่อทำการวิเคราะห์และออกแบบเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเสร็จเรียบร้อยแล้วนั้น ขั้นตอนถัดไปจะเป็นการพัฒนา ทดสอบและประเมินผลเครื่องมือสนับสนุนกระบวนการ โดยรายละเอียดภายในบทนี้จะประกอบด้วยเครื่องมือที่ใช้ในการพัฒนาเครื่องมือ ขั้นตอนของการพัฒนา การทดสอบและวิธีการประเมินผลเครื่องมือ

6.1 เครื่องมือที่ใช้ในการพัฒนาเครื่องมือสนับสนุนกระบวนการ

สำหรับเครื่องที่ใช้ในการพัฒนาเครื่องมือสนับสนุนกระบวนการนั้นได้แบ่งออกเป็น 2 กลุ่มหลัก ดังต่อไปนี้

6.1.1) ฮาร์ดแวร์ (Hardware) สามารถแบ่งแยกออกเป็น 3 กลุ่ม คือ เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาเครื่องมือสนับสนุนกระบวนการ เครื่องลูกข่ายและเครื่องแม่ข่าย โดยมีรายละเอียดดังนี้

1) เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาเครื่องมือสนับสนุนกระบวนการ

1.1) หน่วยประมวลผล อินเทลดูโอคอ ความเร็ว 1.8 กิกะเฮิรตซ์

1.2) หน่วยความจำหลัก 4 กิกะไบต์

1.3) ฮาร์ดดิสก์ ความจุ 120 กิกะไบต์

1.4) รองรับการโอนถ่ายข้อมูลเครือข่ายที่ความเร็ว 10/100 เมกกะบิตต่อวินาที

2) เครื่องคอมพิวเตอร์ลูกข่ายที่รองรับการประมวลผลของเครื่องมือสนับสนุนกระบวนการ

2.1) หน่วยประมวลผล อินเทล เพนเทียมโฟร์ ความเร็ว 2.0 กิกะเฮิรตซ์

2.2) หน่วยความจำหลัก 512 เมกกะไบต์

2.3) ฮาร์ดดิสก์ ความจุ 80 กิกะไบต์

2.4) รองรับการโอนถ่ายข้อมูลเครือข่ายที่ความเร็ว 10/100 เมกกะบิตต่อวินาที

3) เครื่องคอมพิวเตอร์แม่ข่ายที่รองรับการให้บริการ การประมวลผลด้านตรรกะทางธุรกิจและฐานข้อมูล

3.1) หน่วยประมวลผล อินเทล เพนเทียมโฟร์ ความเร็ว 2.4 กิกะเฮิรตซ์

3.2) หน่วยความจำหลัก 512 เมกกะไบต์

3.3) ฮาร์ดดิสก์ ความจุ 100 กิกะไบต์

3.4) รองรับการโอนถ่ายข้อมูลเครือข่ายที่ความเร็ว 10/100 เมกกะบิตต่อวินาที

6.1.2) **ซอฟต์แวร์** (Software) ได้จำแนกตามลักษณะการใช้งานในช่วงของการพัฒนาเครื่องมือสนับสนุนกระบวนการ โดยสามารถแบ่งแยกออกเป็น 4 กลุ่มหลัก โดยมีรายละเอียดดังนี้

1) ระบบปฏิบัติการ

1.1) วินโดวส์ วิสต้า โปรเฟสชันแนล สำหรับเครื่องคอมพิวเตอร์พัฒนาระบบ

1.2) วินโดวส์ 2003 เซิร์ฟเวอร์ขึ้นไป สำหรับเครื่องแม่ข่ายที่รองรับการให้บริการและประมวลผลด้านตรรกะทางธุรกิจ

1.3) วินโดวส์ 2003 เซิร์ฟเวอร์ขึ้นไป สำหรับเครื่องแม่ข่ายที่รองรับการให้บริการและประมวลผลฐานข้อมูล

1.4) วินโดวส์ 2003 เซิร์ฟเวอร์ขึ้นไป สำหรับเครื่องลูกข่าย

2) เครื่องมือที่ใช้ในการออกแบบเครื่องมือและจัดทำเอกสารประกอบ

2.1) สตาร์ ยูเอ็มแอล โอเพ็นซอสล์ 5.0

2.2) ไมโครซอฟท์ วิซีโอ โปรเฟสชันแนล 2007

2.3) อะโดบี อะโครแบท 8.0

2.4) ไมโครซอฟท์ออฟฟิศ 2007

3) เครื่องมือที่ใช้ในการพัฒนาส่วนต่อประสานกับผู้ใช้

3.1) เว็บเบราว์เซอร์ เอ็กซ์โพลเรอร์ 8

3.2) มาโครมีเดียดรีมวีเวอร์ ซีเอส 3

3.3) อะโดบี โฟโตชอป ซีเอส 3

4) เครื่องมือที่ใช้ในการพัฒนาส่วนให้บริการด้านตรรกะทางธุรกิจและฐานข้อมูล

4.1) เว็บเซิร์ฟเวอร์ อาปาเช เวอร์ชัน 2.2.8

4.2) พีเอชพี สคริปท์ เวอร์ชั่น 5.2.6

4.3) จาวา สคริปท์ เวอร์ชั่น 1.2

4.2) ฐานข้อมูลเชิงสัมพันธ์ มายเอสคิวแอล 5.0.51b

4.3) โปรแกรมจัดการฐานข้อมูลสัมพันธ์ พีเอชพี มายด์แอ็ดมิน เวอร์ชัน 2.10.3

4.4) มาโครมีเดียดรีมวีเวอร์ ซีเอส 3

4.5) เว็บเบราว์เซอร์ เอ็กซ์โพลเรอร์ 8

6.2 ขั้นตอนของการพัฒนาเครื่องมือสนับสนุนกระบวนการ

ในการพัฒนาเครื่องมือสนับสนุนกระบวนการ ผู้วิจัยได้เลือกใช้ภาษาโปรแกรมในการพัฒนา คือ ภาษาโปรแกรมพีเอชพีและจาวาสคริปท์ เนื่องจากเครื่องมือมีสถาปัตยกรรมเป็นแบบเว็บเบสแอปพลิเคชัน ซึ่งภาษาโปรแกรมทั้งสองมีคุณสมบัติและลักษณะสนับสนุนสถาปัตยกรรมดังกล่าว โดยขั้นตอนของการพัฒนาเครื่องมือสนับสนุนกระบวนการ มี 4 ขั้นตอนหลัก ดังต่อไปนี้

6.2.1) **พัฒนาหน้าจอต้นแบบ** โดยพัฒนาให้แสดงถึงภาพรวมและหน้าที่การทำงานของเครื่องมือสนับสนุนกระบวนการทั้งหมด ทั้งรูปแบบโครงสร้างของส่วนต่อประสานกับผู้ใช้ในแต่ละหน้าจอการทำงาน รวมถึงข้อมูลนำเข้าและออกที่เกิดขึ้นในแต่ละหน้าที่การทำงาน ซึ่งข้อดีของการพัฒนาในส่วนนี้ คือ ผู้พัฒนาได้เข้าใจถึงโครงสร้างและองค์ประกอบโดยรวมของเครื่องมือสนับสนุนกระบวนการ โดยจะทำให้ง่ายต่อการพัฒนาในส่วนอื่นๆ ต่อไป

6.2.2) **พัฒนาระบบฐานข้อมูล** ส่วนนี้ผู้วิจัยได้สร้างฟิลด์ของแต่ละตาราง และความสัมพันธ์ระหว่างกันของตารางบนระบบฐานข้อมูลมายเอสคิวแอล โดยมีเครื่องมือในการจัดการเป็นพีเอชพี มายด์แอ็ดมิน ซึ่งจะเห็นได้จากแบบจำลองเชิงกายภาพที่ได้ออกแบบไว้ในบทที่ 5 หัวข้อที่ 5.3 การออกแบบฐานข้อมูลสัมพันธ์ของเครื่องมือสนับสนุนกระบวนการ

6.2.3) **พัฒนาส่วนการตรวจสอบข้อมูลด้วยจาวาสคริปท์** ผู้วิจัยได้สร้างจาวาสคริปท์เป็นส่วนประกอบหนึ่งของเครื่องมือสนับสนุนกระบวน เพื่อใช้การตรวจสอบความถูกต้องของข้อมูลก่อนบันทึกหรือการเปลี่ยนแปลงแก้ไขข้อมูลในแต่ละตารางบนระบบฐานข้อมูลที่ได้พัฒนา รวมถึงส่วนการแสดงผลของการกระทำบางส่วน เช่น การแสดงเมนูหลักและเมนูย่อยของเครื่องมือ เป็นต้น

6.2.4) **พัฒนาส่วนการทำงานหลักด้วยพีเอชพี** ผู้วิจัยได้ใช้โปรแกรมภาษาพีเอชพีเป็นหลักของการพัฒนาเครื่องมือสนับสนุนกระบวนการในครั้งนี้ โดยจะพัฒนาเป็นส่วนนำเข้าและนำออกข้อมูลไปแสดงผลบนหน้าจอตามโครงสร้างของส่วนต่อประสานกับผู้ใช้ที่ได้ออกแบบไว้ ควบคุมการไหลของการแสดงผลการทำงานในแต่ละหน้าที่การทำงาน รวมถึงควบคุมการทำงาน

ของจาวาสคริปท์ที่ได้สร้างขึ้น เพื่อให้เกิดการทำงานที่สอดคล้องต้องกันกับตรรกะทางธุรกิจที่ได้กำหนดไว้ เช่น ก่อนการบันทึกข้อมูลลงฐานข้อมูลมายเอสคิวแอลนั้นจะต้องเรียกให้จาวาสคริปท์ตรวจสอบความถูกต้องและครบถ้วนของข้อมูล ถ้าหากมีข้อผิดพลาดเกิดขึ้นจาวาสคริปท์จะแสดงผลข้อความเตือนข้อผิดพลาดตามที่ได้ตรวจสอบไว้

6.3 การทดสอบเครื่องมือสนับสนุนกระบวนการ

ในการทดสอบเครื่องมือสนับสนุนกระบวนที่พัฒนาขึ้นนั้น จะใช้วิธีการทดสอบแบบกล่องดำ (Black Box Testing) ซึ่งข้อมูลที่ใช้ในการทดสอบได้จำลองขึ้นให้มีลักษณะใกล้เคียงกับข้อมูลจริงของระบบมากที่สุด และในการทดสอบครั้งนี้ได้ครอบคลุมทั้งการทดสอบความต้องการเชิงหน้าที่และที่มิใช่หน้าที่ สำหรับกรณีทดสอบที่นำมาใช้ในการทดสอบเครื่องมือสนับสนุนกระบวนการนั้น ผู้วิจัยได้เริ่มต้นจากการพิจารณาเป้าหมายและผลลัพธ์ที่คาดหวังไว้ตามความต้องการของเครื่องมือ โดยกำหนดข้อมูลทดสอบและบันทึกผลการทดสอบของการเพิ่มข้อมูลผู้ใช้เข้าสู่ระบบและการเปลี่ยนรหัสผ่าน ซึ่งเป็นการทดสอบความต้องการเชิงหน้าที่ ดังตารางที่ 6.1 - 6.6 การกำหนดสิทธิของการเข้าใช้งานระบบและการแสดงเส้นทางของการใช้งาน ซึ่งเป็นการทดสอบความต้องการไม่ใช่เชิงหน้าที่ ดังตารางที่ 6.7 - 6.12

ตารางที่ 6.1 ตัวอย่างกรณีทดสอบของการเพิ่มข้อมูลผู้ใช้เข้าสู่ระบบ

ชื่อหน้าที่การทำงานหลัก	การจัดการข้อมูลผู้ใช้งานระบบ
เลขที่กรณีทดสอบ	TF001
ชื่อกรณีทดสอบ	การเพิ่มข้อมูลผู้ใช้งานระบบ
วัตถุประสงค์การทดสอบ	เพื่อทดสอบการเพิ่มข้อมูลผู้ใช้งานเข้าสู่ระบบ
บทบาทผู้ใช้งานที่เกี่ยวข้อง	ผู้ดูแลระบบ
ข้อมูลนำเข้า	1. คำนำหน้าชื่อ 2. ชื่อ 3. นามสกุล 4. ที่อยู่ 5. หมายเลขโทรศัพท์ 6. หมายเลขโทรศัพท์มือถือ 7. อีเมล 8. หน่วยงาน 9. ข้อมูลทักษะหรือความชำนาญ 10. ข้อมูลประสบการณ์ 11. บทบาทภายในระบบ 12. ชื่อผู้ใช้งานระบบ 13. รหัสผ่าน 14. การยืนยันรหัสผ่าน
ผลลัพท์ที่คาดหวัง (กรณีปกติ)	ระบบแสดงหน้าต่างข้อความให้ผู้ใช้งานทราบว่าข้อมูลที่กรอกจากหน้าจอการเพิ่มข้อมูลผู้ใช้ ถูกเก็บลงในฐานข้อมูลอย่างครบถ้วน
ผลลัพท์ที่คาดหวัง (กรณีผิดพลาด)	กรณีผู้ใช้กรอกข้อมูลไม่ครบถ้วน หน้าจอจะแสดงหน้าต่างข้อความเตือนให้ผู้ใช้กรอกข้อมูลในฟิลด์นั้นๆ
ข้อมูลทดสอบ	กรณีปกติ แสดงดังตารางที่ 6.2 กรณีผิดพลาด แสดงดังตารางที่ 6.3
ผลการทดสอบ	เครื่องมือสามารถทำงานในกรณีปกติได้ถูกต้องครบถ้วน ดังรูปที่ 6.1- 6.3 และในกรณีที่ผิดพลาด เครื่องมือจะแสดงข้อความเตือนความผิดพลาดที่เกิดขึ้นได้ดังรูปที่ 6.4
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
หมายเหตุ	……..…….....

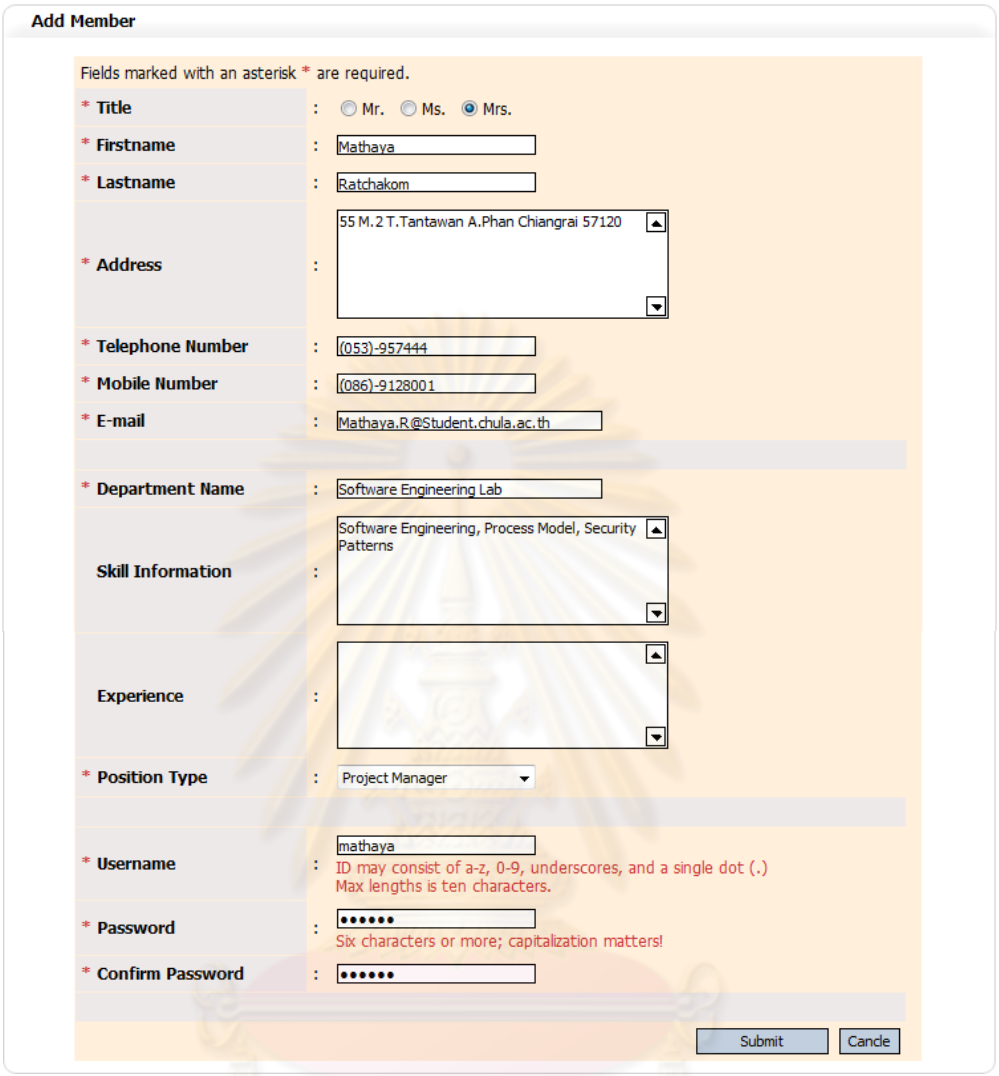
ตารางที่ 6.2 ข้อมูลทดสอบของกรณีทดสอบที่ TF001 (กรณีปกติ)

ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. คำนำหน้าชื่อ	บังคับ	Mrs.
2. ชื่อ	บังคับ	Mathaya
3. นามสกุล	บังคับ	Ratchakom
4. ที่อยู่	บังคับ	55 M.2 T.Tantawan A.Phan Chiangrai 57120
5. หมายเลขโทรศัพท์	บังคับ	(053)-957444
6. หมายเลขโทรศัพท์มือถือ	บังคับ	(086)-9128001
7. อีเมลล์	บังคับ	Mathaya.R@Student.chula.ac.th
8. หน่วยงาน	บังคับ	Software Engineering Team
9. ข้อมูลทักษะหรือความชำนาญ	ไม่บังคับ	Software Engineering, Process Model, Security Patterns
10. ข้อมูลประสบการณ์	ไม่บังคับ	-
11. บทบาทภายในระบบ	บังคับ	Project Management
12. ชื่อผู้ใช้งานระบบ	บังคับ	mathaya
13. รหัสผ่าน	บังคับ	******
14. การยืนยันรหัสผ่าน	บังคับ	******

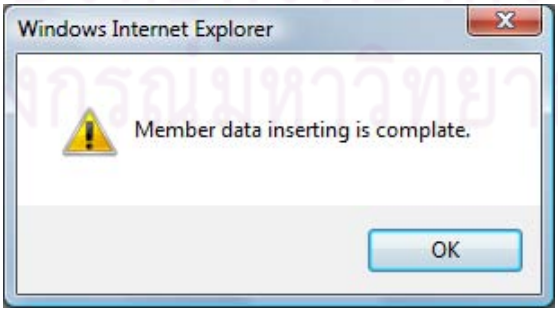
ตารางที่ 6.3 ข้อมูลทดสอบของกรณีทดสอบที่ TF001 (กรณีผิดพลาด)

ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. คำนำหน้าชื่อ	บังคับ	Mrs.
2. ชื่อ	บังคับ	Mathaya
3. นามสกุล	บังคับ	Ratchakom
4. ที่อยู่	บังคับ	55 M.2 T.Tantawan A.Phan Chiangrai 57120
5. หมายเลขโทรศัพท์	บังคับ	(053)-957444
6. หมายเลขโทรศัพท์มือถือ	บังคับ	(086)-9128001
7. อีเมล	บังคับ	Mathaya.R@Student.chula.ac.th
8. หน่วยงาน	บังคับ	ผู้ใช้ไม่กรอกข้อมูล
9. ข้อมูลทักษะหรือความชำนาญ	ไม่บังคับ	Software Engineering, Process Model, Security Patterns
10. ข้อมูลประสบการณ์	ไม่บังคับ	-
11. บทบาทภายในระบบ	บังคับ	Project Management
12. ชื่อผู้ใช้งานระบบ	บังคับ	mathaya
13. รหัสผ่าน	บังคับ	******
14. การยืนยันรหัสผ่าน	บังคับ	******

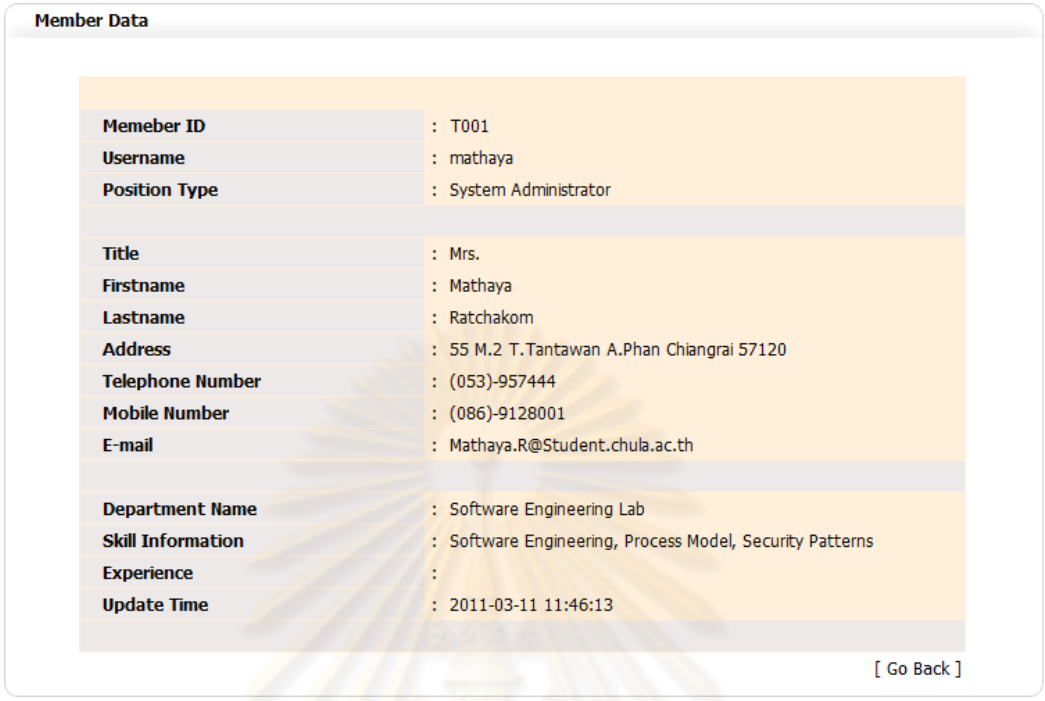
ในกรณีที่การทำงานปกติ หน้าจอของเครื่องมือจะแสดงผลการทำงานดังรูปที่ 6.1- 6.3 และในกรณีที่ผิดพลาด หน้าจอของเครื่องมือจะแสดงผลการทำงานดังรูปที่ 6.4



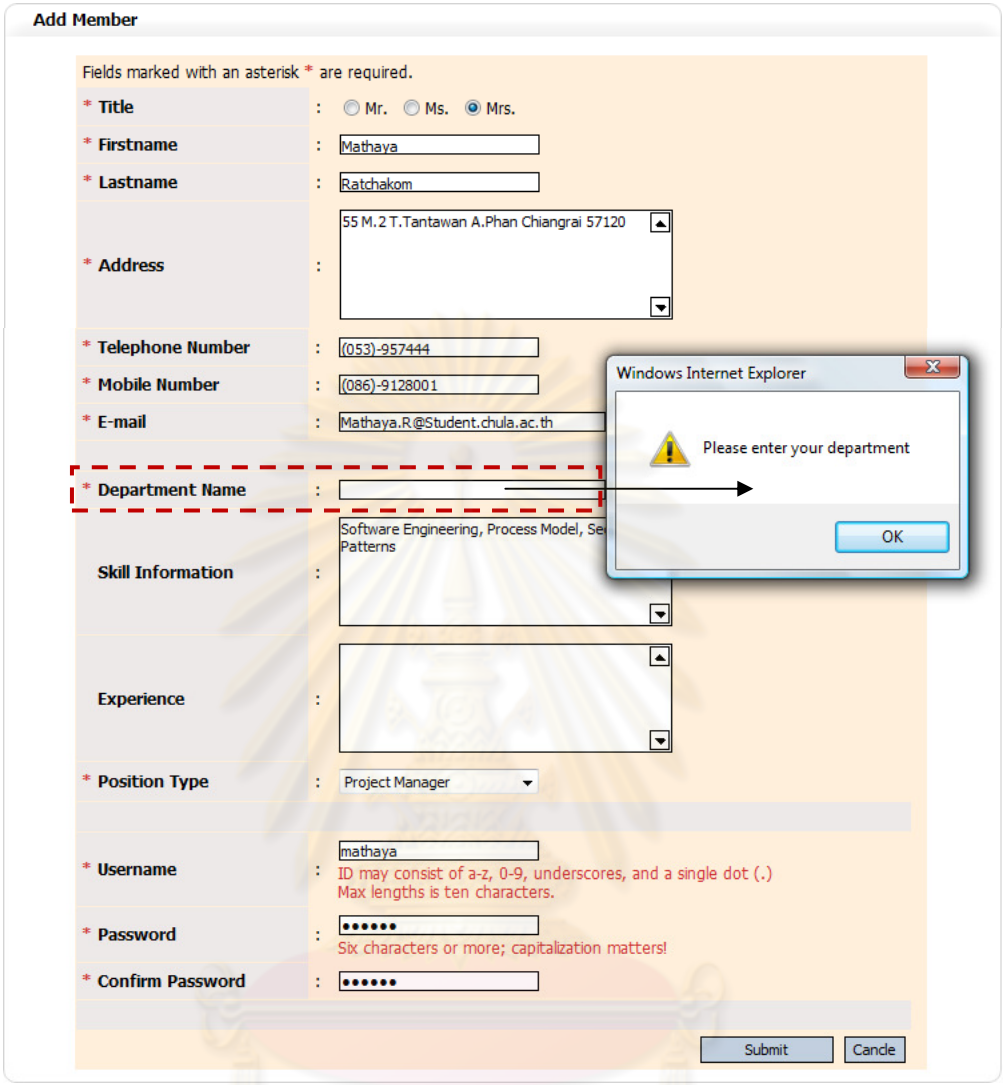
รูปที่ 6.1 หน้าจอแสดงการกรอกข้อมูลของผู้ใช้งานที่ครบถ้วนตามเงื่อนไข (กรณีปกติ)



รูปที่ 6.2 หน้าต่างข้อความแสดงการกรอกข้อมูลผู้ใช้งานที่ครบถ้วน (กรณีปกติ)



รูปที่ 6.3 หน้าจอแสดงผลการบันทึกข้อมูลของผู้ใช้งาน (กรณีปกติ)



รูปที่ 6.4 หน้าจอแสดงการกรอกข้อมูลของผู้ใช้งานที่ไม่ครบถ้วนตามเงื่อนไข (กรณีผิดพลาด)

ตารางที่ 6.4 ตัวอย่างกรณีทดสอบของการเปลี่ยนรหัสผ่าน

ชื่อหน้าที่การทำงานหลัก	การจัดการข้อมูลส่วนบุคคล
เลขที่กรณีทดสอบ	TF002
ชื่อกรณีทดสอบ	การเปลี่ยนรหัสผ่าน
วัตถุประสงค์การทดสอบ	เพื่อทดสอบการเปลี่ยนแปลงข้อมูลรหัสผ่านของผู้ใช้งาน
บทบาทผู้ใช้งานที่เกี่ยวข้อง	ผู้ใช้งานระบบ
ข้อมูลนำเข้า	1. ชื่อผู้ใช้งานระบบ 2. รหัสผ่าน 3. การยืนยันรหัสผ่าน
ผลลัพท์ที่คาดหวัง (กรณีปกติ)	ระบบแสดงหน้าต่างข้อความให้ผู้ใช้งานทราบว่าข้อมูลรหัสผ่านที่ต้องการเปลี่ยนแปลงถูกเก็บลงในฐานข้อมูลอย่างถูกต้องและครบถ้วน
ผลลัพท์ที่คาดหวัง (กรณีผิดพลาด)	กรณีผู้ใช้กรอกข้อมูลไม่เป็นไปตามเงื่อนไข หน้าจอจะแสดงหน้าต่างข้อความเตือนให้ผู้ใช้กรอกข้อมูลในฟิลด์นั้นๆ ใหม่
ข้อมูลทดสอบ	กรณีปกติ แสดงดังตารางที่ 6.5 กรณีผิดพลาด แสดงดังตารางที่ 6.6
ผลการทดสอบ	เครื่องมือสามารถทำงานในกรณีปกติได้ถูกต้องครบถ้วน ดังรูปที่ 6.5 และ 6.6 และในกรณีที่ผิดพลาด เครื่องมือจะแสดงข้อความเตือนความผิดพลาดที่เกิดขึ้นได้ ดังรูปที่ 6.7
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
หมายเหตุ	……

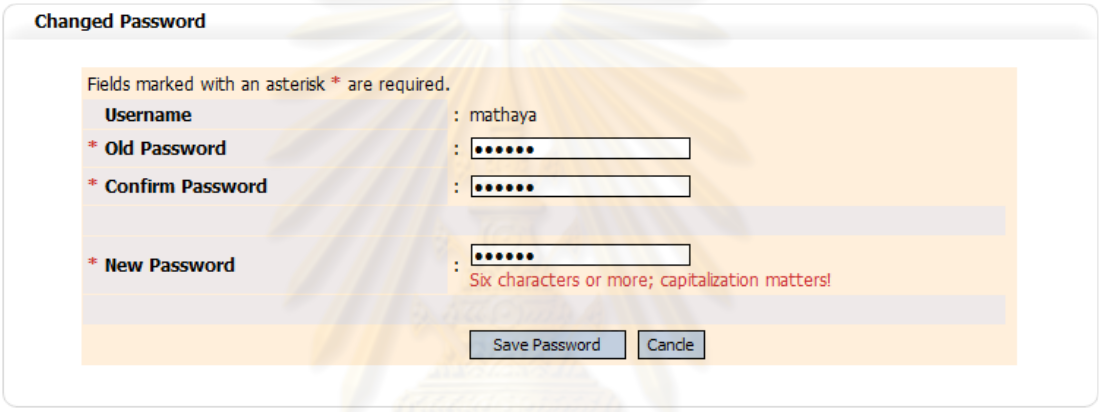
ตารางที่ 6.5 ข้อมูลทดสอบของกรณีทดสอบที่ TF002 (กรณีปกติ)

ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. ชื่อผู้ใช้งานระบบ	บังคับ	mathaya
2. รหัสผ่าน	บังคับ	******
3. การยืนยันรหัสผ่าน	บังคับ	******

ตารางที่ 6.6 ข้อมูลทดสอบของกรณีทดสอบที่ TF002 (กรณีผิดพลาด)

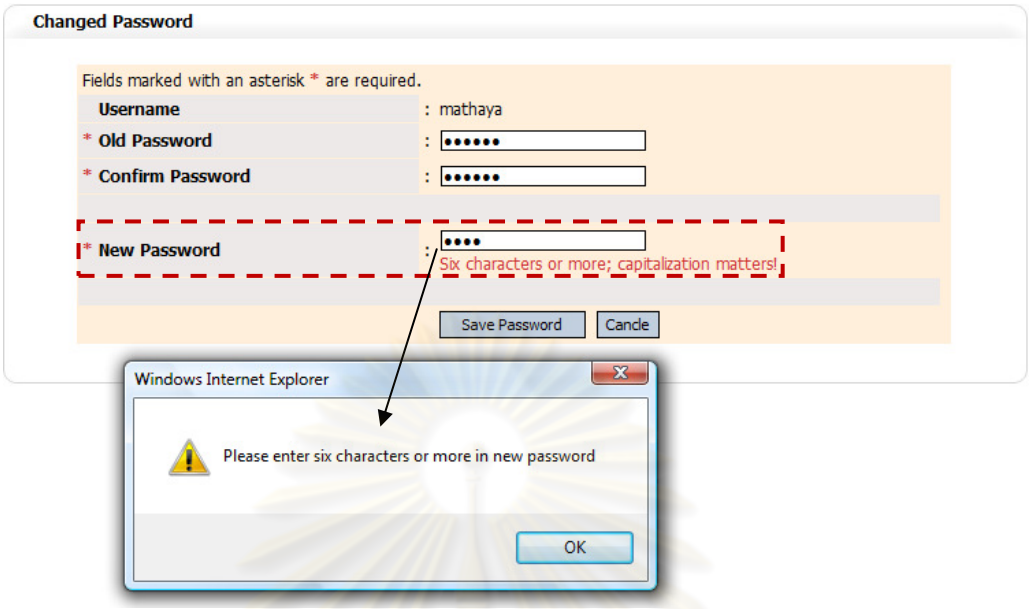
ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. ชื่อผู้ใช้งานระบบ	บังคับ	mathaya
2. รหัสผ่าน	บังคับ	******
3. การยืนยันรหัสผ่าน	บังคับ	**** (ข้อมูลไม่เป็นไปตามเงื่อนไข)

ในกรณีที่การทำงานปกติ หน้าจอของเครื่องมือจะแสดงผลการทำงานดังรูปที่ 6.5 - 6.6 และในกรณีที่ผิดพลาด หน้าจอของเครื่องมือจะแสดงผลการทำงานดังรูปที่ 6.7



รูปที่ 6.5 หน้าจอแสดงการเปลี่ยนรหัสผ่านที่ครบถ้วนตามเงื่อนไข (กรณีปกติ)

รูปที่ 6.6 หน้าต่างข้อความแสดงการเปลี่ยนรหัสผ่านที่ครบถ้วน (กรณีปกติ)



รูปที่ 6.7 หน้าจอแสดงการกรอกข้อมูลรหัสผ่านใหม่ที่ไม่เป็นไปตามเงื่อนไข (กรณีผิดพลาด)

ตารางที่ 6.7 ตัวอย่างกรณีทดสอบของการกำหนดสิทธิของการเข้าใช้งานระบบ

ชื่อหน้าที่การทำงานหลัก	ความมั่นคงของระบบ
เลขที่กรณีทดสอบ	TN01
ชื่อคุณลักษณะที่จะทดสอบ	การกำหนดสิทธิของการเข้าใช้งานระบบ
วัตถุประสงค์การทดสอบ	เพื่อทดสอบสิทธิของการเข้าใช้งานระบบ
ข้อมูลนำเข้า	1. ชื่อผู้ใช้งานระบบ 2. รหัสผ่าน
ผลลัพท์ที่คาดหวัง (กรณีปกติ)	ผู้ใช้งานของระบบเท่านั้นที่จะสามารถใช้งานระบบได้ (ในกรณีของบทบาทผู้ดูแลระบบและบทบาทผู้จัดการโครงการ)
ผลลัพท์ที่คาดหวัง (กรณีผิดพลาด)	กรณีที่ไม่ใช่ผู้ใช้งานระบบ หน้าจอจะแสดงหน้าต่างข้อความเตือนว่าไม่สามารถเข้าใช้งานระบบได้ แล้วกลับสู่หน้าจอการเข้าใช้งานใหม่อีกครั้ง
ข้อมูลทดสอบ	1. กรณีที่ผู้ใช้งานมีบทบาทเป็นผู้ดูแลระบบ แสดงดังตารางที่ 6.8 2. กรณีที่ผู้ใช้งานมีบทบาทเป็นผู้จัดการโครงการ แสดงดังตารางที่ 6.9 3. กรณีที่ไม่ใช่ผู้ใช้งานระบบ แสดงดังตารางที่ 6.10
ผลการทดสอบ	เครื่องมือสามารถทำงานในกรณีปกติได้ถูกต้องครบถ้วน ดังรูปที่ 6.8 - 6.11 และในกรณีที่ผิดพลาด เครื่องมือจะแสดงข้อความเตือนความผิดพลาดที่เกิดขึ้นได้ ดังรูปที่ 6.12 - 6.13
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
หมายเหตุ	.....

ตารางที่ 6.8 ข้อมูลทดสอบของกรณีทดสอบที่ TN01 (กรณีปกติ)

ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. ชื่อผู้ใช้งานระบบ	บังคับ	admin (ผู้ดูแลระบบ)
2. รหัสผ่าน	บังคับ	******

ตารางที่ 6.9 ข้อมูลทดสอบของกรณีทดสอบที่ TN01 (กรณีปกติ)

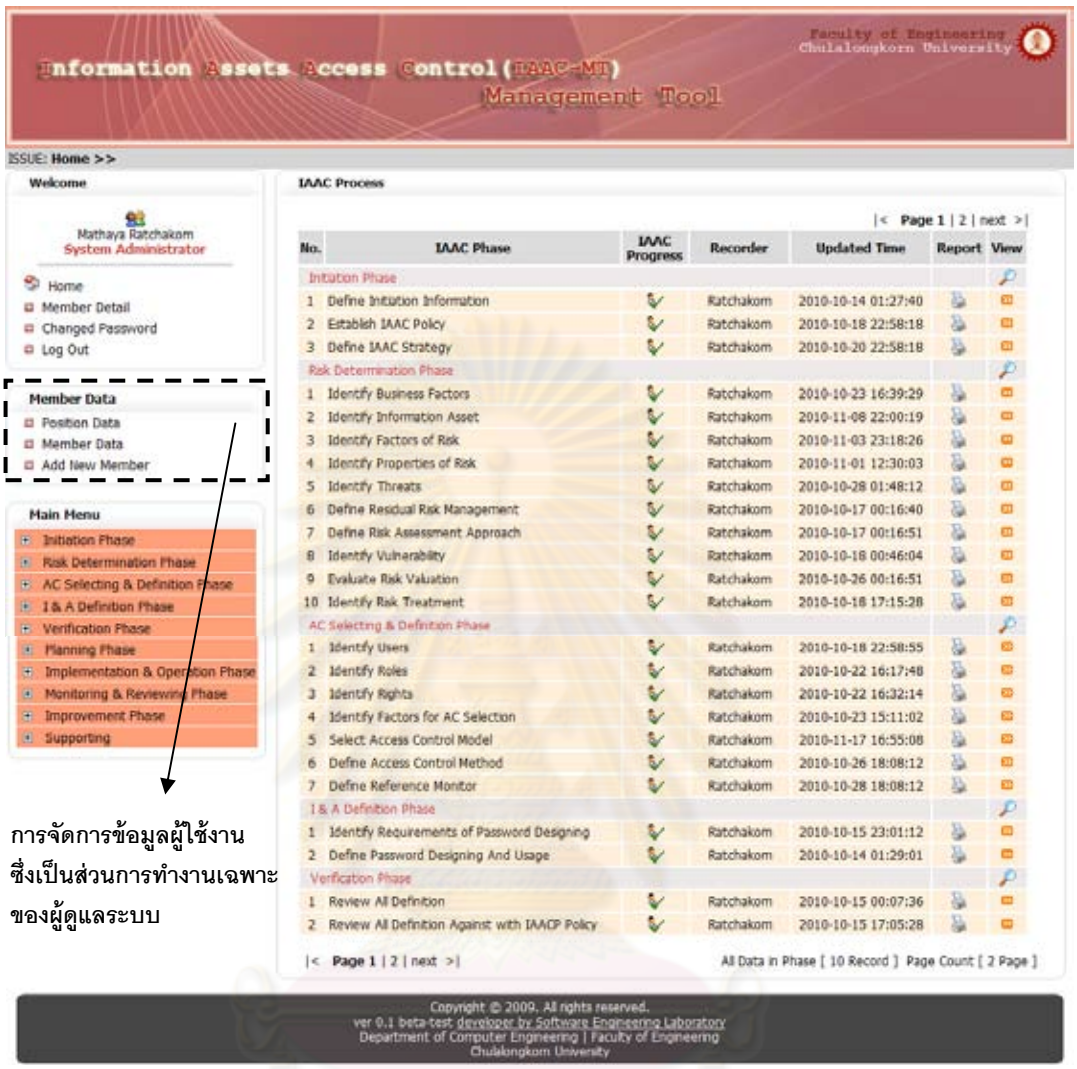
ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. ชื่อผู้ใช้งานระบบ	บังคับ	mathaya (ผู้จัดการโครงการ)
2. รหัสผ่าน	บังคับ	******

ตารางที่ 6.10 ข้อมูลทดสอบของกรณีทดสอบที่ TN01 (กรณีผิดพลาด)

ข้อมูลนำเข้า	การบังคับข้อมูล	ตัวอย่างข้อมูล
1. ชื่อผู้ใช้งานระบบ	บังคับ	abcd (ไม่ใช่ผู้ใช้งานระบบ)
2. รหัสผ่าน	บังคับ	******

ในการเข้าใช้งานระบบนั้น จะต้องทำการระบุและพิสูจน์ก่อนว่า เป็นบุคคลที่ได้รับอนุญาตให้เข้าใช้งานหรือไม่ และต้องพิจารณาด้วยว่า มีบทบาทเป็นอะไรภายในระบบ ดังรูปที่ 6.8 - 6.11 กรณีที่ผู้ใช้งานมีบทบาทเป็นผู้ดูแลระบบและผู้จัดการโครงการ และสำหรับรูปที่ 6.12 - 6.13 กรณีที่ไม่ใช่ผู้ใช้งานของระบบ

รูปที่ 6.8 หน้าจอแสดงการเข้าใช้งานระบบในบทบาทผู้ดูแลระบบ (กรณีปกติ)

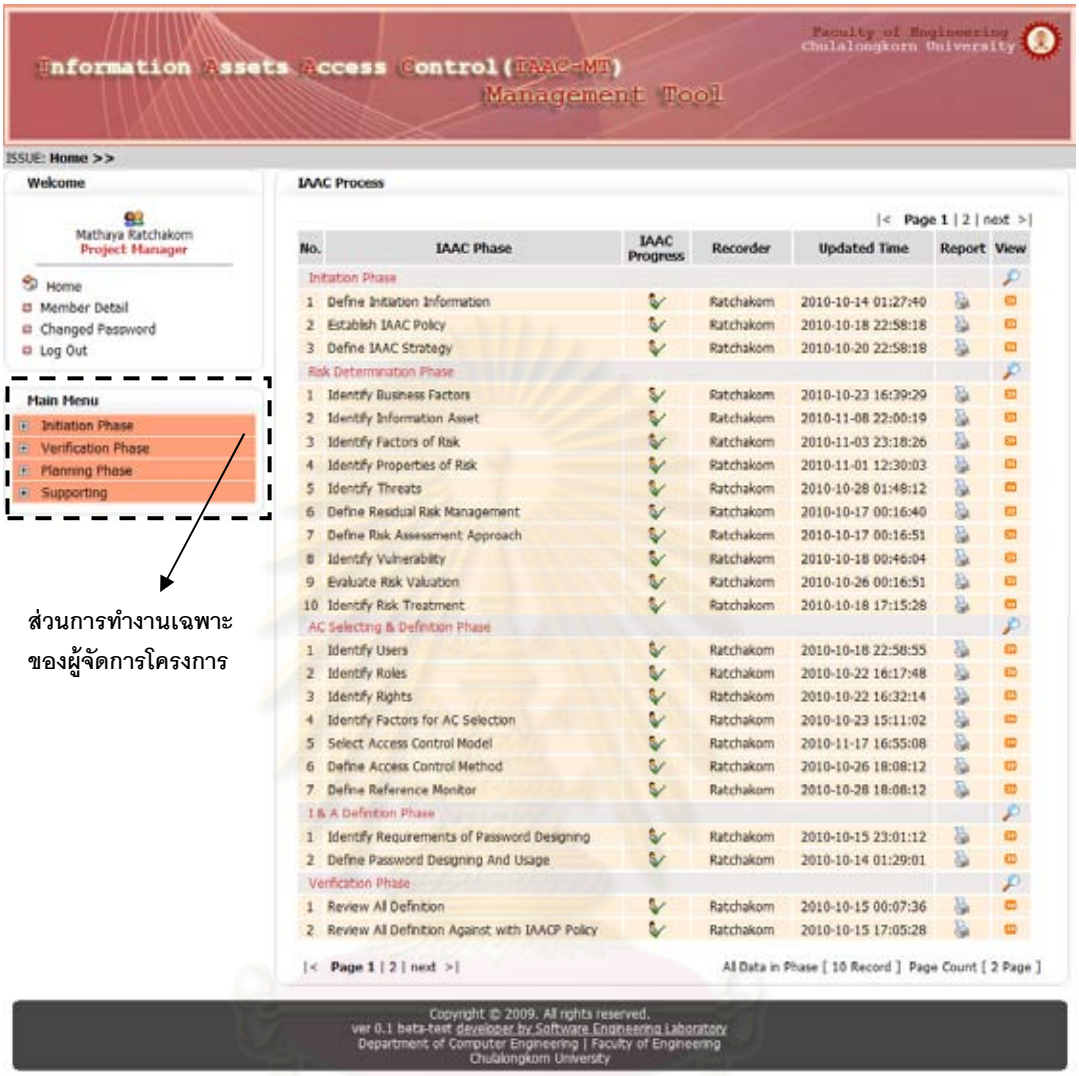


การจัดการข้อมูลผู้ใช้งาน
ซึ่งเป็นส่วนการทำงานเฉพาะ
ของผู้ดูแลระบบ

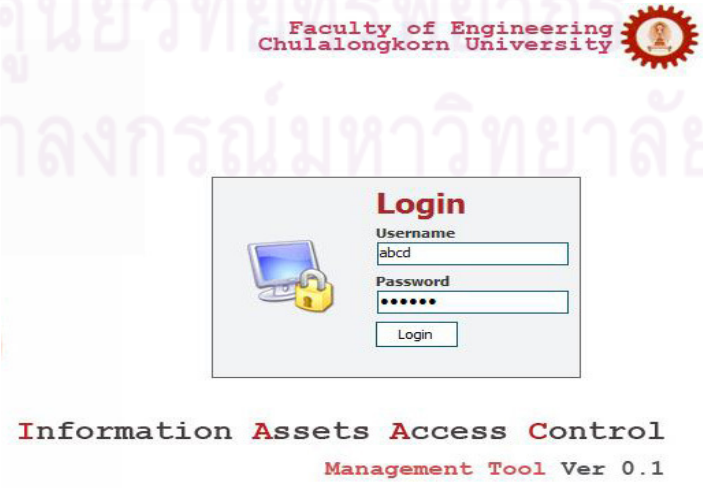
รูปที่ 6.9 หน้าจอแสดงส่วนการทำงานของผู้ดูแลระบบ (กรณีปกติ)

Information Assets Access Control
Management Tool Ver 0.1

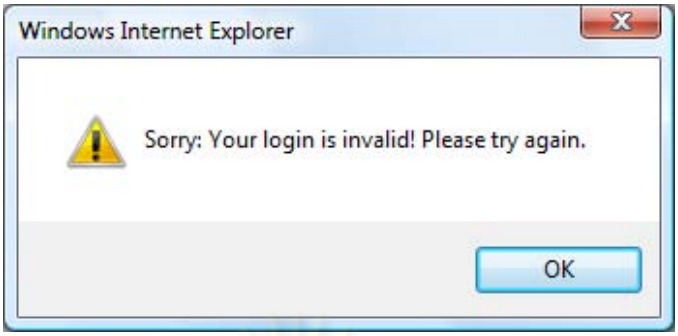
รูปที่ 6.10 หน้าจอแสดงการเข้าใช้งานระบบในบทบาทผู้จัดการโครงการ (กรณีปกติ)



รูปที่ 6.11 หน้าจอแสดงส่วนการทำงานของผู้จัดการโครงการ (กรณีปกติ)



รูปที่ 6.12 หน้าจอแสดงการเข้าใช้งานระบบที่ไม่ใช่ผู้ใช้งาน (กรณีผิดพลาด)



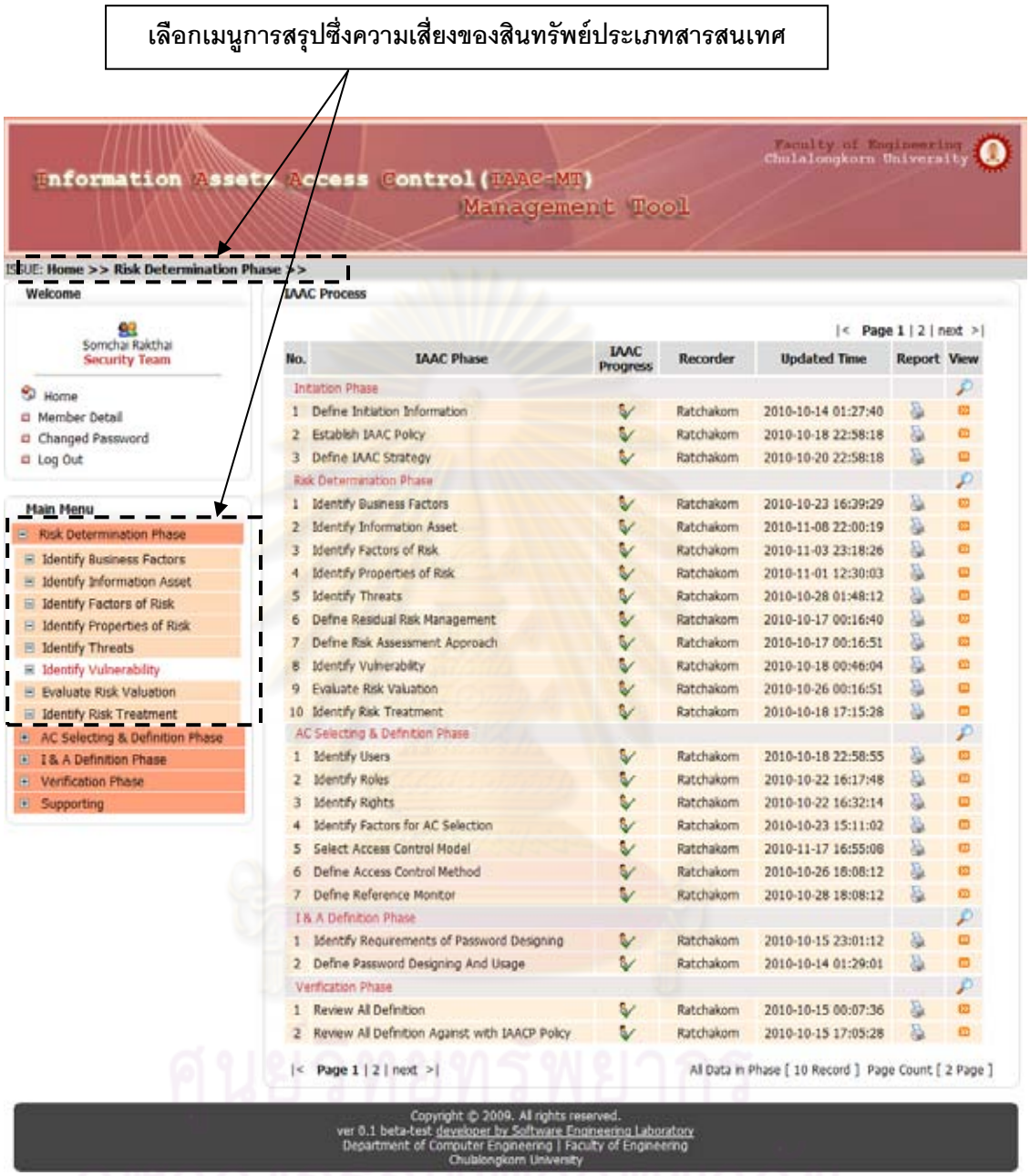
รูปที่ 6.13 หน้าต่างข้อความแสดงการเข้าใช้งานระบบที่ผิดพลาด (กรณีผิดพลาด)

ตารางที่ 6.11 ตัวอย่างกรณีทดสอบของการแสดงเส้นทางของการเข้าใช้งานระบบ

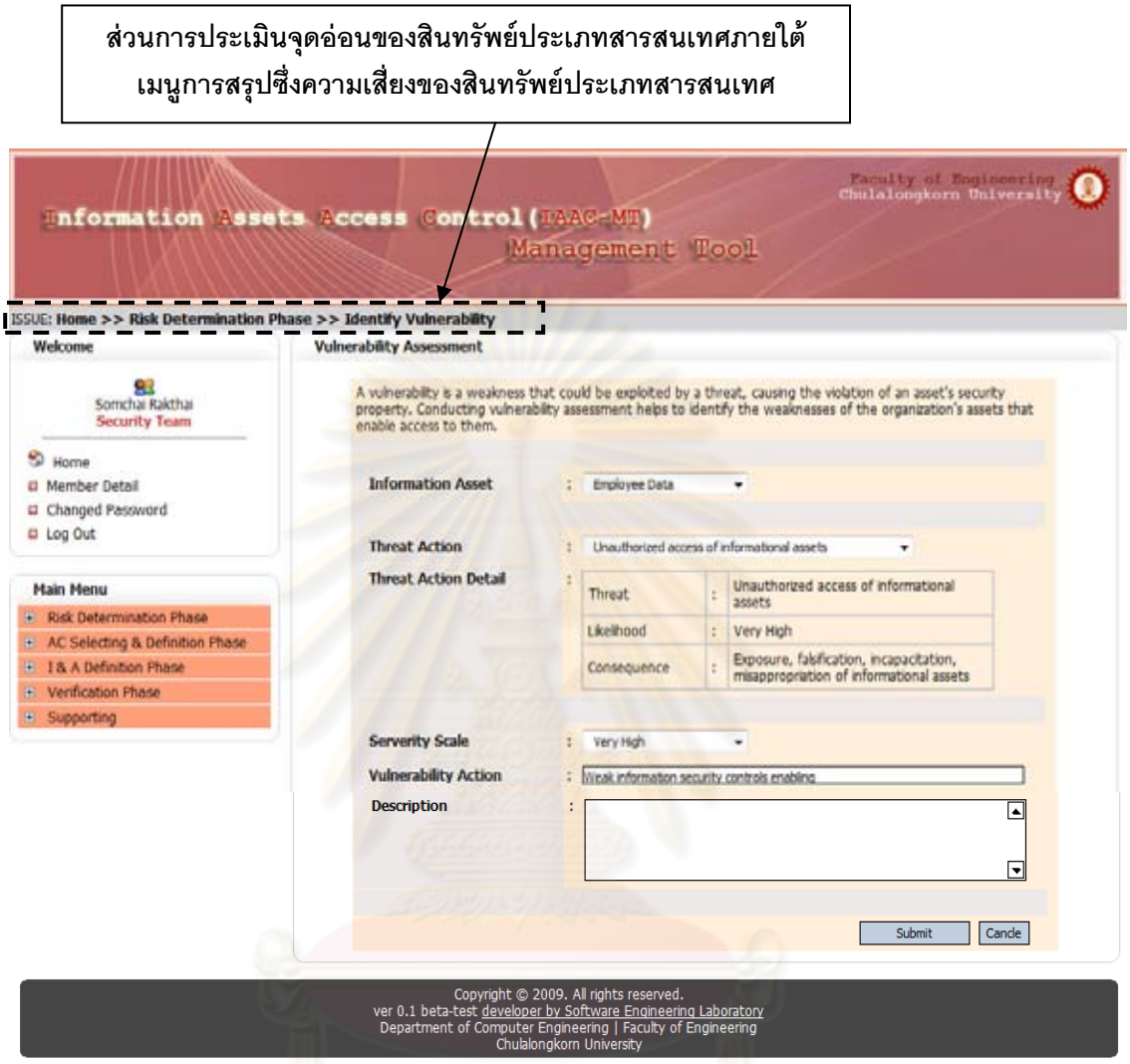
ชื่อหน้าที่การทำงานหลัก	ความสามารถของการใช้งานระบบ
เลขที่กรณีทดสอบ	TN02
ชื่อการทดสอบ	การแสดงเส้นทางของการเข้าใช้งานระบบ
วัตถุประสงค์การทดสอบ	เพื่อทดสอบการแสดงเส้นทางของการเข้าใช้งานระบบ
ข้อมูลนำเข้า	เส้นทางของการเข้าใช้งานระบบ
ผลลัพท์ที่คาดหวัง (กรณีปกติ)	ระบบสามารถแสดงเส้นทาง ณ ขณะที่ผู้ใช้ได้เข้าใช้งานในส่วนการทำงานนั้นๆ
ผลลัพท์ที่คาดหวัง (กรณีผิดพลาด)	ระบบไม่สามารถแสดงเส้นทางและ/หรือแสดงเส้นทางผิดพลาดในส่วนการทำงานที่ผู้ใช้กำลังเข้าใช้งานอยู่
ข้อมูลทดสอบ	กรณีที่ผู้ใช้งานเข้าใช้งานการประเมินภาวะเสี่ยงหรือจุดอ่อนในเมนูการสรุปซึ่งความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ แสดงดังตารางที่ 6.12
ผลการทดสอบ	เครื่องมือสามารถทำงานได้อย่างถูกต้องครบถ้วน ดังรูปที่ 6.14 - 6.15
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน
หมายเหตุ	……..…….……..

ตารางที่ 6.12 ข้อมูลทดสอบของกรณีทดสอบที่ TN02

ข้อมูลนำเข้า	ตัวอย่างข้อมูล
1. <<เลือกใช้งานเมนู>>	Risk Determination Phase
2. <<คลิกเข้าใช้งานส่วนการทำงาน>>	Identify Vulnerability



รูปที่ 6.14 หน้าจอแสดงการเข้าใช้งานเมนูการสรุปซึ่งความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ



รูปที่ 6.15 หน้าจอแสดงการเข้าใช้งานการประเมินจุดอ่อนของสินทรัพย์ประเภทสารสนเทศ

6.4 สรุปผลการทดสอบเครื่องมือสนับสนุนกระบวนการ

ผู้วิจัยได้ดำเนินการทดสอบระบบด้วยวิธีการข้างต้นในทุกส่วนของหน้าที่การทำงานของระบบ พบว่า ระบบสามารถทำงานสอดคล้องตามความต้องการของระบบที่ได้กำหนดขึ้นจากกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้เป็นอย่างดี และทุกส่วนการทำงานของระบบได้ผ่านการทดสอบ โดยสามารถสรุปผลของการทดสอบด้วยตัวอย่างกรณีทดสอบได้ดังตารางที่ 6.13

ตารางที่ 6.13 สรุปผลของการทดสอบด้วยตัวอย่างกรณีทดสอบของระบบ

เลขที่กรณีทดสอบ	ชื่อกรณีทดสอบ	หน้าที่การทำงานหลัก	ผลการทดสอบ	หมายเหตุ
TF001	การเพิ่มข้อมูลผู้ใช้งานระบบ	การจัดการข้อมูลผู้ใช้งานระบบ	ผ่าน	ตารางที่ 6.1
TF002	การเปลี่ยนรหัสผ่าน	การจัดการข้อมูลส่วนบุคคล	ผ่าน	ตารางที่ 6.4
TN01	การกำหนดสิทธิของการเข้าใช้งานระบบ	ความมั่นคงของระบบ	ผ่าน	ตารางที่ 6.7
TN02	การแสดงเส้นทางของการเข้าใช้งานระบบ	ความสามารถของการใช้งานระบบ	ผ่าน	ตารางที่ 6.11

เนื่องจากการทำงานหลายๆ ส่วนของระบบมีกระบวนการทำงานในลักษณะเดียวกัน ดังนั้นผู้วิจัยจึงได้ยกตัวอย่างการทดสอบและสรุปผลการทดสอบเพียงบางส่วนเท่านั้น อย่างไรก็ตามผู้วิจัยได้ทำการทดสอบระบบอย่างละเอียดและครบถ้วนในทุกๆ ส่วนการทำงานของระบบเรียบร้อยแล้ว เพื่อตรวจสอบความถูกต้องก่อนที่จะนำระบบไปใช้งานจริง

6.5 การประเมินผลเครื่องมือสนับสนุนกระบวนการ

การประเมินผลเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ จะทำการประเมินโดยการตรวจสอบว่า เครื่องมือสนับสนุนมีองค์ประกอบและส่วนการทำงานครบถ้วนและเป็นไปตามการดำเนินการของกระบวนการหรือไม่ ซึ่งวิธีการประเมินนั้นได้ใช้รายการตรวจสอบว่า การดำเนินการของกระบวนการนั้น สามารถใช้ระบบหรือหน้าที่การทำงานใดของเครื่องมือสนับสนุนในการทำงาน โดยผลของการประเมินสามารถแสดงได้ดังตารางที่ 6.14

ตารางที่ 6.14 เปรียบเทียบการทำงานของเครื่องมือสนับสนุนและการดำเนินการของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

IAAC Process Model	IAAC Management Tool
Phase I: Initiation	
1. Define IAAC Scope	1. Define Initiation Information
2. Define IAAC Mission & Goal	
3. Establish IAAC Policy	2. Establish IAAC Policy
4. Align with the Organization's Strategic Risk Management	3. Define IAAC Strategy
Phase II: Risk Determination	
1. Define Risk Assessment Approach	1. Define Risk Assessment Approach
2. Define Residual Risk Management	2. Define Residual Risk Management
3. Identify Risks	3. Identify Business Factors 4. Identify Information Assets 5. Identify Factors of Risk 6. Identify Properties of Risk 7. Identify Threats 8. Identify Vulnerability
4. Evaluate Risk Valuation	9. Evaluate Risk Valuation
5. Identify Risk Treatment	10. Identify Risk Treatment
Phase III: Access Control Selection & Definition	
1. Identify Factors for Access Control Model Selection	1. Identify Factors for AC Selection
2. Select & Define Access Control Model	2. Identify User Groups 3. Identify Roles 4. Identify Rights 5. Select Access Control Model 6. Define Access Control Method 7. Define Reference Monitor
Phase IV: I & A Definition	
1. Identify Requirements for Password Designing and Usage	1. Identify Requirements for Password Designing and Usage
2. Define Password Designing And Usage	2. Define Password Designing and Usage

ตารางที่ 6.14 เปรียบเทียบการทำงานของเครื่องมือสนับสนุนและการดำเนินการของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

Phase V: Verification	
1. Review All Definition	1. Review All Definition
2. Review All Definition Against with IAAC and Strategy	2. Review All Definition Against with IAAC and Strategy
Phase VI: Planning	
1. Plan for IAAC System Development	1. Plan for IAAC System 2. Define Risk Management 3. Plan for IAAC System Testing
2. Plan for Monitoring and Reviewing	4. Plan for Monitoring and Reviewing 5. Identify Metrics 6. Plan for Improvement
Phase VII: Implementing & Operating	
1. Train IAAC Team and Stakeholders	1. Train IAAC Team and Stakeholders / Related Users 2. Summarize IAAC Training
2. Implement IAAC System	3. Implement IAAC System 4. Report Change Management 5. Identify Project Management Checklist 6. Summarize Testing Result 7. Record Testing Result
3. Train Users and Aware of IAAC System	มีฟังก์ชันการทำงานเช่นเดียวกับ Train IAAC Team and Stakeholders
4. Operate IAAC System	ไม่มีฟังก์ชันการทำงาน เนื่องจากเป็นขั้นตอนที่ผู้ใช้งานดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งเป็นผลลัพธ์ของการดำเนินการกระบวนการ

ตารางที่ 6.14 เปรียบเทียบการทำงานของเครื่องมือสนับสนุนและการดำเนินการของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

Phase VIII: Monitoring & Reviewing	
1. Execute Monitoring and Reviewing IAAC System	1. Execute Monitoring and Reviewing IAAC System
2. Measure Effectiveness of IAAC System	2. Measure Effectiveness of IAAC System 3. Identify Metrics of Measurement 4. Identify Monitoring Results of Measurement
3. Update Monitoring and Reviewing Plan	5. Record Monitoring Plan Changing
4. Record Actions and Events that Impact on Effectiveness of IAAC System	6. Record Actions and Events that Impact on Effectiveness of IAAC System
Phase IX: Improvement	
1. Define Correctives and Preventives Action	1. Identify Accepted Loss of Actions and Events 2. Define Correctives and Preventives Action
2. Announce Identified Improvement to Stakeholders	3. Announce Identified Improvement to Stakeholders
3. Implement Identified Improvement	ไม่มีฟังก์ชันการทำงาน เนื่องจากเป็นขั้นตอนที่ดำเนินการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศตามการกระทำที่ได้กำหนดไว้

บทที่ 7
สรุปผลการวิจัยและข้อเสนอแนะ

จากการวิจัยเพื่อการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนั้น ผู้วิจัยได้สรุปผลการวิจัย และมีข้อเสนอแนะต่าง ๆ ดังต่อไปนี้

7.1 สรุปผลการวิจัย

สำหรับงานวิจัยนี้ ผู้วิจัยได้นำเสนอการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยพิจารณากระบวนการที่นำเสนอนั้นได้กล่าวถึงองค์ประกอบพื้นฐานที่ผู้วิจัยนำมาใช้ในการวิเคราะห์และออกแบบ เพื่อให้ได้เป็นกระบวนการที่จะนำไปพัฒนาเป็นเครื่องมือสนับสนุนต่อไป ซึ่งผลของการวิจัยสามารถสรุปดังต่อไปนี้

7.1.1) กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยสามารถนำเสนอรายละเอียดออกเป็นแบบจำลองต่างๆ ซึ่งมีความสัมพันธ์กันตั้งแต่ชั้นบนสุดที่แสดงถึงภาพรวมของกระบวนการ โดยอธิบายถึงส่วนนำเข้าและส่วนนำออกที่จำเป็นต่อการดำเนินการกระบวนการ รวมถึงบทบาทและหน้าที่ของผู้ที่เกี่ยวข้อง เรื่อยไปจนถึงชั้นล่างสุดที่แสดงถึงลำดับขั้นตอนและรายละเอียดของกิจกรรมที่เกิดขึ้น เรียงลำดับดังนี้ แบบจำลองเชิงภาพรวม แบบจำลองเชิงกระแสงาน และแบบจำลองเชิงนิยาม รวมทั้งแสดงถึงวิธีการในการประเมินกระบวนการที่นำเสนอขึ้นโดยใช้วิธีการทวนสอบแบบการตรวจตลอด ซึ่งผลของการวิเคราะห์และออกแบบกระบวนการนั้นได้แสดงให้เห็นถึงองค์ประกอบพื้นฐานสำคัญและแนวทางการดำเนินการที่จำเป็นต่อองค์กร เพื่อให้องค์กรสามารถนำไปประยุกต์ใช้ให้เข้ากับสภาวะแวดล้อมของแต่ละองค์กรต่อไป

7.1.2) เอกสารแผ่นแบบสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศจำนวนทั้งสิ้น 39 แผ่นแบบ โดยเอกสารดังกล่าวได้ออกแบบตามกระบวนการที่ได้นำเสนอ ซึ่งจะช่วยสนับสนุนให้องค์กรสามารถดำเนินการได้อย่างชัดเจนมากยิ่งขึ้น โดยองค์กรสามารถเพิ่มเติมรายละเอียดของการเก็บข้อมูลตามความเหมาะสมได้ภายหลังต่อไป

7.1.3) เครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งประกอบด้วยระบบย่อยทั้งหมด 11 ระบบตามลักษณะของการทำงานที่เกิดขึ้นดังนี้ 1)ระบบงานการริเริ่มโครงการ 2) ระบบงานการระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 3) ระบบงานการเลือกและกำหนดวิธีการการควบคุมการเข้าถึง 4) ระบบงานการกำหนดวิธีการระบุและพิสูจน์ตัวตน 5) ระบบงานการตรวจสอบข้อกำหนดของกระบวนการ 6) ระบบงานการวางแผนปฏิบัติการ 7) ระบบงานการพัฒนาระบบ 8) ระบบงานการเฝ้าสังเกตและทวนสอบระบบ 9) ระบบงานการ

ปรับปรุงระบบ 10) ระบบงานการสนับสนุนระบบ และ 11) ระบบงานการจำกัดสิทธิการใช้งานระบบ โดยความต้องการด้านหน้าที่ของแต่ละระบบย่อยที่นำเสนอนั้นเป็นเพียงความต้องการพื้นฐานที่ช่วยสนับสนุนให้องค์กรสามารถดำเนินการได้ตามกระบวนการที่ได้นำเสนอขึ้นเท่านั้น ซึ่งองค์กรสามารถพัฒนาเครื่องมือสนับสนุนเพิ่มเติมให้มีความซับซ้อนตามการใช้งานได้ภายหลังต่อไป

7.2 ปัญหาและข้อจำกัดในการทำวิจัย

ข้อจำกัดของงานวิจัยสำหรับองค์กรที่ต้องการนำกระบวนการที่ได้นำเสนอไปประยุกต์ใช้ มีดังต่อไปนี้

7.2.1) เนื่องจากงานวิจัยนี้เป็นเพียงการออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งมีแนวทางตามแบบรูปความมั่นคง และมีมาตรฐาน ISO/IEC 27001:2005 และ 27002:2005 เป็นกรอบของการดำเนินการ สำหรับองค์กรที่จะนำเอากระบวนการดังกล่าวไปประยุกต์ใช้จำเป็นต้องทำการปรับปรุงหรือเพิ่มเติมกระบวนการให้มีความสอดคล้องตามสภาวะแวดล้อมขององค์กรนั้นด้วย

7.2.2) การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนั้นได้นำเสนอองค์ประกอบพื้นฐานสำคัญและแนวทางการดำเนินการที่จำเป็นต่อการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศเพียงเท่านั้น ซึ่งไม่ได้ขึ้นกับองค์กรใดองค์กรหนึ่งโดยเฉพาะ ดังนั้นการนำกระบวนการดังกล่าวไปประยุกต์ใช้ จำเป็นต้องควบคุมปัจจัยทางด้านอื่นๆ ที่เป็นรายละเอียดสำคัญขององค์กรนั้น เช่น นโยบายองค์กร วัฒนธรรมขององค์กร ความสามารถของบุคลากร สภาพแวดล้อมการทำงาน เทคโนโลยีและต้นทุนที่มี เป็นต้น ทั้งนี้เพื่อให้การดำเนินการกระบวนการเป็นไปตามและบรรลุถึงเป้าหมายที่ได้วางไว้

7.3 ข้อเสนอแนะ

ผู้วิจัยมีข้อเสนอแนะสำหรับองค์กรที่ต้องการนำกระบวนการที่ได้นำเสนอไปประยุกต์ใช้ดังต่อไปนี้

7.3.1) กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่นำเสนอนั้น มีลักษณะความเป็นทั่วไปที่สามารถนำเอาแนวคิดกระบวนการไปประยุกต์ใช้กับประเด็นการทำงานอื่นๆ ที่นอกเหนือจากประเด็นการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศที่เกี่ยวข้องกับการควบคุมการเข้าถึงได้

7.3.2) การดำเนินการกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้สามารถบรรลุตามเป้าหมายที่ได้วางไว้นั้น องค์กรต้องคำนึงถึงและให้ความสำคัญกับองค์ประกอบที่จะส่งผลต่อความสำเร็จของการดำเนินการกระบวนการ ทั้งในประเด็นด้านวัฒนธรรมขององค์กร ความร่วมมือบุคคล และเทคโนโลยีที่นำมาใช้ ซึ่งองค์กรจะต้องประสานความสมดุลระหว่างองค์ประกอบเหล่านี้ร่วมกับกระบวนการที่มีการวางเป้าหมายและกลยุทธ์ที่แน่ชัด

7.3.3) กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนั้น มีความเหมาะสมกับองค์กรที่มีขนาดกลางไปจนถึงขนาดใหญ่ เนื่องจากขั้นตอนภายใต้การดำเนินการกระบวนการนั้นมีความละเอียดอ่อนและซับซ้อน จำเป็นต้องอาศัยทีมการทำงานและผู้ที่เกี่ยวข้องเป็นจำนวนมาก และทีมการทำงานและผู้ที่เกี่ยวข้องดังกล่าวควรมีความรู้และความเข้าใจในหลักการสร้างความมั่นคงเป็นอย่างสูง ทั้งนี้จึงจะสามารถดำเนินการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ

7.3.4) การประยุกต์ใช้กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนั้น องค์กรจะต้องทำการศึกษารายละเอียดของกระบวนการภายใต้แบบจำลองทั้ง 3 ชั้น คือ แบบจำลองเชิงภาพรวม แบบจำลองเชิงกระแสงาน และแบบจำลองเชิงนิยาม ทั้งนี้ต้องพิจารณาควบคู่กับสภาวะแวดล้อมขององค์กรนั้นๆ โดยวิเคราะห์ถึงความเป็นไปได้ของการนำกระบวนการมาประยุกต์ใช้อย่างเหมาะสม ซึ่งอาจมีการเพิ่มเติมหรือปรับปรุงรายละเอียดของกระบวนการ จากนั้นทำการวางแผนการดำเนินการอย่างบูรณาการ โดยเบื้องต้นอาจประยุกต์ใช้สำหรับสินทรัพย์ประเภทสารสนเทศในบางส่วนเพื่อรับทราบผล ทั้งนี้สำหรับปรับปรุงไว้ใช้กับสินทรัพย์ประเภทสารสนเทศทั้งหมดขององค์กร นอกจากนี้กระบวนการควรมีการควบคุมและประเมินผลการดำเนินการอย่างเป็นวงรอบและต่อเนื่อง เพื่อให้มั่นใจได้ว่ากระบวนการมีการดำเนินการอย่างมีประสิทธิภาพต่อไป

7.3.5) การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ องค์กรจะต้องทำการเพิ่มเติมรายละเอียดของความมั่นคงทั้งทางด้านอุปกรณ์ฮาร์ดแวร์ สถานที่และสภาพแวดล้อมของการจัดตั้ง รวมถึงการติดต่อจากภายนอกที่ต้องการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ทั้งนี้เนื่องจากในกระบวนการได้แสดงให้เห็นถึงหลักการสร้างความมั่นคงพื้นฐานที่เกี่ยวข้องกับการควบคุมการเข้าถึงเท่านั้น

7.3.6) เครื่องมือสนับสนุนกระบวนการที่พัฒนาขึ้นนั้นเป็นเพียงระบบต้นแบบ มีหน้าที่พื้นฐานเพื่อสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเท่านั้น ซึ่งสามารถนำไปพัฒนาหน้าที่การทำงานอื่นเพิ่มเติมได้ภายหลังต่อไป

รายการอ้างอิง

[1] Blakley, B. and Heath, C. Security Design Patterns. U.K.: The Open Group, April 2004.

[2] Schumacher, M. Security Engineering with Patterns. Spinger-Verlag Berlin HeidelBerg, 2002.

[3] Schumacher, M. Fernandez-Buglioni, E. Hybertson, D. Buschmann, F. and Sommerlad, P. Security Patterns Intrigrating Security and System Engineering. John Wiley & Sons, Ltd, 2006.

[4] ISO/IEC International Standard 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements. ISO/IEC 27001:2005, 2005.

[5] ISO/IEC International Standard 27002 Information Technology - Security Techniques - Code of Practice Information Security Management. ISO/IEC 27002:2005, 2005.

[6] Yoder, J. and Barcalow, J. "Architectural Patterns for Enabling Applications Security," 4th Proceedings of Pattern Languages of Programs, 1997.

[7] Kienzle, D. M. and Elder, M. C. Security Patterns for Web Application Development. DARPA Contract #F30602-01-C-0164, 2002.

[8] กวิน สุภาพร. การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550.

[9] Rosado, D. G. Gutiarrez, Fernandez-Medina, C. E. and Piattini, M. "A Study of Security Architectural Patterns," 1st International Conference on Availability, Reliability, and Security, pp.358-365, 2006.

[10] Koch, M. and Parisi-Presicce, F. "Formal Access Control Analysis in the Software Development Process," ACM workshop on Formal methods in security engineering, pp.67-76, 2003.

[11] ภมร วรรธกะวิกรานต์. การออกแบบและพัฒนากระบวนการการคัดเลือกผลิตภัณฑ์ซอฟต์แวร์เชิงพาณิชย์ที่ใช้แบบจำลองวุฒิภาวะความสามารถแบบบูรณาการเป็นฐาน. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550.

[12] Sandhu, R. S. Paraboschi, S. and Samarati, P. Access control: Principles and Solutions, in Software - Practice and Experience, April 2003.

[13] Krnchten, P. The Rational Unified Process: an introduction, Third ed, Pearson Education, Inc., 2003.

[14] Ahern, D. M. CMMI SCAMPI Distilled: Appraisals for Process Improvement, Addison-Wesley Professional, 2005.

[15] Heyman, T. Scandariato, R. Huygens, C. and Joosen, W. "Using Security Patterns to Combine Security Metrics," 3th International Conference on Availability, Reliability and Security, pp. 1156-1163, 2008.

ภาคผนวก

ภาคผนวก ก
อภิธานศัพท์

Process Model	แบบจำลองกระบวนการ
Process Operation	การดำเนินการกระบวนการ
Business Value	มูลค่าทางธุรกิจ
Security Pattern	แบบรูปความมั่นคง
Information Asset	สินทรัพย์ประเภทสารสนเทศ
Information Security Management	การจัดการความมั่นคงสารสนเทศ
Risk Assessment	การประเมินความเสี่ยง
Residual Risk	ความเสี่ยงที่คงเหลือ
Access Control	การควบคุมการเข้าถึง
Authorization	การให้อำนาจ
Role-Based Access Control	การควบคุมการเข้าถึงเชิงบทบาท
Multilevel Security	ความมั่นคงหลายระดับ
Reference Monitor	การตรวจสอบการเข้าถึง
Identification and Authentication	การระบุและพิสูจน์ตัวตน
Template Document	เอกสารแผ่นแบบ

ภาคผนวก ข
การนิยามกิจกรรมของกระบวนการ

กิจกรรมของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศภายใต้แบบจำลองเชิงนิยามนั้นมีทั้งหมด 32 กิจกรรม ซึ่งสามารถสรุปได้ดังตารางที่ ข.1 และสามารถอธิบายรายละเอียดของกิจกรรมดังกล่าวได้ดังตารางที่ ข.2 - ข.33

ตารางที่ ข.1 กิจกรรมของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	ชื่อกิจกรรม	หน้าที่
1	การกำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	118
2	การกำหนดเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	119
3	การจัดตั้งนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	120
4	การปรับนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้สอดคล้องกับกลยุทธ์องค์กรด้านการจัดการความเสี่ยง	121
5	การกำหนดกลยุทธ์ของการประเมินความเสี่ยง	123
6	การกำหนดการจัดการความเสี่ยงที่คงเหลือ	124
7	การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ	125
8	การประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ	127
9	การระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ	128
10	การกำหนดปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง	130
11	การเลือกโมเดลการควบคุมการเข้าถึงที่เหมาะสม	131
12	การกำหนดวิธีการการให้อำนาจ	132
13	การกำหนดวิธีการเข้าถึงเชิงบทบาท	133
14	การกำหนดวิธีการของความมั่นคงหลายระดับ	134
15	การกำหนดวิธีการของการตรวจสอบการเข้าถึง	135
16	การกำหนดความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน	136
17	การออกแบบและใช้งานรหัสผ่าน	137
18	การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน	139

ตารางที่ ข.1 กิจกรรมของกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

ลำดับ	ชื่อกิจกรรม	หน้าที่
19	การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน โดยยึดเอานโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นหลัก	140
20	การวางแผนสำหรับการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	142
21	การวางแผนสำหรับการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	145
22	การฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	148
23	การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	150
24	การฝึกอบรมผู้ใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	153
25	การดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	154
26	การดำเนินการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	155
27	การประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	157
28	การปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	158
29	การบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	160
30	การกำหนดการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	161
31	การประกาศการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	162
32	การปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	164

ตารางที่ ข.2 การกำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Define IAAC Scope)
จุดประสงค์	เพื่อกำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร รวมถึงอธิบายที่มาและความสำคัญของความจำเป็นต้องมี ทั้งนี้เพื่อใช้เป็นแนวทางในการดำเนินการควบคุมสินทรัพย์ประเภทสารสนเทศต่อไป
เงื่อนไขก่อนการดำเนินกิจกรรม	1. องค์กรต้องการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศของตน โดยวิธีการควบคุมการเข้าถึง ซึ่งเกิดจากการเล็งเห็นถึงความสำคัญ และผลกระทบที่เกิดจากการสูญหาย หรือเปลี่ยนแปลงแก้ไขสินทรัพย์ประเภทสารสนเทศเหล่านั้นจากบุคคลที่ไม่มีสิทธิการเข้าถึง 2. ได้รับการพิจารณาเห็นชอบจากผู้บริหารระดับสูงให้สามารถดำเนินการได้ รวมถึงการลงนามและประกาศรับรองโครงการ 3. มีการกำหนดนโยบายองค์กรด้านความมั่นคงไว้ก่อนหน้านี้แล้ว โดยที่นโยบายดังกล่าวอาจถูกจัดเตรียมไว้ตั้งแต่เริ่มจัดตั้งองค์กร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารอนุมัติการดำเนินการโครงการจากผู้บริหารระดับสูง 2. <<เอกสาร>> เอกสารนโยบายองค์กรด้านความมั่นคง 3. <<เอกสารแผ่นแบบ>> แผ่นแบบขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. อธิบายที่มาและความสำคัญของความจำเป็นในการสร้างการควบคุมการเข้าถึงให้กับสินทรัพย์ประเภทสารสนเทศขององค์กร ทั้งนี้เพื่อให้ตระหนักถึงความจำเป็นต้องมีและการจัดตั้งโครงการขึ้นมา 2. พิจารณาและอภิปรายถึงสิ่งที่จะมาเป็นขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยพิจารณาจากสภาพแวดล้อมขององค์กร รวมถึงนโยบายองค์กรด้านความมั่นคงเป็นหลัก 3. กำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งต้องอธิบายโดยเฉพาะในมุมมองของทางด้านธุรกิจและด้านองค์กร ทั้งนี้เพื่อใช้เป็นกรอบในการดำเนินการต่อไป
ส่วนนำออก	<<เอกสาร>> เอกสารขอบเขตของการควบคุมการเข้าถึงสินทรัพย์สารสนเทศ
เงื่อนไขการออกจากกิจกรรม	ที่มาความสำคัญและขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายองค์กรด้านความมั่นคง
ผู้รับผิดชอบ	ผู้จัดการโครงการและหัวหน้าทีมความมั่นคง

ตารางที่ ข.3 การกำหนดเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Define IAAC Goal and Mission)
จุดประสงค์	เพื่อกำหนดเป้าหมายและพันธกิจสำหรับใช้เป็นแนวทางของการดำเนินการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขก่อนการดำเนินกิจกรรม	มีการกำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารขอบเขตการควบคุมการเข้าถึงสินทรัพย์สารสนเทศ 2. <<เอกสารแผ่นแบบ>> แผ่นแบบเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบรายนามสมาชิกทีมความมั่นคง
ขั้นตอนการทำงาน	1. พิจารณาและอภิปรายถึงสิ่งที่จะมาเป็นเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยพิจารณาจากขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ได้กำหนดมาจากกิจกรรมที่ 1 เป็นหลัก 2. กำหนดเป้าหมายของการปฏิบัติ ทั้งนี้เพื่อใช้เป็นแนวทางของการดำเนินการควบคุมการเข้าถึงให้กับสินทรัพย์ประเภทสารสนเทศขององค์กร 3. กำหนดพันธกิจที่ต้องปฏิบัติสำหรับการดำเนินการสร้างการควบคุมการเข้าถึงให้กับสินทรัพย์ประเภทสารสนเทศ ซึ่งจะต้องมีความสอดคล้องต้องกันกับเป้าหมายของการปฏิบัติ **<u>หมายเหตุ</u>** ให้ทำการระบุรายนามสมาชิกภายใต้ทีมความมั่นคง ซึ่งต้องมีการระบุในกิจกรรมนี้ เนื่องจากทีมความมั่นคงดังกล่าวจะทำหน้าที่ในการประเมินความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ กำหนดวิธีการการควบคุมการเข้าถึง และวิธีการระบุและพิสูจน์ตัวตน ซึ่งเป็นกิจกรรมสำคัญภายหลังจากนี้
ส่วนนำออก	1. <<เอกสาร>> เอกสารเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารรายนามสมาชิกทีมความมั่นคง
เงื่อนไขการออกจากกิจกรรม	เป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดอย่างชัดเจนภายใต้ขอบเขตการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ รวมถึงรายนามสมาชิกภายใต้ทีมความมั่นคงได้ถูกระบุ
ผู้รับผิดชอบ	ผู้จัดการโครงการและหัวหน้าทีมความมั่นคง

ตารางที่ ข.4 การจัดตั้งนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การจัดตั้งนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Establish IAAC Policy)
จุดประสงค์	เพื่อจัดตั้งนโยบายสำหรับใช้ควบคุมการกำหนดต่างๆ ของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรให้มีความชัดเจน โดยนโยบายดังกล่าวควรประกอบไปด้วยเนื้อหาสำคัญ เช่น หลักการ (Principle) กฎหรือข้อบังคับ (Relevant Legislation) มาตรฐาน (Standard) และเอกสาร (Documents) ต่างๆ ที่มีความเกี่ยวข้อง เป็นต้น
เงื่อนไขก่อนการดำเนินกิจกรรม	มีการกำหนดเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายองค์กรด้านความมั่นคง 2. <<เอกสาร>> เอกสารขอบเขตการควบคุมการเข้าถึงสินทรัพย์สารสนเทศ 3. <<เอกสาร>> เอกสารเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสารแผ่นแบบ>> แผ่นแบบนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. กำหนดนโยบาย (โดยเฉพาะนโยบายสำหรับสินทรัพย์ประเภทสารสนเทศที่สามารถทำการเผยแพร่และสมควรแก่การควบคุมการเข้าถึง) หลักการ กฎหรือข้อบังคับขององค์กร รวมถึงมาตรฐานที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 1.1 ทวนสอบความสอดคล้องต้องกันของการควบคุมการเข้าถึงกับนโยบายด้านการจัดแบ่งประเภทสินทรัพย์สารสนเทศขององค์กร 1.2 กำหนดการจัดการสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งจะต้องครอบคลุมทุกๆ เส้นทางของการเชื่อมต่อ 1.3 จำแนกกฎข้อบังคับของการควบคุมการเข้าถึง ทั้งในการร้องขอ การอนุญาตให้เข้าถึง รวมถึงการบริหารจัดการการเข้าถึงใดๆ 1.4 กำหนดความต้องการของการอนุญาตให้เข้าถึงสินทรัพย์ประเภทสารสนเทศสำหรับแต่ละการร้องขอ 1.5 กำหนดการจัดการการถอนสิทธิการเข้าถึงออกจากที่ได้กำหนดไว้ 2. ระบุถึงทุกๆ เอกสารที่เกี่ยวข้อง ซึ่งอาจรวมถึงสัญญาหรือข้อตกลงที่มุ่งเน้นการป้องกันการเข้าถึงสินทรัพย์ประเภทสารสนเทศ และเอกสารที่ระบุถึงการเข้าถึงสินทรัพย์ดังกล่าวของผู้ใช้งานซึ่งเป็นไปตามบทบาทในองค์กร

ตารางที่ ข.4 การจัดตั้งนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำออก	<<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกจัดตั้งขึ้น
ผู้รับผิดชอบ	ผู้จัดการโครงการ หัวหน้าทีมความมั่นคง และผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.5 การปรับนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้สอดคล้องกับกลยุทธ์องค์กรด้านการจัดการความเสี่ยง

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การปรับนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้สอดคล้องกับกลยุทธ์องค์กรด้านการจัดการความเสี่ยง (Align IAAC with the Organization's Strategic Risk Management)
จุดประสงค์	เพื่อวางกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งจะต้องสอดคล้องและเป็นไปตามกลยุทธ์องค์กรด้านการจัดการความเสี่ยง รวมถึงกำหนดกระบวนการเพื่อให้ดำเนินการเป็นไปตามกลยุทธ์ที่ได้วางไว้
เงื่อนไขก่อนการดำเนินกิจกรรม	1. มีการกำหนดกลยุทธ์องค์กรด้านการจัดการความเสี่ยงไว้ก่อนหน้านี้แล้ว โดยที่กลยุทธ์ดังกล่าวอาจถูกจัดเตรียมไว้ตั้งแต่เริ่มจัดตั้งองค์กร 2. มีการกำหนดนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารกลยุทธ์องค์กรด้านการจัดการความเสี่ยง 2. <<เอกสาร>> เอกสารขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสารแผ่นแบบ>> แผ่นแบบกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสารแผ่นแบบ>> แผ่นแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ข.5 การปรับนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้สอดคล้องกับกลยุทธ์องค์กรด้านการจัดการความเสี่ยง (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. วิเคราะห์ความเหมือนและต่าง (Gap Analysis) ระหว่างนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและกลยุทธ์องค์กรด้านการจัดการความเสี่ยง 2. อภิปรายและปรับนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศในส่วนที่มีความแตกต่างให้มีความสอดคล้องต้องกันกับกลยุทธ์องค์กรด้านการจัดการความเสี่ยง ทั้งนี้เพื่อจัดวางกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้มีความชัดเจนมากยิ่งขึ้น 3. กำหนดกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งจะต้องเป็นไปตามกลยุทธ์ที่ได้วางเอาไว้ในข้อที่ 2 4. สมาชิกภายใต้ทีมความมั่นคงทำความเข้าใจเกี่ยวกับขอบเขต เป้าหมายและพันธกิจ นโยบาย กลยุทธ์และกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ส่วนนำออก	1. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	1. นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและกลยุทธ์องค์กรด้านการจัดการความเสี่ยงเป็นไปในทิศทางเดียวกัน 2. กลยุทธ์และกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดอย่างชัดเจน และต้องสอดคล้องเป็นไปตามขอบเขต เป้าหมาย พันธกิจและนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. สมาชิกทีมความมั่นคงมีความเข้าใจเกี่ยวกับขอบเขต เป้าหมายและพันธกิจ นโยบาย กลยุทธ์และกระบวนการการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศอย่างถ่องแท้
ผู้รับผิดชอบ	ผู้จัดการโครงการ หัวหน้าทีมความมั่นคง และผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.6 การกำหนดกลยุทธ์ของการประเมินความเสี่ยง

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	กำหนดกลยุทธ์ของการประเมินความเสี่ยง (Define Risk Assessment Approach)
จุดประสงค์	เพื่อกำหนดกลยุทธ์ของการประเมินความเสี่ยง ซึ่งจะต้องถูกนำมาใช้เป็นเกณฑ์ในการประเมินความเสี่ยงของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร และถูกใช้ในการสรุปค่าความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศ ซึ่งผลที่ได้จะนำไปวิเคราะห์เพื่อสรุปผลเป็นการป้องกันรักษาความเสี่ยงต่อไป
เงื่อนไขก่อนการดำเนินกิจกรรม	ทีมความมั่นคงมีความเข้าใจในนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นอย่างดี
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบกลยุทธ์ของการประเมินความเสี่ยง
ขั้นตอนการทำงาน	1. กำหนดวิธีการของการประเมินความเสี่ยง (Risk Assessment Methodology) ซึ่งจะต้องเหมาะสมกับการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและเป็นไปตามกลยุทธ์ขององค์กรด้านการจัดการความเสี่ยง 2. กำหนดเกณฑ์ของการยอมรับความเสี่ยง (Criteria for Accepting Risk) 3. ระบุถึงระดับของการยอมรับความเสี่ยง (Acceptable Levels of Risk) **<u>หมายเหตุ</u>** วิธีการประเมินความเสี่ยง รวมถึงเกณฑ์และระดับของการยอมรับความเสี่ยงนั้น ได้มีแนวทางของการกำหนดไว้ในกิจกรรมที่ 7 ระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ และกิจกรรมที่ 8 ประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
ส่วนนำออก	<<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง
เงื่อนไขการออกจากกิจกรรม	กลยุทธ์ของการประเมินความเสี่ยงได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.7 การกำหนดการจัดการความเสี่ยงที่คงเหลือ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดการจัดการความเสี่ยงที่คงเหลือ (Define Residual Risk Management)
จุดประสงค์	เพื่อกำหนดการจัดการสำหรับความเสี่ยงใดๆ ที่คงเหลือจากที่ได้ทำการประเมินความเสี่ยงครั้งก่อน รวมถึงการระบุเกณฑ์และระดับของการยอมรับความเสี่ยงที่คงเหลือ และผลกระทบของความเสี่ยงใดๆ ที่มีต่อองค์กรที่คาดว่าจะเกิดขึ้น
เงื่อนไขก่อนการดำเนินกิจกรรม	ทีมความมั่นคงมีความเข้าใจในนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นอย่างดี
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบการจัดการความเสี่ยงที่คงเหลือ
ขั้นตอนการทำงาน	1. กำหนดวิธีการจัดการเพื่อรองรับการแก้ไขปัญหาของความเสี่ยงใดๆ ที่ยังคงเหลือจากการที่ได้ประเมินความเสี่ยงในครั้งก่อน โดยวิธีการดังกล่าวจะต้องเป็นไปตามกลยุทธ์ขององค์กรด้านการจัดการความเสี่ยง 2. กำหนดเกณฑ์ในการยอมรับความเสี่ยงที่คงเหลือ 3. ระบุระดับในการยอมรับความเสี่ยงที่คงเหลือ 4. ระบุถึงผลกระทบที่มีต่อองค์กรที่คาดว่าจะเกิดขึ้น ซึ่งเกิดจากความเสี่ยงที่คงเหลือ **<u>หมายเหตุ</u>** ความเสี่ยงที่คงเหลือ (Residual Risk) คือ ความเสี่ยงที่ยังคงเหลือจากการประเมินความเสี่ยงครั้งก่อน โดยเป็นผลจากความเสี่ยงที่มีปัจจัยที่ไม่สามารถควบคุมได้อย่างแน่นอน เช่น กฎหรือข้อบังคับที่มีความซับซ้อน รายละเอียดของการเก็บข้อมูลที่มีความกำกวม การกระทำและบุคคลที่มีความเกี่ยวข้องกับสินทรัพย์ประเภทสารสนเทศที่มีเป็นจำนวนมาก เป็นต้น โดยที่การจัดการกับความเสี่ยงที่คงเหลือนั้น ควรมุ่งเน้นไปในด้านของการจัดการด้านของเงินเป็นสำคัญ
ส่วนนำออก	<<เอกสาร>> เอกสารการจัดการความเสี่ยงที่คงเหลือ
เงื่อนไขการออกจากกิจกรรม	การจัดการความเสี่ยงที่คงเหลือได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.8 การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ*

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Identify Risks of Information Asset)
จุดประสงค์	เพื่อระบุถึงความเสี่ยงใดๆ ที่อาจจะเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศขององค์กร โดยมองในมุมมองของการดำเนินการโดยรวมและปัจจัยทางด้านธุรกิจเป็นสำคัญ ทั้งนี้ได้รวมถึงการประเมินมูลค่าของสินทรัพย์ประเภทสารสนเทศ (Asset Value) ในด้านต่างๆ การกำหนดภัยคุกคาม (Threat) ที่อาจจะเกิดขึ้น และภาวะจุดอ่อน (Vulnerability) ที่อาจเป็นช่องทางให้ภัยคุกคามใดๆ นั้นโจมตี
เงื่อนไขก่อนการดำเนินกิจกรรม	มีการกำหนดกลยุทธ์ของการประเมินความเสี่ยงเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 4. <<เอกสารแผ่นแบบ>> แผ่นแบบความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. ระบุสินทรัพย์ประเภทสารสนเทศทั้งหมดขององค์กรที่ต้องการการควบคุมการเข้าถึง 2. ระบุปัจจัยทางธุรกิจ (Business Factors) ทั้งภายในและภายนอกองค์กรที่มีผลต่อความมั่นคงของสินทรัพย์ประเภทสารสนเทศที่ระบุไว้ในข้อที่ 1 3. ระบุคุณสมบัติด้านความมั่นคง (Security Properties) ให้กับสินทรัพย์ประเภทสารสนเทศในข้อที่ 1 โดยใช้ปัจจัยทางธุรกิจของแต่ละสินทรัพย์ประเภทสารสนเทศในการระบุ ซึ่งโดยทั่วไปแล้วคุณสมบัติด้านความมั่นคงจะประกอบด้วย - การรักษาความลับ (Confidentiality) - ความบูรณาภาพ (Integrity) - สภาพพร้อมใช้งาน (Availability) - ภาระรับผิดชอบ (Accountability) 4. ระบุถึงผลกระทบที่มีต่อองค์กรของแต่ละสินทรัพย์ประเภทสารสนเทศ เมื่อเกิดการสูญเสียคุณสมบัติด้านความมั่นคง

ตารางที่ ข.8 การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ* (ต่อ)

<table>
<tr><th>หัวข้อ</th><th>คำอธิบาย</th></tr>
<tr><td>ขั้นตอนการทำงาน</td><td>5. ประเมินมูลค่าของแต่ละสินทรัพย์ประเภทสารสนเทศ โดยถือเป็นการกำหนดความสำคัญของสินทรัพย์ประเภทสารสนเทศที่มีต่อองค์กรที่เป็นเจ้าของ ทั้งนี้เพื่อระบุว่าเมื่อเกิดความสูญเสียสินทรัพย์ประเภทสารสนเทศนั้นๆ จะกระทบในด้านใดบ้างและระดับของผลกระทบนั้นมาก-น้อยเพียงใด ซึ่งในที่นี้จะมองในมุมมอง 3 ด้าน ดังนี้
- ด้านความมั่นคง (Security Value)
- ด้านการเงิน (Financial Value)
- ทางด้านธุรกิจ (Business Value)
6. สรุปมูลค่าโดยรวม (Overall Value) ของแต่ละสินทรัพย์ประเภทสารสนเทศ ซึ่งเกิดจากการนำมูลค่าของทั้ง 3 ด้านที่ระบุไว้ในข้อที่ 5 มาเปรียบเทียบ โดยถือเอาค่าที่มากที่สุดเป็นมูลค่าโดยรวมของสินทรัพย์นั้น
7. ระบุภัยคุกคามใดๆ ที่อาจจะเกิดขึ้นกับแต่ละสินทรัพย์ประเภทสารสนเทศ
8. กำหนดระดับความถี่ (Likelihood) ของแต่ละภัยคุกคามที่ระบุไว้ในข้อที่ 7
9. ระบุถึงผลกระทบที่มีต่อองค์กรเมื่อแต่ละภัยคุกคามใดๆ เกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศนั้น
10. เลือกข้อมูลภัยคุกคามที่อาจจะเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศใดๆ ทั้งนี้เพื่อใช้ในการระบุจุดอ่อนซึ่งจะถูกใช้โดยภัยคุกคามในการโจมตี
11. ระบุจุดอ่อนที่จะถูกใช้โดยแต่ละภัยคุกคาม
12. กำหนดระดับความรุนแรง (Servility Scale) เมื่อถูกภัยคุกคามใดๆ โจมตีจุดอ่อนที่ระบุไว้ในข้อที่ 11
<u>หมายเหตุ</u> ในการประเมินมูลค่าสินทรัพย์ประเภทสารสนเทศข้อที่ 5 และ 6 การกำหนดระดับความถี่ของแต่ละภัยคุกคามข้อที่ 8 และระดับความรุนแรงเมื่อถูกภัยคุกคามใดๆ โจมตีจุดอ่อนนั้นในข้อที่ 12 ได้แบ่งระดับออกเป็น
<table>
<tr><td>- สูงที่สุด (Extreme)</td><td>- ปานกลาง (Medium)</td></tr>
<tr><td>- สูงมาก (Very High)</td><td>- น้อย (Low)</td></tr>
<tr><td>- สูง (High)</td><td>- เล็กน้อย (Negligible)</td></tr>
</table>
</td></tr>
<tr><td>ส่วนนำออก</td><td><<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ</td></tr>
<tr><td>เงื่อนไขการออกจากกิจกรรม</td><td>ความเสี่ยงใดๆ ที่คาดว่าจะเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศขององค์กรได้ถูกกำหนดอย่างชัดเจน</td></tr>
<tr><td>ผู้รับผิดชอบ</td><td>ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง</td></tr>
</table>

ตารางที่ ข.9 การประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ*

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Evaluate Risk Valuation of Information Asset)
จุดประสงค์	เพื่อประเมินผลค่าของความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศที่ได้ระบุไว้ในกิจกรรมที่ 7 การระบุความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ ทั้งนี้จะต้องวิเคราะห์และประเมินผลโดยถือเอาผลกระทบในด้านต่างๆ เช่น ด้านความมั่นคง ด้านการเงิน และทางธุรกิจ เป็นต้น ที่มีต่อองค์กรเป็นหลัก
เงื่อนไขก่อนการดำเนินกิจกรรม	ความเสี่ยงใดๆ ที่คาดว่าจะเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศขององค์กรได้ถูกกำหนดเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 2. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบการวิเคราะห์และประเมินผลค่าความเสี่ยง
ขั้นตอนการทำงาน	1. เลือกข้อมูลการประเมินมูลค่าสินทรัพย์ประเภทสารสนเทศ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงของแต่ละสินทรัพย์ประเภทสารสนเทศมาใช้เป็นข้อมูลนำเข้า 2. คำนวณผลค่าความเสี่ยง (Risk Value) [12] ตามสมการดังนี้ ค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ = [ผลรวม (ความเป็นไปได้ของภัยคุกคามใดๆ x ระดับความรุณแรงเมื่อภัยคุกคามนั้นโจมตีจุดอ่อนใดๆ)] x มูลค่าสินทรัพย์ประเภทสารสนเทศ Risk Value of Information Asset = [SUM(Likelihood x Servility Scale) x Asset Value] 3. สรุปผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ โดยกำหนดเป็นระดับของการยอมรับความเสี่ยงนั้น

ตารางที่ ข.9 การประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ* (ต่อ)

<table>
<tr><th>หัวข้อ</th><th>คำอธิบาย</th></tr>
<tr><td>ขั้นตอนการทำงาน</td><td><u>หมายเหตุ</u> สมการในการคำนวณผลค่าความเสี่ยงข้างต้นและระดับของการยอมรับความเสี่ยง องค์กรควรอ้างอิงจากการกำหนดในกิจกรรมที่ 5 การกำหนดกลยุทธ์ของการประเมินความเสี่ยง และสำหรับระดับของการยอมรับความเสี่ยงโดยทั่วไปสามารถสรุปได้ดังนี้
<table><tr><td>- สูงที่สุด (Extreme)</td><td>5S + 1 ถึง 6S</td></tr><tr><td>- สูงมาก (Very High)</td><td>4S + 1 ถึง 5S</td></tr><tr><td>- สูง (High)</td><td>3S + 1 ถึง 4S</td></tr><tr><td>- ปานกลาง (Medium)</td><td>2S + 1 ถึง 3S</td></tr><tr><td>- น้อย (Low)</td><td>S + 1 ถึง 2</td></tr><tr><td>- เล็กน้อย (Negligible)</td><td>1 ถึง S</td></tr></table>โดยที่ M คือ ค่าความเสี่ยงที่มากที่สุดที่ได้จากการคำนวณ และ S คือ M / 6</td></tr>
<tr><td>ส่วนนำออก</td><td><<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์</td></tr>
<tr><td>เงื่อนไขการออกจากกิจกรรม</td><td>1. ค่าของความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศได้ถูกวิเคราะห์และประเมินผล
2. สามารถสรุปถึงระดับของการยอมรับความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศได้อย่างชัดเจน</td></tr>
<tr><td>ผู้รับผิดชอบ</td><td>ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง</td></tr>
</table>

ตารางที่ ข.10 การระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ*

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Identify Risk Treatment of Information Asset)
จุดประสงค์	เพื่อระบุถึงการป้องกันรักษาความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศขององค์กร ซึ่งจะกำหนดเป็นแนวคิดและบริการทางด้านความมั่นคง โดยในที่นี้จะมุ่งเน้นการสร้างการควบคุมการเข้าถึงและมีการระบุและพิสูจน์ตัวตนเป็นแบบการใช้งานรหัสผ่าน เนื่องจากมีความเกี่ยวข้องกับการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศโดยตรง
เงื่อนไขก่อนการดำเนินกิจกรรม	1. ค่าความเสี่ยงของแต่ละสินทรัพย์ประเภทสารสนเทศได้ถูกวิเคราะห์และประเมินผลแล้ว 2. ผ่านการสรุประดับของการยอมรับความเสี่ยงของแต่ละสินทรัพย์

ตารางที่ ข.10 การระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ* (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. กำหนดแนวคิดความมั่นคงโดยพิจารณาตามคุณสมบัติด้านความมั่นคงและค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศเป็นหลัก โดยแนวคิดความมั่นคงสามารถแบ่งออกเป็น 3 ด้าน ดังนี้ - การป้องกัน (Detection) - การทวนหา (Prevention) - การตอบสนอง (Response) 2. ระบุระดับความสำคัญของแต่ละแนวคิดความมั่นคงทั้ง 3 ด้านข้างต้น โดยระดับความสำคัญได้แบ่งออกเป็น - สูง (High) - ปานกลาง (Medium) - น้อย (Low) 3. กำหนดบริการความมั่นคงให้กับแต่ละสินทรัพย์ประเภทสารสนเทศ โดยอาศัยข้อมูลจากข้อที่ 1 และ 2 ในการพิจารณา ทั้งนี้ตัวอย่างบริการด้านความมั่นคงเบื้องต้น เช่น - การควบคุมการเข้าถึง (Access Control) - การระบุและพิสูจน์ตัวตน (Identification & Authentication) เป็นต้น
ส่วนนำออก	<<เอกสาร>> เอกสารการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	การป้องกันรักษาความเสี่ยงสำหรับสินทรัพย์ประเภทสารสนเทศใดๆ ได้ถูกระบุอย่างชัดเจน โดยมุ่งเน้นไปในด้านการระบุและพิสูจน์ตัวตน และการควบคุมการเข้าถึงเป็นสำคัญ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

<u>หมายเหตุ</u> เครื่องหมาย * ที่แสดงภายหลังกิจกรรมที่ 7, 8 และ 9 มีการอ้างอิงเนื้อหาของจุดประสงค์ ขั้นตอนการทำงาน รวมถึงเงื่อนไขก่อนและหลังกิจกรรม มาจากแบบรูปความมั่นคง [3] ในบทที่ 6 เรื่องการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง

ตารางที่ ข.11 การกำหนดปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง (Define Factors for Access Control Model Selection)
จุดประสงค์	เพื่อกำหนดปัจจัยในการเลือกใช้โมเดลการควบคุมการเข้าถึง โดยต้องมีความเหมาะสมกับสภาพแวดล้อมโดยรวมขององค์กร
เงื่อนไขก่อนการดำเนินกิจกรรม	ทีมความมั่นคงมีความเข้าใจในเรื่องของโมเดลการควบคุมการเข้าถึง รวมถึงสภาพแวดล้อมโดยรวมขององค์กรเป็นอย่างดี
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง
ขั้นตอนการทำงาน	กำหนดปัจจัยในการเลือกใช้โมเดลการควบคุมการเข้าถึง ซึ่งต้องมีความเหมาะสมกับสภาพแวดล้อมโดยรวมขององค์กร ทั้งนี้ได้ใช้ข้อมูลภายใต้นโยบายและกลยุทธ์การสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศในการกำหนดเป็นหลัก โดยตัวอย่างปัจจัยในการเลือกโมเดล เช่น ขนาดขององค์กร จำนวนผู้ใช้งานสินทรัพย์ประเภทสารสนเทศ การจัดแบ่งระดับของสินทรัพย์ประเภทสารสนเทศ เป็นต้น
ส่วนนำออก	<<เอกสาร>> เอกสารปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง
เงื่อนไขการออกจากกิจกรรม	ปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึงได้ถูกกำหนดอย่างชัดเจน โดยต้องมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.12 การเลือกโมเดลการควบคุมการเข้าถึงที่เหมาะสม

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การเลือกโมเดลการควบคุมการเข้าถึงที่เหมาะสม (Select Access Control Model)
จุดประสงค์	เพื่อเลือกโมเดลการควบคุมการเข้าถึงที่มีความเหมาะสมกับสภาพแวดล้อมโดยรวมขององค์กร ทั้งนี้ได้พิจารณาจากปัจจัยสำหรับการเลือกใช้โมเดลที่ได้กำหนดมาจากกิจกรรมที่ 10 การกำหนดปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง
เงื่อนไขก่อนการดำเนินกิจกรรม	ปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึงได้ถูกกำหนดเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง 2. <<เอกสารแผ่นแบบ>> แผ่นแบบการระบุโมเดลการควบคุมการเข้าถึงที่ความเหมาะสมกับองค์กร
ขั้นตอนการทำงาน	1. เลือกโมเดลการควบคุมการเข้าถึงที่มีความเหมาะสมกับสภาพแวดล้อมโดยรวมขององค์กร โดยพิจารณาจากปัจจัยสำหรับการเลือกใช้โมเดลที่ได้กำหนดมาจากกิจกรรมที่ 10 สำหรับโมเดลการควบคุมการเข้าถึงได้แบ่งออกเป็น - โมเดลการให้อำนาจ (Authorization Model) - โมเดลการเข้าถึงเชิงบทบาท (RBAC Model) - โมเดลความมั่นคงหลายระดับ (Multilevel Security Model) 2. ระบุสาเหตุของการเลือกใช้โมเดลการควบคุมการเข้าถึงนั้น
ส่วนนำออก	<<เอกสาร>>เอกสารการระบุโมเดลการควบคุมการเข้าถึงที่ความเหมาะสมกับองค์กร
เงื่อนไขการออกจากกิจกรรม	ได้โมเดลการควบคุมการเข้าถึงที่มีความเหมาะสมกับสภาพแวดล้อมขององค์กร
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.13 การกำหนดวิธีการการให้อำนาจ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดวิธีการการให้อำนาจ (Define Authorization Method)
จุดประสงค์	เพื่อกำหนดว่า ผู้ใช้งานใดที่มีสิทธิเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรภายใต้สภาพแวดล้อมที่มีการควบคุมการเข้าถึง และเพื่อแสดงให้เห็นว่าสินทรัพย์ประเภทสารสนเทศใดถูกเข้าถึงและเข้าถึงด้วยสิทธิอะไรบ้าง
เงื่อนไขก่อนการดำเนินกิจกรรม	นโยบาย กฎหรือข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องโดยตรงกับการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ได้ถูกรวบรวมเอาไว้เรียบร้อยแล้วภายใต้เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสารแผ่นแบบ>> แผ่นแบบวิธีการการให้อำนาจ
ขั้นตอนการทำงาน	1. ระบุถึงสินทรัพย์ประเภทสารสนเทศขององค์กรที่จะถูกเข้าถึงโดยผู้ใช้งานหรือกลุ่มผู้ใช้งานใดๆ 2. ระบุถึงผู้ใช้งานหรือกลุ่มผู้ใช้งานที่มีสิทธิเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร ซึ่งต้องสัมพันธ์ตามสินทรัพย์ประเภทสารสนเทศที่ได้ระบุไว้ในข้อที่ 1 3. ระบุถึงสิทธิของการเข้าถึงในแต่ละสินทรัพย์ประเภทสารสนเทศของผู้ใช้งานหรือกลุ่มผู้ใช้งานนั้น **<u>หมายเหตุ</u>** ในการระบุข้อที่ 2 และ 3 ให้พิจารณาว่าผู้ใช้งานใดๆ สามารถเข้าถึงสินทรัพย์ประเภทสารสนเทศใดได้บ้าง และด้วยสิทธิการเข้าถึงอะไร
ส่วนนำออก	<<เอกสาร>> เอกสารวิธีการการให้อำนาจ
เงื่อนไขการออกจากกิจกรรม	วิธีการการให้อำนาจในการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้งานได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.14 การกำหนดวิธีการเข้าถึงเชิงบทบาท

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดวิธีการเข้าถึงเชิงบทบาท (Define RBAC Method)
จุดประสงค์	เพื่อกำหนดวิธีการในการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรของผู้ใช้งาน โดยมีการควบคุมการเข้าถึงบนพื้นฐานของบทบาทที่ผู้ใช้งานควรจะได้รับ
เงื่อนไขก่อนการดำเนินกิจกรรม	นโยบาย กฎหรือข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องโดยตรงกับการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ได้ถูกรวบรวมเอาไว้เรียบร้อยแล้วภายใต้เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสารแผ่นแบบ>> แผ่นแบบวิธีการเข้าถึงเชิงบทบาท
ขั้นตอนการทำงาน	1. กำหนดบทบาทในการเข้าถึงแต่ละสินทรัพย์ประเภทสารสนเทศขององค์กร 2. ระบุถึงผู้ใช้งานหรือกลุ่มผู้ใช้งานที่จะได้รับบทบาทนั้นตามที่ได้กำหนดไว้ในข้อที่ 1 3. ระบุถึงสินทรัพย์ประเภทสารสนเทศที่ผู้ใช้งานหรือกลุ่มผู้ใช้งานสามารถเข้าถึงได้ตามบทบาทที่กำหนดไว้ในข้อที่ 1 4. ระบุถึงสิทธิของการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้งานหรือกลุ่มผู้ใช้งานตามบทบาทที่ได้กำหนดไว้ในข้อที่ 1
ส่วนนำออก	<<เอกสาร>> เอกสารวิธีการเข้าถึงเชิงบทบาท
เงื่อนไขการออกจากกิจกรรม	วิธีการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้งานในเชิงบทบาทได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.15 การกำหนดวิธีการของความมั่นคงหลายระดับ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดวิธีการของความมั่นคงหลายระดับ (Define Multilevel Security Method)
จุดประสงค์	เพื่อกำหนดวิธีการของความมั่นคงหลายระดับ โดยวิธีการนี้จะใช้กำหนดในกรณีที่ผู้ใช้งานหรือสินทรัพยสารสนเทศขององค์กรมีระดับความสำคัญที่แตกต่างกันออกไป ซึ่งจะช่วยให้กลุ่มหรือระดับของผู้ใช้งานหรือสินทรัพย์ประเภทสารสนเทศมีการจำแนกออกอย่างชัดเจน รวมถึงการระบุสิทธิของการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่สัมพันธ์กับกลุ่มหรือระดับที่ได้ถูกจำแนกดังกล่าว
เงื่อนไขก่อนการดำเนินกิจกรรม	1. นโยบาย กฎหรือข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องโดยตรงกับการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ และโดยเฉพาะนโยบายด้านการจัดแบ่งประเภทสินทรัพย์ประเภทสารสนเทศได้ถูกรวบรวมเอาไว้เรียบร้อยแล้ว ภายใต้เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. วิธีการการให้อำนาจหรือวิธีการเข้าถึงเชิงบทบาทได้ถูกกำหนดมาก่อนหน้า
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ 3. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสารแผ่นแบบ>> แผ่นแบบวิธีการของความมั่นคงหลายระดับ
ขั้นตอนการทำงาน	1. จำแนกกลุ่มหรือระดับของผู้ใช้งานหรือกลุ่มผู้ใช้งานในแต่ละสินทรัพย์ประเภทสารสนเทศขององค์กร (ถ้ามี) 2. จำแนกกลุ่มหรือระดับของแต่ละสินทรัพย์ประเภทสารสนเทศขององค์กร ซึ่งต้องมีความสัมพันธ์กันกับการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้งานหรือกลุ่มผู้ใช้งาน (ถ้ามี) 3. กำหนดสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยพิจารณาตามกลุ่มหรือระดับของผู้ใช้งานหรือกลุ่มผู้ใช้งาน หรือพิจารณาตามกลุ่มหรือระดับของสินทรัพย์ประเภทสารสนเทศ ตามที่ได้กำหนดไว้ในข้อที่ 1 และ 2

ตารางที่ ข.15 การกำหนดวิธีการของความมั่นคงหลายระดับ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	**<u>หมายเหตุ</u>** กลุ่มหรือระดับของผู้ใช้งานและสินทรัพย์ประเภทสารสนเทศโดยทั่วไปแบ่งออกเป็น - สูงที่สุด (Extreme) - สูงมาก (Very High) - สูง (High) - ปานกลาง (Medium) - น้อย (Low) - เล็กน้อย (Negligible)
ส่วนนำออก	<<เอกสาร>> เอกสารวิธีการของความมั่นคงหลายระดับ
เงื่อนไขการออกจากกิจกรรม	วิธีการของความมั่นคงหลายระดับซึ่งกำหนดให้กับกลุ่มหรือระดับของผู้ใช้งานและสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.16 การกำหนดวิธีการของการตรวจสอบการเข้าถึง

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดวิธีการของการตรวจสอบการเข้าถึง (Define Reference Monitor Method)
จุดประสงค์	เพื่อกำหนดกฎและข้อบังคับสำหรับการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศสำหรับการร้องขอใดๆของผู้ใช้งาน โดยจะตรวจสอบกับเซตของผู้ใช้งานหรือบทบาทที่ได้รับอนุญาตให้เข้าถึงและสิทธิสำหรับผู้ใช้งานหรือบทบาทดังกล่าว
เงื่อนไขก่อนการดำเนินกิจกรรม	1. นโยบาย กฎหรือข้อบังคับ และเอกสารใดๆ ที่เกี่ยวข้องโดยตรงกับการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ได้ถูกรวบรวมเอาไว้เรียบร้อยแล้วภายใต้เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. วิธีการการให้อำนาจหรือวิธีการเข้าถึงเชิงบทบาท รวมถึงวิธีการของความมั่นคงหลายระดับได้ถูกกำหนดมาก่อนหน้านี้แล้ว

ตารางที่ ข.16 การกำหนดวิธีการของการตรวจสอบการเข้าถึง (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	1. <<เอกสาร>> นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารวิธีการการให้อำนาจ หรือ <<เอกสาร>> เอกสารวิธีการเข้าถึงเชิงบทบาท 3. และ/หรือ <<เอกสาร>> เอกสารวิธีการของความมั่นคงหลายระดับ 4. <<เอกสารแผ่นแบบ>> เอกสารกฎและข้อบังคับสำหรับการตรวจสอบการเข้าถึง
ขั้นตอนการทำงาน	กำหนดกฎและข้อบังคับของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศสำหรับการร้องขอและการอนุญาตให้เข้าถึงตามเอกสารวิธีการที่ได้กำหนดมาก่อนหน้านี้ โดยพิจารณาทั้งจากบทบาทที่ผู้ใช้งานได้รับและสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ส่วนนำออก	<<เอกสาร>> เอกสารกฎและข้อบังคับสำหรับการตรวจสอบการเข้าถึง
เงื่อนไขการออกจากกิจกรรม	กฎและข้อบังคับสำหรับการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดอย่างชัดเจน
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.17 การกำหนดความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การกำหนดความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน (Identify Requirements for Password Design and Use)
จุดประสงค์	เพื่อกำหนดความต้องการพื้นฐานสำหรับใช้ในการออกแบบและใช้งานรหัสผ่าน ซึ่งสนับสนุนการทวนสอบผู้ใช้งานในการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร
เงื่อนไขก่อนการดำเนินกิจกรรม	ทีมความมั่นคงต้องมีความเข้าใจในพื้นฐานของการออกแบบและใช้งานรหัสผ่านเป็นอย่างดี
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน

ตารางที่ ข.17 การกำหนดความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. พิจารณาและอภิปรายผลจากการวิเคราะห์เอกสารนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ทั้งนี้เพื่อหาแนวทางในการกำหนดเป็นขอบเขตและความต้องการของการออกแบบและใช้งานรหัสผ่าน 2. ระบุขอบเขตของการออกแบบและใช้งานรหัสผ่าน 3. กำหนดความต้องการของการออกแบบและใช้งานรหัสผ่านในแต่ละขอบเขตที่ระบุไว้ในข้อที่ 1 4. ระบุปัจจัยที่มีผลต่อการกำหนดความต้องการของการออกแบบและใช้งานรหัสผ่าน
ส่วนนำออก	<<เอกสาร>> เอกสารความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน
เงื่อนไขการออกจากกิจกรรม	ความต้องการสำหรับการออกแบบและใช้งานรหัสผ่านได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.18 การออกแบบและใช้งานรหัสผ่าน

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การออกแบบและใช้งานรหัสผ่าน (Define Password Designing and Usage)
จุดประสงค์	เพื่อกำหนดการออกแบบลักษณะหรือคุณสมบัติของรหัสผ่าน รวมถึงการจัดการที่ซึ่งมีความเหมาะสมกับการใช้งานของผู้ใช้ ทั้งนี้จะได้นำไปพัฒนาในระบบเพื่อใช้ระบุและพิสูจน์ตัวตนต่อไป
เงื่อนไขก่อนการดำเนินกิจกรรม	ความต้องการสำหรับการออกแบบและใช้งานรหัสผ่านได้ถูกกำหนดอย่างชัดเจน
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน 2. <<เอกสารแผ่นแบบ>> แผ่นแบบการออกแบบและใช้งานรหัสผ่าน

ตารางที่ ข.18 การออกแบบและใช้งานรหัสผ่าน (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	กำหนดการออกแบบและใช้งานรหัสผ่าน โดยทั่วไปจะกำหนดตามขอบเขตดังต่อไปนี้ 1. กำหนดตัวอักษรที่จะใช้ในรหัสผ่าน เช่น ในลักษณะของตัวเลข หรือตัวอักษร หรือมีการผสมกันระหว่างตัวเลขและตัวอักษร เป็นต้น 2. กำหนดความยาวของรหัสผ่าน ซึ่งควรมีความยาวไม่เกิน 6-8 ตัวอักษร หรือน้อยกว่า หรือมากกว่า ซึ่งแล้วแต่ความเหมาะสมที่จะกำหนดขึ้น 3. กำหนดที่มาของรหัสผ่าน เช่น ได้จากการสร้างแบบอัตโนมัติ เป็นต้น 4. กำหนดอายุการใช้งานของรหัสผ่าน เช่น มีอายุการใช้งานประมาณ 1 เดือน เป็นต้น 5. กำหนดบุคคลที่มีสิทธิในการใช้งานรหัสผ่าน เช่น เฉพาะบุคคล หรือเป็นกลุ่มของผู้ใช้งาน เป็นต้น 6. กำหนดวิธีการในการกรอกรหัสผ่าน เช่น อนุญาตให้กรอกผ่านแป้นคีย์บอร์ดเท่านั้น เป็นต้น 7. กำหนดระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน เช่น มีการตอบสนองภายในเวลา 5 วินาที ภายหลังจากการล็อกอินเข้าสู่ระบบ เป็นต้น 8. กำหนดวิธีการในการส่งรหัสผ่านให้ผู้ใช้งาน เช่น ส่งรหัสผ่านผ่านทางอีเมลของบุคคล เป็นต้น 9. กำหนดวิธีการในการจัดเก็บรหัสผ่าน เช่น ในการจัดเก็บรหัสผ่าน มีการเข้ารหัสก่อนการจัดเก็บ เป็นต้น 10. กำหนดวิธีการในการถ่ายโอนรหัสผ่านเพื่อใช้ในการทวนสอบ เช่น ในระหว่างที่มีการถ่ายโอนนั้นได้มีการเข้ารหัสเอาไว้ เป็นต้น **<u>หมายเหตุ</u>** การกำหนดการออกแบบและใช้งานรหัสผ่านนั้น อาจมีนอกเหนือจาก 10 ข้อกำหนดข้างต้น ทั้งนี้ต้องมีความสอดคล้องเป็นไปตามขอบเขตและความต้องการของการออกแบบและใช้งานรหัสผ่าน ซึ่งได้ถูกกำหนดไว้ในกิจกรรมที่ 15 การกำหนดความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน
ส่วนนำออก	<<เอกสาร>> เอกสารการออกแบบและใช้งานรหัสผ่าน
เงื่อนไขการออกจากกิจกรรม	การออกแบบและใช้งานรหัสผ่านได้ถูกกำหนดไว้เรียบร้อยแล้ว
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.19 การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน (Review Risks of Information Asset and their Treatment, Access Control Definition and Password Design and Use Definition)
จุดประสงค์	เพื่อทำการตรวจสอบข้อกำหนดต่างๆ ที่ได้จากกิจกรรมการระบุความเสี่ยงและการป้องกันรักษาความเสี่ยง การกำหนดวิธีการการควบคุมการเข้าถึง และวิธีการการออกแบบและใช้งานรหัสผ่าน โดยเน้นไปที่ความถูกต้องของการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศขององค์กรเป็นหลัก
เงื่อนไขก่อนการดำเนินกิจกรรม	ความเสี่ยงและการป้องกันรักษาความเสี่ยง วิธีการการควบคุมการเข้าถึง และการออกแบบและใช้งานรหัสผ่านได้ถูกกำหนดเป็นข้อกำหนดขึ้น ภายใต้การสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารปัจจัยสำหรับการเลือกใช้โมเดลการควบคุมการเข้าถึง 5. <<เอกสาร>> เอกสารการระบุโมเดลการควบคุมการเข้าถึงที่ความเหมาะสมกับองค์กร 6. <<เอกสาร>> เอกสารวิธีการการให้อำนาจ หรือ <<เอกสาร>> เอกสารวิธีการเข้าถึงเชิงบทบาท 7. และ/หรือ <<เอกสาร>> เอกสารวิธีการของความมั่นคงหลายระดับ 8. <<เอกสาร>> เอกสารความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน 9. <<เอกสาร>> เอกสารการออกแบบและใช้งานรหัสผ่าน 10. <<เอกสารแผ่นแบบ>> แผ่นแบบรายการตรวจสอบข้อกำหนดสำหรับทีมความมั่นคง

ตารางที่ ข.19 การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. ระบุถึงจุดหรือตำแหน่งที่จะต้องทำการแก้ไข เมื่อเห็นสมควรว่าไม่ถูกต้องหรือไม่เป็นไปตามหลักการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศขององค์กร 2. ระบุถึงสาเหตุของการผิดพลาดหรือไม่ถูกต้อง เมื่อเปรียบเทียบกับหลักการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศ 3. ระบุถึงสิ่งที่ผิดพลาดหรือที่ต้องการแก้ไข ตามจุดหรือตำแหน่งที่ได้ระบุไว้ในข้อที่ 1 รวมถึงระบุระดับความรุนแรงของแต่ละสิ่งที่ผิดพลาดหรือที่ต้องการแก้ไขนั้น 4. ระบุถึงข้อคิดเห็นหรือการแก้ไขที่ถูกต้องของสิ่งที่ผิดพลาดหรือที่ต้องการแก้ไข ตามที่ระบุไว้ในข้อที่ 2
ส่วนนำออก	<<เอกสาร>> เอกสารรายการตรวจสอบข้อกำหนดสำหรับทีมความมั่นคง
เงื่อนไขการออกจากกิจกรรม	รายการตรวจสอบข้อกำหนดต่างๆ ภายใต้การสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่รับผิดชอบโดยทีมความมั่นคงได้ถูกระบุไว้อย่างชัดเจน
ผู้รับผิดชอบ	ทีมความมั่นคงและผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.20 การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน โดยยึดเอานโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นหลัก

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน โดยยึดเอานโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นหลัก (Review Risks of Information Asset and their Treatment, Access Control Definition and Password Design and Use Definition Against with IAAC Policy and Strategy)

ตารางที่ ข.20 การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน โดยยึดเอานโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นหลัก (ต่อ)

หัวข้อ	คำอธิบาย
จุดประสงค์	เพื่อทำการตรวจสอบข้อกำหนดต่างๆ ที่ได้จากกิจกรรมการระบุความเสี่ยงและการป้องกันรักษาความเสี่ยง การกำหนดวิธีการการควบคุมการเข้าถึง และการออกแบบและใช้งานรหัสผ่าน ว่าเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรที่ได้กำหนดไว้หรือไม่
เงื่อนไขก่อนการดำเนินกิจกรรม	ความเสี่ยงและการป้องกันรักษาความเสี่ยง วิธีการการควบคุมการเข้าถึง และการออกแบบและใช้งานรหัสผ่านได้ถูกกำหนดเป็นข้อกำหนดขึ้น ภายใต้การสร้างการควบคุมการเข้าถึงสินทรัพยสารสนเทศ
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารการวิเคราะห์และประเมินผลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารการระบุการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารปัจจัยของการเลือกใช้โมเดลการควบคุมการเข้าถึง 6. <<เอกสาร>> เอกสารระบุถึงโมเดลการควบคุมการเข้าถึงที่ความเหมาะสมกับองค์กร 7. <<เอกสาร>> เอกสารวิธีการการให้อำนาจ หรือ <<เอกสาร>> เอกสารวิธีการเข้าถึงเชิงบทบาท 8. และหรือ <<เอกสาร>> เอกสารวิธีการของความมั่นคงหลายระดับ 9. <<เอกสาร>> เอกสารความต้องการสำหรับการออกแบบและใช้งานรหัสผ่าน 10. <<เอกสาร>> เอกสารการออกแบบและใช้งานรหัสผ่าน 11. <<เอกสารแผ่นแบบ>> แผ่นแบบรายการตรวจสอบข้อกำหนดสำหรับผู้จัดการโครงการ

ตารางที่ ข.20 การตรวจสอบข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น ข้อกำหนดวิธีการการควบคุมการเข้าถึง และข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน โดยยึดเอานโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นหลัก (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. ระบุถึงจุดหรือตำแหน่งที่จะต้องทำการแก้ไข เมื่อเห็นสมควรว่าไม่ถูกต้องหรือไม่เป็นไปตามหลักของนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรที่ได้กำหนดไว้มาตั้งแต่ตอนแรกเริ่มโครงการ 2. ระบุถึงสาเหตุของการผิดพลาดหรือไม่ถูกต้อง เมื่อเปรียบเทียบกับนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. ระบุถึงสิ่งที่ผิดพลาดหรือที่ต้องการแก้ไข ตามจุดหรือตำแหน่งที่ได้ระบุไว้ในข้อที่ 1 รวมถึงระบุระดับความรุนแรงของแต่ละสิ่งที่ผิดพลาดหรือที่ต้องการแก้ไขนั้น 4. ระบุถึงข้อคิดเห็นหรือการแก้ไขที่ถูกต้องของสิ่งที่ผิดพลาดหรือที่ต้องการแก้ไข ตามที่ระบุไว้ในข้อที่ 3
ส่วนนำออก	<<เอกสาร>> เอกสารรายการตรวจสอบข้อกำหนดสำหรับผู้จัดการโครงการ
เงื่อนไขการออกจากกิจกรรม	รายการตรวจสอบข้อกำหนดต่างๆ ภายใต้การสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่รับผิดชอบโดยผู้จัดการโครงการได้ถูกระบุไว้อย่างชัดเจน
ผู้รับผิดชอบ	ผู้จัดการโครงการ หัวหน้าทีมความมั่นคง และผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.21 การวางแผนสำหรับการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การวางแผนสำหรับการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Plan IAAC System)
จุดประสงค์	เพื่อวางแผนสำหรับการพัฒนาระบบในการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร
เงื่อนไขก่อนการดำเนินกิจกรรม	กลยุทธ์และกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดมาก่อนหน้านี้แล้วในกิจกรรมที่ 4 การปรับนโยบายของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้สอดคล้องกับกลยุทธ์ขององค์กรด้านการจัดการความเสี่ยง

ตารางที่ ข.21 การวางแผนสำหรับการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสารแผ่นแบบ>> แผ่นแบบแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสารแผ่นแบบ>> แผ่นแบบการจัดการความเสี่ยงในการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสารแผ่นแบบ>> แผ่นแบบแผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. วางแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยระบุเป็นกิจกรรมก่อน-หลัง ทั้งนี้กิจกรรมที่เกิดขึ้นควรอยู่ภายใต้ระเบียบวิธี (Methodology) ที่ได้กำหนดเอาไว้ 2. แสดงถึงโครงสร้างของกิจกรรม (Work Break Down Structure) ที่เกิดขึ้นในการพัฒนาระบบ รวมถึงโครงสร้างของผลิตภัณฑ์ (Product Break Down Structure) ซึ่งเป็นไปตามโครงสร้างกิจกรรมดังกล่าว 3. กำหนดระยะเวลาที่ใช้ในแต่ล่ะกิจกรรมของการพัฒนา จนเสร็จสิ้นการส่งมอบระบบที่ได้ 4. ระบุถึงมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาระบบ รวมถึงเทคโนโลยีที่ต้องการนำมาใช้ 5. กำหนดงบประมาณและทรัพยากรที่จำเป็นต้องใช้ในการพัฒนาระบบ ทั้งนี้จะต้องคำนึงถึงความคุ้มทุนเป็นหลัก 6. ระบุถึงสมาชิกภายใต้ทีมพัฒนาระบบ รวมถึงระบุหน้าที่ความรับผิดชอบให้กับสมาชิก

ตารางที่ ข.21 การวางแผนสำหรับพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์สารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	**<u>หมายเหตุ</u>** ทั้งนี้ในการวางแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนั้น จะต้องมีการกำหนดการจัดการความเสี่ยง (Risk Management) ที่อาจจะเกิดขึ้นระหว่างการพัฒนาระบบ ทั้งนี้เพื่อใช้ในการควบคุมการพัฒนาให้เป็นตามแผนการพัฒนาระบบที่ได้วางเอาไว้ นอกจากนี้ยังรวมถึงแผนที่ใช้ในการทดสอบระบบ (Test Plan) ซึ่งจะกระทำการทดสอบในระหว่างการพัฒนาและภายหลังจากการพัฒนาเสร็จสิ้น เพื่อทดสอบว่าระบบที่ได้สามารถควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพหรือไม่ ดังนั้นจะเห็นได้ว่ามีกิจกรรมย่อยเกิดขึ้น 2 กิจกรรม โดยในแต่ละกิจกรรมมีสิ่งที่ต้องคำนึงถึง ดังต่อไปนี้ <u>กิจกรรม 19.2 การจัดการความเสี่ยง</u> 1. ระบุความเสี่ยงที่อาจจะเกิดขึ้นในช่วงระหว่างการพัฒนาระบบ รวมถึงประเภทของความเสี่ยงนั้น เช่น การบริหารจัดการการพัฒนาระบบ (Project Management) เทคนิคของการพัฒนา (Technical) ส่วนภายนอกที่มีความเกี่ยวข้อง (External) เป็นต้น 2. ระบุระดับของความเสี่ยง ระดับโอกาสของการเกิดความเสี่ยง รวมถึงระดับความรุนแรงของผลกระทบเมื่อความเสี่ยงนั้นเกิดขึ้น 3. กำหนดวิธีการในการจัดการกับความเสี่ยงนั้น <u>กิจกรรม 19.3 การวางแผนการทดสอบระบบ</u> 1. กำหนดระเบียบวิธีที่ใช้ในการทดสอบระบบ วัตถุประสงค์และขอบเขตของการทดสอบ ระดับของการยอมรับ ส่วนที่ต้องการทำการทดสอบ รวมถึงผลิตภัณฑ์ที่ได้จากการทดสอบ 2. กำหนดระยะเวลาของการทดสอบระบบ มาตรฐานต่างๆ ที่เกี่ยวข้อง งบประมาณและผู้ที่มีหน้าที่รับผิดชอบ
ส่วนนำออก	1. <<เอกสาร>> เอกสารแผนพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ 2. <<เอกสารแผ่นแบบ>> แผ่นแบบการจัดการความเสี่ยงในการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบแผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ได้ถูกกำหนดอย่างชัดเจนและสอดคล้องเป็นไปตามกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์สารสนเทศ
ผู้รับผิดชอบ	ผู้จัดการโครงการ หัวหน้าทีมความมั่นคง และผู้เชี่ยวชาญด้านความมั่นคง

ตารางที่ ข.22 การวางแผนสำหรับการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การวางแผนสำหรับการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Plan for Monitoring and Reviewing)
จุดประสงค์	เพื่อวางแผนสำหรับการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร ทั้งนี้เพื่อให้ระบบมีการทำงานในการควบคุมการเข้าถึงเป็นไปอย่างมีประสิทธิภาพและเป็นไปตามหลักการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขก่อนการดำเนินกิจกรรม	มีการกำหนดแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 3. <<เอกสาร>> เอกสารการจัดการความเสี่ยงที่คงเหลือ 4. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น 5. <<เอกสาร>> เอกสารข้อกำหนดวิธีการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 7. <<เอกสารแผ่นแบบ>> แผ่นแบบแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. วางแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยในการวางแผนนั้นจะต้องคำนึงถึง 1.1 กำหนดวัตถุประสงค์และขอบเขตของการเฝ้าสังเกตและทวนสอบระบบ รวมถึงการประเมินประสิทธิภาพ โดยพิจารณาว่า จะต้องมุ่งสังเกตและตรวจสอบในประสิทธิภาพของระบบ เพื่อที่จะสามารถสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศอย่างสูงสุด 1.2 ระบุตัวชี้วัดสำหรับใช้ประเมินประสิทธิภาพการทำงานในด้านต่างๆ ของระบบ โดยมุ่งเน้นไปที่การควบคุมการเข้าถึงของแต่ละสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ข.22 การวางแผนสำหรับการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1.3 ระบุถึงค่าคาดหมายในแต่ละตัวชี้วัดของประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ต้องการบรรลุ 1.4 เลือกและกำหนดวิธีการประเมินประสิทธิภาพของระบบ ซึ่งต้องมีความสอดคล้องกับตัวชี้วัดในด้านต่างๆ ที่ได้กำหนดไว้ 1.5 การกำหนดส่วนนำเข้าและออก ฟังก์ชันหรือส่วนการทำงานใดๆ ของระบบ ความเสี่ยงของสินทรัพย์ประเภทสารสนเทศที่จะต้องทำการเฝ้าสังเกตและทวนสอบ รวมถึงส่วนการประเมินประสิทธิภาพ ซึ่งต้องสอดคล้องกับตัวชี้วัดที่ได้ทำการระบุเอาไว้ ยกตัวอย่างเช่น - ภัยคุกคามและจุดอ่อนที่ได้ทำการประเมินความเสี่ยงไว้ก่อนหน้า อีกทั้งยังรวมถึงความเสี่ยงใดๆ ที่อาจขึ้นใหม่ - การกระทำและการป้องกันใดๆ ที่เป็นผลจากการวัดประสิทธิภาพและการปรับปรุงระบบ - ข้อเสนอแนะของการปรับปรุงจากผู้ที่เกี่ยวข้องกับกระบวนการ เป็นต้น 2. กำหนดระยะเวลาที่ใช้สำหรับเฝ้าสังเกตและทวนสอบระบบ โดยการกำหนดนั้นเป็นระยะเวลาหนึ่งภายหลังจากที่ผู้ใช้ได้ดำเนินการใช้งานไปแล้ว 3. ระบุถึงมาตรฐานต่างๆ ที่เกี่ยวข้องกับการเฝ้าสังเกตุและทวนสอบระบบ รวมถึงเทคโนโลยีที่ต้องการนำมาใช้ 4. กำหนดงบประมาณและทรัพยากรที่จำเป็นต้องใช้ในการเฝ้าสังเกตุและทวนสอบระบบ ทั้งนี้จะต้องคำนึงถึงความคุ้มทุนเป็นหลัก 5. ระบุถึงสมาชิกภายใต้ทีมเฝ้าสังเกตและทวนสอบระบบ รวมถึงระบุหน้าที่ความรับผิดชอบให้กับสมาชิก 6. รายงานการวางแผนทั้งแผนการพัฒนาระบบและแผนการเฝ้าสังเกตและทวนสอบให้กับผู้บริหารระดับสูงได้รับทราบ

ตารางที่ ข.22 การวางแผนสำหรับการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

<table>
<tr><th>หัวข้อ</th><th>คำอธิบาย</th></tr>
<tr><td>ขั้นตอนการทำงาน</td><td><u>หมายเหตุ</u> ในการวางแผนนั้น ควรมีการกำหนดระยะเวลาในลักษณะวนซ้ำและเป็นไปอย่างต่อเนื่องของการเฝ้าสังเกตและทวนสอบระบบ และสำหรับตัวชี้วัดประสิทธิภาพของระบบสามารถยกตัวอย่าง [15] ได้ต่อไปนี้
<table>
<tr><td rowspan="2">Secure Logger</td><td>M1. จำนวนล็อกไฟล์ของการร้องขอการเข้าใช้งานระบบนั้น จะต้องถูกนำมาเปรียบเทียบกับรายการล็อกที่ถูกบันทึกไว้ ซึ่งผลการเปรียบเทียบต้องให้ผลที่เท่ากัน</td></tr>
<tr><td>M2. จำเป็นต้องมีการจัดเตรียมส่วนของการตรวจสอบล็อกเอนทรี (Log Entries) เพื่อนับจำนวนของล็อกเอนทรีที่ผิดพลาด</td></tr>
<tr><td rowspan="2">Authentication Enforcer</td><td>M3. จำนวนของการร้องขอการเข้าถึงระบบ จะต้องถูกนำมาเปรียบเทียบกับจำนวนของการร้องขอการระบุและพิสูจน์ตัวตน</td></tr>
<tr><td>M4. จำนวนของความสำเร็จของการระบุและพิสูจน์ตัวตน ลบด้วยจำนวนของเหตุการณ์ของการล็อกเอาท์นั้น ต้องเท่ากับจำนวนของการสร้างการระบุและพิสูจน์ตัวตน</td></tr>
</table></td></tr>
<tr><td>ส่วนนำออก</td><td>1. <<เอกสาร>> เอกสารแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
2. <<เอกสาร>> เอกสารอนุมัติให้ดำเนินการพัฒนาระบบจากผู้บริหารระดับสูง</td></tr>
<tr><td>เงื่อนไขการออกจากกิจกรรม</td><td>1. แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดอย่างชัดเจน และมีความสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
2. แผนการพัฒนาและแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศถูกพิจารณาเห็นชอบและอนุมัติจากผู้บริหารระดับสูงเรียบร้อยแล้ว</td></tr>
<tr><td>ผู้รับผิดชอบ</td><td>ผู้จัดการโครงการ หัวหน้าทีมความมั่นคง และผู้เชี่ยวชาญด้านความมั่นคง</td></tr>
</table>

ตารางที่ ข.23 การฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Train IAAC Team and Stakeholders)
จุดประสงค์	เพื่อทำการฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องให้มีความรู้ความเข้าใจเกี่ยวกับการสร้างการควบคุมการเข้าถึงสินทรัพย์สารสนเทศขององค์กร ทั้งนี้เพื่อให้การสร้างการควบคุมการเข้าถึงที่ได้มีประสิทธิภาพอย่างสูงสุด
เงื่อนไขก่อนการดำเนินกิจกรรม	ได้ทำการระบุสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องทั้งหมดเรียบร้อยแล้ว
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารเป้าหมายและพันธกิจของการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ 3. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ 4. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น 6. <<เอกสาร>> เอกสารข้อกำหนดวิธีการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 7. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 8. <<เอกสาร>> เอกสารแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 9. <<เอกสาร>> เอกสารแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 10. <<เอกสารแผ่นแบบ>> แผ่นแบบแผนการฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 11. <<เอกสารแผ่นแบบ>> แผ่นแบบเอกสารการฝึกอบรมสำหรับสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 12. <<เอกสารแผ่นแบบ>> แผ่นแบบการประเมินการฝึกอบรมสำหรับสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 13. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานผลการประเมินและสรุปผลการฝึกอบรม

ตารางที่ ข.23 การฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. วิเคราะห์ส่วนนำเข้าของกิจกรรมนี้ เพื่อจัดเตรียมเป็นเอกสารเพื่อการฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 2. วางแผนการฝึกอบรม โดยกำหนดเป็นขอบเขตของการฝึกอบรม วัตถุประสงค์หรือจุดมุ่งหมาย กำหนดการ ระยะเวลา สถานที่สำหรับการฝึกอบรม มาตรฐานต่างๆ เทคโนโลยีที่ใช้ งบประมาณ รวมถึงการระบุผู้ที่มีหน้าที่รับผิดชอบในการฝึกอบรม 3. กำหนดเกณฑ์และระดับในการประเมินผลการฝึกอบรม 4. จัดดำเนินการฝึกอบรมตามแผนการฝึกอบรม 5. ประเมินผลการฝึกอบรม 6. สรุปผลเพื่อวางแผนปรับปรุงการฝึกอบรมในครั้งต่อไป
ส่วนนำออก	1. <<เอกสาร>> เอกสารแผนการฝึกอบรมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 2. <<เอกสาร>> เอกสารการฝึกอบรมสำหรับสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 3. <<ฟอร์ม>> แบบฟอร์มการประเมินการฝึกอบรมสำหรับสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง 4. <<เอกสาร>> เอกสารรายงานผลการประเมินและสรุปผลการฝึกอบรม
เงื่อนไขการออกจากกิจกรรม	เชื่อได้ว่าสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องจะสามารถดำเนินการตามบทบาทและหน้าที่ความรับผิดชอบได้อย่างถูกต้อง จนเป็นผลให้การสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศมีประสิทธิภาพ
ผู้รับผิดชอบ	ทีมความมั่นคง

ตารางที่ ข.24 การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Implement IAAC System)
จุดประสงค์	เพื่อทำการพัฒนาระบบซึ่งจะใช้ในการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร
เงื่อนไขก่อนการดำเนินกิจกรรม	สมาชิกของทีมพัฒนาระบบด้านความมั่นคงมีความรู้ความเข้าใจในการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศเป็นอย่างดี
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยง 6. <<เอกสาร>> เอกสารข้อกำหนดวิธีการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 7. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 8. <<เอกสารแผ่นแบบ>> แผ่นแบบความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 9. <<เอกสารแผ่นแบบ>> แผ่นแบบกรณีทดสอบที่ใช้ทดสอบระบบ 10. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานผลการทดสอบและสรุปผลการทดสอบระบบ 11. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานความก้าวหน้าของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 12. <<เอกสารแผ่นแบบ>> แผ่นแบบการจัดการกับการเปลี่ยนแปลงที่อาจเกิดขึ้นระหว่างการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 13. <<เอกสารแผ่นแบบ>> แผ่นแบบรายการตรวจสอบของการพัฒนาระบบ

ตารางที่ ข.24 การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. วิเคราะห์ความต้องการและออกแบบฟังก์ชันการทำงานหลัก รวมทั้งส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. ออกแบบกรณีทดสอบตามวิธีการทดสอบที่ได้กำหนดไว้ในแผนของการทดสอบระบบภายใต้กิจกรรมที่ 19 การวางแผนสำหรับการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ทั้งนี้เพื่อใช้ในการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศในระหว่างที่พัฒนาและเมื่อพัฒนาเสร็จสิ้นแล้ว 3. ดำเนินการพัฒนาระบบตามแผนที่ได้วางเอาไว้ในกิจกรรมที่ 19 การวางแผนสำหรับการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. เมื่อเสร็จสิ้นการพัฒนา ให้ทำการทดสอบระบบด้วยกรณีทดสอบที่ได้ออกแบบไว้ในข้อที่ 2 ทั้งนี้เพื่อให้ได้ระบบที่สามารถดำเนินการตามความต้องการที่ได้ระบุไว้ในข้อที่ 1 5. บันทึกและสรุปผลการทดสอบ ทั้งนี้เพื่อใช้ในการแก้ไขและปรับปรุงระบบก่อนการส่งมอบ 6. ส่งมอบระบบที่เสร็จสมบูรณ์ **<u>หมายเหตุ</u>** ในขณะที่ทำการพัฒนาระบบนั้น ทีมพัฒนาควรมีการรายงานความก้าวหน้า (Progress Reporting) กับผู้จัดการโครงการเป็นระยะๆ ตามกำหนดเวลาในแผนงาน นอกจากนี้ควรมีการจัดการกับการเปลี่ยนแปลง (Change Management) ที่อาจจะเกิดขึ้น ซึ่งการเปลี่ยนแปลงดังกล่าวอาจจะทำให้การพัฒนาระบบนั้นไม่เป็นไปตามแผนงานที่ได้วางเอาไว้ตั้งแต่เริ่มพัฒนาระบบ รวมถึงเมื่อพัฒนาส่วนใดส่วนหนึ่งเสร็จสิ้น ควรทำรายการตรวจสอบ (Project Checklist) เพื่อตรวจสอบว่า การพัฒนาระบบได้พัฒนาครบตามความต้องการที่ได้ออกแบบไว้แล้ว ดังนั้นจะเห็นได้ว่ามีกิจกรรมย่อยเกิดขึ้น 3 กิจกรรม โดยในแต่ละกิจกรรมมีสิ่งที่ต้องคำนึงถึง ดังต่อไปนี้ <u>กิจกรรม 23.1 การรายงานความก้าวหน้าของการพัฒนาระบบ</u> 1. ระบุกิจกรรมหรือส่วนการพัฒนาที่ต้องการส่งมอบพร้อมอธิบายรายละเอียด รวมถึงช่วงระยะเวลาที่ใช้ในการพัฒนากิจกรรมนั้น 2. ระบุถึงการเสนอแนะเมื่อเห็นกิจกรรมหรือส่วนการพัฒนานั้นยังไม่สมบูรณ์และในกรณีที่ต้องการมอบหมายงานต่อเนื่อง ทั้งนี้ต้องระบุช่วงระยะเวลาของการพัฒนาส่วนการปรับปรุงหรือส่วนเพิ่มเติมด้วย

ตารางที่ ข.24 การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	<u>กิจกรรม 23.2 การจัดการกับการเปลี่ยนแปลงที่อาจเกิดขึ้นระหว่างการพัฒนาระบบ</u> 1. ระบุกิจกรรมหรือส่วนการพัฒนาที่เกิดการเปลี่ยนแปลง ระดับความสำคัญของกิจกรรมหรือส่วนการพัฒนานั้น สาเหตุของการเปลี่ยนแปลง และผลกระทบโดยรวมที่เกิดขึ้นกับการพัฒนาระบบ 2. วิเคราะห์การเปลี่ยนแปลงนั้นว่ามีผลกระทบในด้านต่างๆ อย่างไรบ้าง เช่น ด้านความต้องการของระบบ ด้านความเสี่ยงที่อาจจะเกิดขึ้นระหว่างการพัฒนาระบบ ด้านระยะเวลา ด้านงบประมาณ เป็นต้น 3. อภิปรายและสรุปถึงสิ่งที่ต้องจัดการกับการเปลี่ยนแปลงที่อาจจะเกิดขึ้น พร้อมระบุเหตุผลถึงสิ่งที่ได้สรุปนั้น <u>กิจกรรม 23.3 รายการตรวจสอบของการพัฒนาระบบ</u> 1. ระบุถึงรายการที่ต้องทำการตรวจสอบว่าได้ดำเนินการเสร็จสิ้นแล้วหรือไม่ ทั้งในส่วนการพัฒนาและผลิตภัณฑ์ที่ได้จากการพัฒนานั้น 2. ระบุสถานะของรายการตรวจสอบว่าอยู่ในสถานะใด เช่น ยังไม่ได้ทำการพัฒนา อยู่ระหว่างการพัฒนา หรือพัฒนาเสร็จสิ้นเรียบร้อยแล้ว เป็นต้น
ส่วนนำออก	1. <<เอกสาร>> เอกสารความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารกรณีทดสอบที่ใช้ทดสอบระบบ 3. <<เอกสาร>> เอกสารรายงานผลการทดสอบและสรุปผลการทดสอบระบบ 4. <<เอกสาร>> เอกสารรายงานความก้าวหน้าของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารการจัดการกับการเปลี่ยนแปลงที่อาจเกิดขึ้นระหว่างการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 6. <<เอกสาร>> เอกสารรายการตรวจสอบของการพัฒนาระบบ 7. <<ระบบ>> ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกสร้างขึ้นและมีการส่งมอบเรียบร้อยแล้ว
ผู้รับผิดชอบ	ทีมพัฒนาระบบด้านความมั่นคง

ตารางที่ ข.25 การฝึกอบรมผู้ใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การฝึกอบรมผู้ใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Train Users and Aware of IAAC System)
จุดประสงค์	เพื่อทำการฝึกอบรมผู้ใช้งานให้มีความรู้ความเข้าใจเบื้องต้นเกี่ยวกับการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร
เงื่อนไขก่อนการดำเนินกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้พัฒนาเสร็จสิ้น
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารเป้าหมายและพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยง 6. <<เอกสาร>> เอกสารข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 7. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 8. <<เอกสาร>> เอกสารความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 9. <<ระบบ>> ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 10. <<เอกสารแผ่นแบบ>> แผ่นแบบแผนการฝึกอบรมผู้ใช้งาน 11. <<เอกสารแผ่นแบบ>> แผ่นแบบเอกสารการฝึกอบรมสำหรับผู้ใช้งาน 12. <<เอกสารแผ่นแบบ>> แผ่นแบบการประเมินการฝึกอบรมสำหรับผู้ใช้งาน 13. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานผลการประเมินและสรุปผลการฝึกอบรม

ตารางที่ ข.25 การฝึกอบรมผู้ใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. วิเคราะห์ส่วนนำเข้าของกิจกรรมนี้ เพื่อจัดเตรียมเป็นเอกสารเพื่อใช้ฝึกอบรมผู้ใช้งาน 2. วางแผนการฝึกอบรม โดยกำหนดเป็นขอบเขตของการฝึกอบรม วัตถุประสงค์หรือจุดมุ่งหมาย กำหนดการ ระยะเวลา สถานที่สำหรับการฝึกอบรม มาตรฐานต่างๆ เทคโนโลยที่ใช้ งบประมาณ รวมถึงการระบุผู้ที่มีหน้าที่รับผิดชอบในการฝึกอบรม 3. กำหนดเกณฑ์และระดับในการประเมินผลการฝึกอบรม 4. จัดดำเนินการฝึกอบรมตามแผนการฝึกอบรม 5. ประเมินผลการฝึกอบรม 6. สรุปผลเพื่อวางแผนปรับปรุงการฝึกอบรมในครั้งต่อไป
ส่วนนำออก	1. <<เอกสาร>> เอกสารแผนการฝึกอบรมผู้ใช้งาน 2. <<เอกสาร>> เอกสารการฝึกอบรมสำหรับผู้ใช้งาน 3. <<ฟอร์ม>> แบบฟอร์มการประเมินการฝึกอบรมสำหรับผู้ใช้งาน 4. <<เอกสาร>> เอกสารรายงานผลการประเมินและสรุปผลการฝึกอบรม
เงื่อนไขการออกจากกิจกรรม	เชื่อได้ว่าผู้ใช้งานสามารถใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้อย่างถูกต้องและมีประสิทธิภาพ
ผู้รับผิดชอบ	ทีมพัฒนาระบบด้านความมั่นคง

ตารางที่ ข.26 การดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Operate IAAC System)
จุดประสงค์	เพื่อให้ผู้ใช้ได้ดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กร
เงื่อนไขก่อนการดำเนินกิจกรรม	ผู้ใช้ได้ผ่านการฝึกอบรมการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ และระบบมีสภาพพร้อมใช้ทั้งการติดตั้งที่เป็นฮาร์ดแวร์และซอฟต์แวร์
ส่วนนำเข้า	1. <<ระบบ>> ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<ระบบ>> แผ่นแบบรายงานบันทึกการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้

ตารางที่ ข.26 การดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. ดำเนินการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรตามสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ตามที่ได้กำหนดไว้ 2. ในกรณีที่การดำเนินการใช้งานระบบเกิดความผิดพลาดหรือมีข้อขัดข้อง ให้ระบบบันทึกสิ่งที่ผิดพลาดหรือข้อขัดข้องนั้น พร้อมทั้งระบุที่มาและสาเหตุของการเกิด
ส่วนนำออก	<<ระบบ>> เอกสารรายงานบันทึกการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้
เงื่อนไขการออกจากกิจกรรม	ผู้ใช้สามารถใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศขององค์กรไปในช่วงระยะเวลาหนึ่ง
ผู้รับผิดชอบ	ผู้ใช้งานระบบ

ตารางที่ ข.27 การดำเนินการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การดำเนินการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Execute Monitoring and Reviewing IAAC System)
จุดประสงค์	เพื่อเฝ้าสังเกตและทวนสอบประสิทธิภาพการทำงานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ว่าเป็นไปตามขอบเขต เป้าหมายและพันธกิจ นโยบาย กลยุทธ์และกระบวนการที่ได้กำหนดไว้ตั้งแต่เริ่มจัดตั้งโครงการหรือไม่
เงื่อนไขก่อนการดำเนินกิจกรรม	1. แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ได้ถูกกำหนดเป็นเอกสาร 2. ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกใช้งานจากผู้ใช้มาในระยะเวลาหนึ่ง
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 2. <<เอกสาร>> เอกสารการจัดการความเสี่ยงที่คงเหลือ 3. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยง 4. <<เอกสาร>> เอกสารข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ 5. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน

ตารางที่ ข.27 การดำเนินการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	6. <<เอกสาร>> เอกสารความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 7. <<เอกสาร>> เอกสารแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 8. <<เอกสาร>> เอกสารรายงานบันทึกการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ 9. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. ดำเนินการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยเน้นไปที่ประสิทธิภาพของการทำงาน ส่วนนำเข้าและออก รวมถึงส่วนการทำงานใดๆ ของระบบตามแผนการที่ได้กำหนดเอาไว้ 2. ดำเนินการทวนสอบความเสี่ยงของสินทรัพย์สารสารเทศภายใต้ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศกับกลยุทธ์ของการประเมินความเสี่ยงที่ได้กำหนดไว้ นอกจากนี้ควรมีการทวนสอบในส่วนของความเสี่ยงที่คงเหลือด้วย 3. บันทึกผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยระบุเป็นส่วนนำเข้าและออก ส่วนการทำงานหรือความเสี่ยงของสินทรัพย์ประเภทสารสนเทศที่ได้ทำการเฝ้าสังเกตและทวนสอบ กระทำภายใต้ตัวชี้วัดใด ผลที่ได้จากการเฝ้าสังเกต และข้อเสนอแนะเพิ่มเติมจากผู้ที่ดำเนินการ
ส่วนนำออก	<<เอกสาร>> เอกสารรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ผ่านการเฝ้าสังเกตและทวนสอบ โดยมีการบันทึกผลเป็นรายงานเรียบร้อยแล้ว
ผู้รับผิดชอบ	ทีมเฝ้าสังเกตและทวนสอบด้านความมั่นคง

ตารางที่ ข.28 การประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Measure Effectiveness of IAAC System)
จุดประสงค์	เพื่อทำการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ตามแผนการและตัวชี้วัดที่กำหนดเอาไว้ด้วยวิธีการประเมินที่เหมาะสม
เงื่อนไขก่อนการดำเนินกิจกรรม	1. แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดเป็นเอกสาร 2. ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกเฝ้าสังเกตและทวนสอบประสิทธิภาพเรียบร้อยแล้ว
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 2. <<เอกสาร>> เอกสารการจัดการความเสี่ยงที่คงเหลือ 3. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยง 4. <<เอกสาร>> เอกสารข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 6. <<เอกสาร>> เอกสารความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 7. <<เอกสาร>> เอกสารแผนการเฝ้าสังเกตและทวนสอบระบบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 8. <<เอกสาร>> เอกสารรายงานบันทึกการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้ 9. <<เอกสาร>> เอกสารรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 10. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานบันทึกผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ข.28 การประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. วิเคราะห์และประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศตามวิธีการและตัวชี้วัดที่ได้กำหนดเอาไว้ โดยยึดเอาบันทึกการใช้งานระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้และผลการเฝ้าสังเกตและทวนสอบระบบเป็นข้อมูลนำเข้าเป็นหลัก 2. บันทึกผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยระบุเป็นผลการวิเคราะห์เมื่อเทียบกับค่าคาดหมายของตัวชี้วัด และตัวชี้วัดนั้นระบุอยู่ภายใต้ประสิทธิภาพในด้านใด รวมถึงระดับในการยอมรับค่าที่ได้จากการประเมินผล 3. สรุปผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ส่วนนำออก	<<เอกสาร>> เอกสารรายงานบันทึกผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกประเมินประสิทธิภาพของการทำงานด้วยวิธีการประเมินที่เหมาะสมเรียบร้อยแล้ว
ผู้รับผิดชอบ	ทีมเฝ้าสังเกตและทวนสอบด้านความมั่นคง

ตารางที่ ข.29 การปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Update Monitoring and Reviewing Plan)
จุดประสงค์	เพื่อทำการปรับปรุงแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้มีความเหมาะสม สามารถนำไปใช้เป็นแผนการเฝ้าสังเกตและทวนสอบระบบในครั้งต่อไป
เงื่อนไขก่อนการดำเนินกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกเฝ้าสังเกตและทวนสอบ และผ่านการประเมินประสิทธิภาพเรียบร้อยแล้ว
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ข.29 การปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	3. <<เอกสาร>> เอกสารรายงานบันทึกผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสารแผ่นแบบฉบับใหม่>> แผ่นแบบแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานบันทึกผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. วิเคราะห์วิธีการประเมินประสิทธิภาพระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ควบคู่กับรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบและรายงานบันทึกผลการประเมินประสิทธิภาพของระบบ 2. อภิปรายผลการวิเคราะห์ที่ได้จากข้อที่ 1 เพื่อหาแนวทางในการปรับปรุงแผนการเฝ้าสังเกตและทวนสอบระบบในครั้งถัดไปให้มีความเหมาะสม ทั้งนี้เพื่อต้องการให้ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศมีการทำงานที่ถูกต้องและมีประสิทธิภาพเป็นไปตามหลักการสร้างความมั่นคงให้กับสินทรัพย์ประเภทสารสนเทศ 3. ปรับปรุงแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศตามผลการอภิปรายในข้อที่ 2 4. บันทึกผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยระบุเป็นส่วนที่ได้ทำการปรับปรุง เช่น ส่วนนำเข้าและออก ส่วนการทำงานใดๆ ของระบบ ความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ หรือตัวชี้วัดประสิทธิภาพ เป็นต้น รวมถึงสาเหตุของการปรับปรุงส่วนนั้น
ส่วนนำออก	1. <<เอกสารฉบับใหม่>> เอกสารแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศฉบับใหม่ 2. <<เอกสาร>> เอกสารรายงานบันทึกผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกปรับปรุงเรียบร้อยแล้ว
ผู้รับผิดชอบ	ทีมเฝ้าสังเกตและทวนสอบด้านความมั่นคง

ตารางที่ ข.30 การบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Record Actions and Events that Impact on Effectiveness of IAAC System)
จุดประสงค์	เพื่อบันทึกการกระทำและเหตุการณ์ที่ซึ่งส่งผลกระทบต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ทั้งนี้ข้อมูลที่ได้จะถูกนำไปวิเคราะห์เพื่อเลือกการปรับปรุงที่เหมาะสมต่อไป
เงื่อนไขก่อนการดำเนินกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกเฝ้าสังเกตและทวนสอบ และผ่านการประเมินประสิทธิภาพเรียบร้อยแล้ว
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารวิธีการประเมินประสิทธิภาพระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารรายงานบันทึกผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. วิเคราะห์วิธีการประเมินประสิทธิภาพระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ควบคู่กับรายงานบันทึกผลการเฝ้าสังเกตและทวนสอบระบบและรายงานบันทึกผลการประเมินประสิทธิภาพของระบบ 2. อภิปรายผลการวิเคราะห์ที่ได้จากข้อที่ 1 เพื่อระบุเป็นการกระทำและเหตุการณ์ที่ซึ่งส่งผลกระทบต่อประสิทธิภาพการทำงานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. สรุปและบันทึกเป็นการกระทำและเหตุการณ์ รวมถึงระบุถึงระดับของการส่งผลกระทบและผลกระทบที่เกิดขึ้นจริง
ส่วนนำออก	<<เอกสาร>> เอกสารรายงานบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	การกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกบันทึกไว้เรียบร้อยแล้ว
ผู้รับผิดชอบ	ทีมเฝ้าสังเกตและทวนสอบด้านความมั่นคง

ตารางที่ ข.31 การกำหนดการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	กำหนดการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Select Corrective and Preventive Action)
จุดประสงค์	เพื่อกำหนดการกระทำและการป้องกันที่เหมาะสมสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ภายหลังจากการเฝ้าสังเกตและทวนสอบระบบ
เงื่อนไขก่อนการดำเนินกิจกรรม	รายงานบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศถูกกำหนดเป็นเอกสาร
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ 3. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์สารสนเทศ 4. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 5. <<เอกสาร>> เอกสารการจัดการความเสี่ยงที่คงเหลือ 6. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยง 7. <<เอกสาร>> เอกสารข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 8. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 9. <<เอกสาร>> เอกสารความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 10. <<เอกสาร>> เอกสารรายงานบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 11. <<เอกสารฉบับก่อนหน้า>> เอกสารการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ถ้ามี) 12. <<เอกสารแผ่นแบบ>> แผ่นแบบการวิเคราะห์กระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 13. <<เอกสารแผ่นแบบ>> แผ่นแบบการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ข.31 การกำหนดการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	1. วิเคราะห์รายงานบันทึกการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. อภิปรายผลการวิเคราะห์ที่ได้จากข้อที่ 1 เพื่อระบุระดับและผลของการยอมรับการกระทำหรือเหตุการณ์ที่ซึ่งส่งผลกระทบต่อประสิทธิภาพของระบบนั้น 3. วิเคราะห์และอภิปรายระดับและผลของการยอมรับในข้อที่ 2 เพื่อกำหนดเป็นการกระทำและการป้องกันสำหรับการปรับปรุงระบบ ซึ่งควรมีการพิจารณาเปรียบเทียบกับเอกสารบันทึกการกระทำและการป้องกันฉบับก่อนหน้า (ถ้ามี) 4. ในการกำหนดข้อที่ 3 จะต้องระบุที่มา การกระทำหรือการป้องกันที่เป็นการปรับปรุงระบบ รวมถึงระดับความสำคัญของการกระทำหรือเหตุการณ์นั้น
ส่วนนำออก	1. <<เอกสาร>> แผ่นแบบการวิเคราะห์กระทำและเหตุการณ์ที่ส่งผลกระทบต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	การกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนด
ผู้รับผิดชอบ	ทีมปรับปรุงด้านความมั่นคง

ตารางที่ ข.32 การประกาศการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การประกาศการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Announce Identified Improvement to Stakeholders)
จุดประสงค์	เพื่อทำการประกาศการระบุการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้กับสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องได้รับทราบ
เงื่อนไขก่อนการดำเนินกิจกรรม	การกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนดเป็นเอกสาร

ตารางที่ ข.32 การประกาศการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<แผ่นประกาศ>> ประกาศกิจกรรมและการกระทำสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสารแผ่นแบบ>> แผ่นแบบแบบแสดงความคิดเห็นต่อการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
ขั้นตอนการทำงาน	1. จัดเตรียมสถานที่ วันและเวลา พร้อมทั้งเอกสารประกอบการประชุมเพื่อแจ้งให้ทราบ 2. จัดประชุมสมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. แจ้งให้ทราบถึงการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ พร้อมเอกสารประกอบ 4. รับผลการแสดงความคิดเห็นจากที่ประชุมต่อการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ทั้งนี้เพื่อทำการวิเคราะห์และปรับปรุงการกระทำและการป้องกันที่ได้กำหนดขึ้นครั้งนั้น
ส่วนนำออก	1. <<เอกสาร>> เอกสารแบบแสดงความคิดเห็นต่อการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสารฉบับปรับปรุง>> เอกสารการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
เงื่อนไขการออกจากกิจกรรม	1. สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องได้รับทราบถึงการระบุการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์เรียบร้อยแล้ว 2. เอกสารการกระทำและการป้องกันสำหรับการปรับปรุงระบบได้รับการแก้ไขปรับปรุงอย่างถูกต้อง สอดคล้องเป็นไปตามความคิดเห็นหลักจากที่ประชุม
ผู้รับผิดชอบ	ทีมปรับปรุงด้านความมั่นคง

ตารางที่ ข.33 การปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

หัวข้อ	คำอธิบาย
ชื่อกิจกรรม	การปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (Implement Identified Improvement)
จุดประสงค์	เพื่อดำเนินการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ตามความต้องการของการกระทำและการป้องกันสำหรับการปรับปรุงที่ได้กำหนดไว้ในกิจกรรมที่ 30
เงื่อนไขก่อนการดำเนินกิจกรรม	การกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้ถูกกำหนด ผ่านการแจ้งให้ทราบต่อผู้ที่เกี่ยวข้อง รวมถึงได้รับการปรับปรุงเมื่อเห็นสมควรตามความคิดเห็นจากที่ประชุม
ส่วนนำเข้า	1. <<เอกสาร>> เอกสารนโยบายการควบคุมการเข้าถึงสินทรัพย์ 2. <<เอกสาร>> เอกสารกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ 3. <<เอกสาร>> เอกสารกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารกลยุทธ์ของการประเมินความเสี่ยง 5. <<เอกสาร>> เอกสารการจัดการความเสี่ยงที่คงเหลือ 6. <<เอกสาร>> เอกสารข้อกำหนดของความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยง 7. <<เอกสาร>> เอกสารข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 8. <<เอกสาร>> เอกสารข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน 9. <<เอกสาร>> เอกสารความต้องการ การวิเคราะห์และออกแบบฟังก์ชันการทำงานและส่วนต่อประสานของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 10. <<ระบบ>> ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 11. <<เอกสารฉบับปรับปรุง>> เอกสารการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 12. <<เอกสารแผ่นแบบ>> แผ่นแบบเอกสารความต้องการของการกระทำและการป้องกันสำหรับปรุงปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 13. <<เอกสารแผ่นแบบ>> แผ่นแบบเอกสารแผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ข.33 การปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ส่วนนำเข้า	14. <<เอกสารแผ่นแบบ>> แผ่นแบบเอกสารการวิเคราะห์และออกแบบฟังก์ชันการทำงานในส่วนที่ต้องการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 15. <<เอกสารแผ่นแบบ>> แผ่นแบบเอกสารแผนการทดสอบส่วนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 16. <<เอกสารแผ่นแบบ>> แผ่นแบบกรณีทดสอบที่ใช้ทดสอบระบบ 17. <<เอกสารแผ่นแบบ>> แผ่นแบบรายงานผลการทดสอบและสรุปผลการทดสอบส่วนการปรับปรุงระบบ
ขั้นตอนการทำงาน	1. วิเคราะห์และอภิปรายการกระทำและการป้องกันสำหรับปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ เพื่อกำหนดเป็นความต้องการของกระทำและการป้องกันดังกล่าว 2. วางแผนการปรับปรุงระบบ โดยที่การกระทำและระยะเวลาของการดำเนินการที่สอดคล้องกับแผนการเฝ้าสังเกตและทวนสอบระบบ เนื่องจากการปรับปรุงเป็นผลการกระทำต่อเนื่องจากการประเมินประสิทธิภาพของระบบที่อยู่ภายใต้การเฝ้าสังเกตและทวนสอบนั่นเอง ซึ่งรายละเอียดของแผนการปรับปรุงระบบจะรวมถึง วัตถุประสงค์และขอบเขตของการปรับปรุง ความต้องการของการกระทำและการป้องกันในข้อที่ 1 ขั้นตอนวิธีการดำเนินการ ระยะเวลาดำเนินการ มาตรฐานต่างๆ หรือเทคโนโลยีที่นำมาใช้ งบประมาณหรือทรัพยากร และสมาชิกที่มีหน้าที่รับผิดชอบ 3. จากความต้องการในข้อที่ 1 นำมาปรับปรุงข้อกำหนดหรือออกแบบในส่วนที่ต้องการทำการปรับปรุงระบบ ทั้งนี้การปรับปรุงให้ระบบสามารถควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้อย่างมีประสิทธิภาพนั้น อาจเกิดจากความผิดพลาดของข้อกำหนดต่างๆ ไม่ว่าทั้งทางด้านความเสี่ยงของสินทรัพย์ การควบคุมการเข้าถึง หรือการออกแบบรหัสผ่าน 4. วางแผนการทดสอบเพื่อใช้ทดสอบระบบในส่วนที่ต้องการทำการปรับปรุง รวมถึงออกแบบกรณีทดสอบตามความต้องการที่ได้ออกแบบไว้ในข้อที่ 3 5. ดำเนินการปรับปรุงระบบตามความต้องการและการออกแบบที่ได้กำหนดไว้ในข้อที่ 1 และ 3 โดยดำเนินการภายใต้แผนการปรับปรุงระบบที่ได้กำหนดไว้ในข้อที่ 2 6. เมื่อเสร็จสิ้นการปรับปรุงให้ดำเนินการทดสอบระบบด้วยกรณีทดสอบที่ได้ออกแบบไว้ในข้อที่ 4 โดยดำเนินการภายใต้แผนของการทดสอบระบบ

ตารางที่ ข.33 การปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

หัวข้อ	คำอธิบาย
ขั้นตอนการทำงาน	7. บันทึกและสรุปผลการทดสอบ ทั้งนี้เพื่อใช้ในการแก้ไขและปรับปรุงระบบก่อนการส่งมอบ 8. ส่งมอบระบบที่ได้รับการปรับปรุง
ส่วนนำออก	1. <<เอกสาร>> เอกสารความต้องการของการกระทำและการป้องกันสำหรับปรุงปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 2. <<เอกสาร>> เอกสารแผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 3. <<เอกสาร>> เอกสารการวิเคราะห์และออกแบบฟังก์ชันการทำงานในส่วนที่ต้องการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 4. <<เอกสาร>> เอกสารแผนการทดสอบส่วนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ 5. <<เอกสาร>> เอกสารกรณีทดสอบที่ใช้ทดสอบส่วนการปรับปรุงระบบ 6. <<เอกสาร>> รายงานผลการทดสอบและสรุปผลการทดสอบส่วนการปรับปรุงระบบ 7. <<ระบบ>> ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ผ่านการปรับปรุง
เงื่อนไขการออกจากกิจกรรม	ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศได้รับการปรับปรุง และพร้อมสำหรับการใช้งานในครั้งต่อไป
ผู้รับผิดชอบ	ทีมปรับปรุงด้านความมั่นคง

ภาคผนวก ค
เอกสารแผ่นแบบสนับสนุนกระบวนการ

สำหรับกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ มีเอกสารแผ่นแบบที่ผู้วิจัยได้ออกแบบเพื่อสนับสนุนกระบวนการ โดยแบ่งออกเป็น 3 ประเภทหลัก ซึ่งในแต่ละประเภทมีรายชื่อเอกสารดังแสดงในตารางที่ ค.1 - ค.3

ตารางที่ ค.1 เอกสารแผ่นแบบประเภทเอกสาร

ลำดับ	เอกสารแผ่นแบบ	หน้าที่
1	นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	170
2	กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	177
3	การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ	183
4	การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ	189
5	การออกแบบและใช้งานรหัสผ่าน	195
6	แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	202
7	แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	209
8	แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	216
9	แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	223
10	แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	230

ตารางที่ ค.2 เอกสารแผ่นแบบประเภทฟอร์ม

ลำดับ	เอกสารแผ่นแบบ	หน้าที่
1	แบบฟอร์มรายนามสมาชิกทีมความมั่นคง	237
2	แบบฟอร์มรายการสินทรัพย์ประเภทสารสนเทศที่ต้องการการควบคุมการเข้าถึง	238
3	แบบฟอร์มรายการคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ	239
4	แบบฟอร์มการประเมินมูลค่าของสินทรัพย์ประเภทสารสนเทศ	240
5	แบบฟอร์มการประเมินภัยคุกคามของสินทรัพย์ประเภทสารสนเทศ	241
6	แบบฟอร์มการประเมินภาวะเสี่ยงของสินทรัพย์ประเภทสารสนเทศ	242
7	แบบฟอร์มการกำหนดค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ	243
8	แบบฟอร์มการกำหนดแนวคิดความมั่นคงของสินทรัพย์ประเภทสารสนเทศ	244
9	แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภทสารสนเทศแบบให้อำนาจ	246

ตารางที่ ค.2 เอกสารแผ่นแบบประเภทฟอร์ม (ต่อ)

ลำดับ	เอกสารแผ่นแบบ	หน้าที่
10	แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภทสารสนเทศเชิงบทบาท	247
11	แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภทสารสนเทศแบบความมั่นคงหลายระดับ	248
12	แบบฟอร์มรายการกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	249
13	แบบฟอร์มรายการจัดการความเสี่ยงโครงการ	250
14	แบบฟอร์มรายงานผลการประเมินการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	252
15	แบบฟอร์มรายงานความก้าวหน้าการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	253
16	แบบฟอร์มรายงานความเปลี่ยนแปลงของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	254
17	แบบฟอร์มรายการกรณีทดสอบสำหรับใช้ทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	257
18	แบบฟอร์มรายงานผลการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	258
19	แบบฟอร์มรายงานผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	260
20	แบบฟอร์มรายงานผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	261
21	แบบฟอร์มรายงานผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบ	262
22	แบบฟอร์มรายการการกระทำและเหตุการณ์ที่ซึ่งส่งผลต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	263
23	แบบฟอร์มวิเคราะห์การกระทำและเหตุการณ์ที่ซึ่งส่งผลต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	264
24	แบบฟอร์มรายการการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	265
25	แบบฟอร์มข้อเสนอแนะของผู้ที่เกี่ยวข้องต่อการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	266

ตารางที่ ค.3 เอกสารแผ่นแบบประเภทรายการตรวจสอบ

ลำดับ	เอกสารแผ่นแบบ	หน้าที่
1	แบบฟอร์มรายการทวนสอบข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	267
2	แบบฟอร์มรายการทวนสอบข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศโดยยึดนโยบายและกลยุทธ์เป็นหลัก	268
3	แบบฟอร์มรายการตรวจสอบความครบถ้วนของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	269

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Policy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Policy)

ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชัน** : [1.0]

ชื่อโครงการ : [โครงการ.....]

[ชื่อหน่วยงาน]

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Policy)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Policy)	**สถานะรายงาน** [ขื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Policy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **ที่มาและความสำคัญ** (Abstracting)

   [ระบุที่มาและความสำคัญของความจำเป็นต้องมีการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

2. **ขอบเขต** (Scope)

   [กำหนดขอบเขตของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งอธิบายในมุมมองของธุรกิจและองค์กร]

3. **เป้าหมาย** (Goal)

   [ระบุเป้าหมายของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

4. **พันธกิจ** (Mission)

   [ระบุพันธกิจของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

5. **ถ้อยแถลงนโยบาย** (Policy Statement)

   [ระบุถ้อยแถลงนโยบายของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

   5.1 **ความสอดคล้องต้องกันของการควบคุมการเข้าถึงกับนโยบายด้านการจัดแบ่งประเภทสินทรัพย์ประเภทสารสนเทศ**

   [ระบุถึงความสอดคล้องต้องกันของการควบคุมการเข้าถึงกับนโยบายด้านการจัดแบ่งประเภทสินทรัพย์สารสนเทศขององค์กร]

   5.2 **การจัดการสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ**

   [กำหนดการจัดการสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ ซึ่งจะต้องครอบคลุมทุกๆ เส้นทางของการเชื่อมต่อ]

นโยบายการสร้างการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

5.3 **ข้อบังคับของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ**

[ระบุกฎหรือข้อบังคับของการควบคุมการเข้าถึง ทั้งในการร้องขอ การอนุญาตให้เข้าถึง รวมถึงการบริหารจัดการการเข้าถึงใดๆ]

5.4 **ความต้องการของการอนุญาตให้เข้าถึงสินทรัพย์ประเภทสารสนเทศ**

[ระบุความต้องการของการอนุญาตให้เข้าถึงสินทรัพย์ประเภทสารสนเทศสำหรับแต่ละการร้องขอใดๆ]

5.5 **การจัดการการถอนสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ**

[กำหนดการจัดการการถอนสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศออกจากที่ได้กำหนดไว้]

6. **เอกสารที่เกี่ยวข้อง** (Related Documents)

[ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับนโยบาย ซึ่งอาจรวมถึงสัญญาหรือข้อตกลงที่มุ่งเน้นการป้องกันการเข้าถึงสินทรัพย์ประเภทสารสนเทศ และเอกสารระบุการเข้าถึงสินทรัพย์ประเภทสารสนเทศของผู้ใช้งานโดยเป็นไปตามบทบาทที่มีอยู่ภายในองค์กร]

7. **เงื่อนไขข้อยกเว้น** (Exemption Criteria)

[ระบุเงื่อนไขข้อยกเว้นภายใต้นโยบายที่ได้ระบุไว้]

8. **การแก้ปัญหาข้อขัดแย้ง** (Conflict Resolution)

[ระบุการแก้ปัญหาข้อขัดแย้งกับเอกสารนโยบายฉบับอื่น]

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Policy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

นโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
ตรวจสอบโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
อนุมัติโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
พยาน (หน่วยงาน/องค์กรที่เกี่ยวข้อง)	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
พยาน (หน่วยงาน/องค์กรที่เกี่ยวข้อง)	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
พยาน (หน่วยงาน/องค์กรที่เกี่ยวข้อง)	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)

ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **ความเหมือน-ต่างระหว่างนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและกลยุทธ์องค์กรด้านการจัดการความเสี่ยง** (GAP-Analysis)
   [วิเคราะห์ความเหมือนและต่างระหว่างนโยบายการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและกลยุทธ์องค์กรด้านการจัดการความเสี่ยง]

2. **กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ** (Information Assets Access Control Strategy)
   [กำหนดกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศให้มีความชัดเจน โดยพิจารณาจากความเหมือนและต่างที่ได้วิเคราะห์มาก่อนหน้า]

3. **กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ** (Information Assets Access Control Process)
   [กำหนดกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยสอดคล้องตามกลยุทธ์ที่ได้กำหนดไว้มาก่อนหน้า]

4. **เอกสารที่เกี่ยวข้อง** (Related Documents)
   [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับกลยุทธ์และกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Strategy)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

กลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
ตรวจสอบโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
อนุมัติโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

(Information Asset's Risk Management)

ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

(Information Asset's Risk Management)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Information Asset's Risk Management)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Information Asset's Risk Management)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Information Asset's Risk Management)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

1. **วิธีการประเมินความเสี่ยง** (Risk Assessment Approach)

   [กำหนดวิธีการประเมินความเสี่ยง ซึ่งจะต้องเหมาะสมกับการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศและเป็นไปตามกลยุทธ์ขององค์กรด้านการจัดการความเสี่ยง]

   1.1 **เกณฑ์ของการยอมรับความเสี่ยง** (Criteria for Accepting Risk)

   [ระบุเกณฑ์ในการยอมรับความเสี่ยงที่จะเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ]

   1.2 **ระดับของการยอมรับความเสี่ยง** (Acceptable Levels of Risk)

   [ระบุระดับของการยอมรับความเสี่ยง]

2. **การจัดการความเสี่ยงที่คงเหลือ** (Residual Risk Management)

   [กำหนดวิธีการในการจัดการกับความเสี่ยงใดๆ ที่ยังคงเหลือจากการที่ได้ประเมินความเสี่ยงในครั้งก่อน โดยวิธีการดังกล่าวจะต้องเป็นไปตามกลยุทธ์ขององค์กรด้านการจัดการความเสี่ยง]

   2.1 **เกณฑ์ในการยอมรับค่าความเสี่ยงที่คงเหลือ** (Criteria for Accepting Residual Risk)

   [ระบุเกณฑ์ในการยอมรับค่าความเสี่ยงที่คงเหลือที่จะเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ]

   2.2 **ระบุระดับในการยอมรับค่าความเสี่ยงที่คงเหลือ** (Acceptable Levels of Residual Risk)

   [ระดับในการยอมรับค่าความเสี่ยงที่คงเหลือ]

   2.3 **ผลกระทบที่คาดว่าจะเกิดขึ้นจากความเสี่ยงที่คงเหลือ** (Impaction of Residual Risk)

   [ระบุถึงผลกระทบที่มีต่อองค์กรที่คาดว่าจะเกิดขึ้น ซึ่งเกิดจากความเสี่ยงที่คงเหลือใดๆ]

3. **เอกสารที่เกี่ยวข้อง** (Related Documents)

   [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับการจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ]

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Information Asset's Risk Management)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ (Information Asset's Risk Management)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การจัดการความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย [ลงนาม] [วัน เดือน ปี]
[ชื่อ-สกุล] วันที่ลงนาม
[ตำแหน่ง]

ตรวจสอบโดย [ลงนาม] [วัน เดือน ปี]
[ชื่อ-สกุล] วันที่ลงนาม
[ตำแหน่ง]

อนุมัติโดย [ลงนาม] [วัน เดือน ปี]
[ชื่อ-สกุล] วันที่ลงนาม
[ตำแหน่ง]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)		
ตัวแบบอ้างอิง : แบบรูปความมั่นคง	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ

(Access Control Model Selection for Information Asset)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ

1. **ปัจจัยในการเลือกใช้โมเดลการควบคุมการเข้าถึง** (Factor for Access Control Model Selection)
   [กำหนดปัจจัยในการเลือกใช้โมเดลการควบคุมการเข้าถึง ซึ่งต้องมีความเหมาะสมกับสภาพแวดล้อมโดยรวมขององค์กร โดยตัวอย่างปัจจัยในการเลือกโมเดล เช่น ขนาดขององค์กร จำนวนผู้ใช้งานสินทรัพย์ประเภทสารสนเทศ การจัดแบ่งระดับของสินทรัพย์ประเภทสารสนเทศ เป็นต้น]

2. **โมเดลการควบคุมการเข้าถึงที่ได้เลือกใช้** (Access Control Model)
   [ระบุโมเดลการควบคุมการเข้าถึงที่มีความเหมาะสมกับสภาพแวดล้อมโดยรวมขององค์กร ซึ่งต้องพิจารณาจากปัจจัยในข้อที่ 1 โดยโมเดลการควบคุมการเข้าถึงได้แบ่งออกเป็น โมเดลการให้อำนาจ (Authorization Model) โมเดลการเข้าถึงเชิงบทบาท (RBAC Model) โมเดลความมั่นคงหลายระดับ (Multilevel Security Model) และโมเดลการตรวจสอบการเข้าถึง (Reference Monitor Model)]

3. **เหตุผลในการเลือกใช้โมเดลการควบคุมการเข้าถึง** (Reason for Access Control Model Selection)
   [ระบุสาเหตุของการเลือกใช้โมเดลการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศนั้น]

4. **เอกสารที่เกี่ยวข้อง** (Related Documents)
   [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับการเลือกใช้โมเดลการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ (Access Control Model Selection for Information Asset)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การเลือกใช้โมเดลการควบคุมการเข้าถึงสำหรับสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
ตรวจสอบโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
อนุมัติโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	

การออกแบบและใช้งานรหัสผ่าน (Password Designing and Usage)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การออกแบบและใช้งานรหัสผ่าน (Password Designing and Usage)		
ตัวแบบอ้างอิง : แบบรูปความมั่นคง	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

การออกแบบและใช้งานรหัสผ่าน

(Password Designing and Usage)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

การออกแบบและใช้งานรหัสผ่าน (Password Designing and Usage)	**สถานะรายงาน** [ขื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

การออกแบบและใช้งานรหัสผ่าน (Password Designing and Usage)	**สถานะรายงาน** [ขื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

การออกแบบและใช้งานรหัสผ่าน

1. **ขอบเขตของการออกแบบและใช้งานรหัสผ่าน** (Scope of Password Designing and Usage)
   [ระบุขอบเขตของการออกแบบและใช้งานรหัสผ่าน ทั้งนี้ต้องสอดคล้องเป็นไปตามนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

2. **ความต้องการของการออกแบบและใช้งานรหัสผ่าน** (Requirements of Password Designing and Usage)
   [กำหนดความต้องการของการออกแบบและใช้งานรหัสผ่านในแต่ละขอบเขตที่ระบุไว้ในข้อที่ 1]

3. **ปัจจัยที่มีผลต่อการกำหนดความต้องการของการออกแบบและใช้งานรหัสผ่าน** (Factor for Password Defining)
   [ระบุปัจจัยต่างๆ ที่มีผลต่อการกำหนดความต้องการของการออกแบบและใช้งานรหัสผ่านในข้อที่ 2]

4. **การออกแบบและใช้งานรหัสผ่าน** (Password Designing and Usage) **โดยทั่วไปแล้วจะกำหนดตามขอบเขตต่าง ๆ ดังต่อไปนี้**

   4.1 **ตัวอักษรที่จะใช้ในรหัสผ่าน**
   [กำหนดตัวอักษรที่จะใช้ในรหัสผ่าน เช่น ในลักษณะของตัวเลข หรือตัวอักษร หรือมีการผสมกันระหว่างตัวเลขและตัวอักษร เป็นต้น]

   4.2 **ความยาวของรหัสผ่าน**
   [กำหนดความยาวของรหัสผ่าน ซึ่งควรมีความยาวไม่เกิน 6-8 ตัวอักษร หรือน้อยกว่า หรือมากกว่า ซึ่งแล้วแต่ความเหมาะสมที่จะกำหนดขึ้น]

   4.3 **ที่มาของรหัสผ่าน**
   [กำหนดที่มาของรหัสผ่าน เช่น ได้จากการสร้างแบบอัตโนมัติ เป็นต้น]

   4.4 **อายุการใช้งานของรหัสผ่าน**
   [กำหนดอายุการใช้งานของรหัสผ่าน เช่น มีอายุการใช้งานประมาณ 1 เดือน เป็นต้น]

การออกแบบและใช้งานรหัสผ่าน

4.5 **บุคคลที่มีสิทธิในการใช้งานรหัสผ่าน**

[กำหนดบุคคลที่มีสิทธิในการใช้งานรหัสผ่าน เช่น เฉพาะบุคคล หรือเป็นกลุ่มของผู้ใช้งาน เป็นต้น]

4.6 **วิธีการในการกรอกรหัสผ่าน**

[กำหนดวิธีการในการกรอกรหัสผ่าน เช่น อนุญาตให้กรอกผ่านแป้นคีย์บอร์ดเท่านั้น เป็นต้น]

4.7 **ระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน**

[กำหนดระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน เช่น มีการตอบสนองภายในเวลา 5 วินาที ภายหลังจากการล็อกอินเข้าสู่ระบบ เป็นต้น]

4.8 **วิธีการส่งรหัสผ่านไปยังผู้ใช้งาน**

[กำหนดวิธีการในการส่งรหัสผ่านให้ผู้ใช้งาน เช่น ส่งรหัสผ่านผ่านทางอีเมลของบุคคล เป็นต้น]

4.9 **วิธีการจัดเก็บรหัสผ่าน**

[กำหนดวิธีการในการจัดเก็บรหัสผ่าน เช่น ในการจัดเก็บรหัสผ่าน มีการเข้ารหัสก่อนการจัดเก็บ เป็นต้น]

4.10 **วิธีการถ่ายโอนรหัสผ่าน**

[กำหนดวิธีการในการถ่ายโอนรหัสผ่านเพื่อใช้ในการทวนสอบ เช่น ในระหว่างที่มีการถ่ายโอนนั้นได้มีการ เข้ารหัสเอาไว้ เป็นต้น]

4.11 **อื่นๆ**

5. **เอกสารที่เกี่ยวข้อง** (Related Documents)

[ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับการออกแบบและใช้งานรหัสผ่าน]

การออกแบบและใช้งานรหัสผ่าน (Password Designing and Usage)	**สถานะรายงาน** [ชื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การออกแบบและใช้งานรหัสผ่าน

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

การออกแบบและใช้งานรหัสผ่าน (Password Designing and Usage)	**สถานะรายงาน** [ขื่อสถานะ]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

การออกแบบและใช้งานรหัสผ่าน

จัดทำโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
ตรวจสอบโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
อนุมัติโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)

ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

(IAAC System Plan)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **บทนำ** (Introduction)
   [ระบุรายละเอียดของบทนำ]

2. **วัตถุประสงค์ของการพัฒนาระบบ** (Objective of System Implementation)
   [กำหนดวัตถุประสงค์ของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

3. **ขอบเขตของการพัฒนาระบบ** (Scope of System Implementation)
   [กำหนดขอบเขตของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

4. **ระเบียบวิธีที่ใช้ในการพัฒนาระบบ** (Methodology)
   [ระบุถึงระเบียบวิธีที่ใช้ในการดำเนินการพัฒนาระบบ ทั้งนี้เพื่อเป็นแนวทางในการกำหนดกิจกรรมก่อน-หลังของการดำเนินการ]

5. **โครงสร้างกิจกรรม** (Work Break Down Structure)
   [ระบุกิจกรรมที่จะเกิดขึ้นของการพัฒนาระบบ โดยอยู่ในรูปแบบของโครงสร้างหรือแผนผัง]

6. **โครงสร้างผลิตภัณฑ์** (Product Break Down Structure)
   [ระบุถึงผลิตภัณฑ์หรือสิ่งที่ได้ภายหลังจากการกระทำตามกิจกรรมของการพัฒนาระบบ]

7. **ระยะเวลาดำเนินการ** (Period of Time)
   [ระบุช่วงระยะเวลาของการดำเนินการพัฒนาระบบ ตั้งแต่เริ่มต้นจนถึงส่งมอบระบบที่แล้วเสร็จ]

8. **เป้าหมายกิจกรรม** (Milestone)
   [ระบุลำดับของกิจกรรมที่จะเกิดขึ้น ภายใต้ขอบเขตของระยะเวลาดำเนินการ]

9. **มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้** (Related Standard and Technology)
   [ระบุมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาระบบและเทคโนโลยีที่ต้องการนำมาใช้]

แผนการพัฒนาระบบการควบคุมการเข้าถึงเข้าถึงสินทรัพย์ประเภทสารสนเทศ

10. **งบประมาณและทรัพยากรที่จำเป็นต้องใช้** (Budget and Resource)

    [กำหนดงบประมาณสำหรับการพัฒนาระบบและระบุถึงทรัพยากรที่จำเป็นต้องใช้]

11. **สมาชิกผู้รับผิดชอบและบทบาทหน้าที่** (Role and Responsibility)

    [ระบุถึงสมาชิกภายใต้ทีมพัฒนาระบบ รวมถึงระบุบทบาทหน้าที่ความรับผิดชอบให้กับสมาชิก]

12. **เอกสารที่เกี่ยวข้อง** (Related Documents)

    [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC System Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
ตรวจสอบโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
อนุมัติโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)		
ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

(IAAC Testing Plan)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)	**สถานะรายงาน** [ขื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **บทนำ** (Introduction)
   [ระบุรายละเอียดของบทนำ]

2. **วัตถุประสงค์ของการทดสอบระบบ** (Objective's Test)
   [ระบุวัตถุประสงค์ของการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศที่ได้พัฒนา]

3. **ขอบเขตของการทดสอบระบบ** (Scope of Test)
   [กำหนดขอบเขตของการทดสอบระบบ]

4. **ระเบียบวิธีที่ใช้ในการทดสอบระบบ** (Methodology)
   [ระบุถึงระเบียบวิธีที่ใช้ในการดำเนินการทดสอบระบบ ทั้งนี้เพื่อเป็นแนวทางในการกำหนดกิจกรรมก่อน-หลังของการดำเนินการ]

5. **บรรทัดฐานของการทดสอบ** (Criteria of Test)
   [ระบุถึงเกณฑ์สำหรับใช้ทดสอบระบบ]

6. **ระดับของการยอมรับ** (Level of Accepted)
   [ระบุระดับในการยอมรับถึงผลของการทดสอบระบบ]

7. **ฟังก์ชันที่ต้องการทดสอบ** (Function need to Test)
   [ระบุฟังก์ชันหรือส่วนการทำงานของระบบที่ต้องการทำการทดสอบ]

8. **ผลิตภัณฑ์ที่ได้จากการทดสอบ** (Product of Test)
   [ระบุถึงผลิตภัณฑ์หรือสิ่งที่ได้จากการทดสอบระบบ]

9. **ระยะเวลาดำเนินการ** (Period of Time)
   [ระบุช่วงระยะเวลาของการดำเนินการทดสอบระบบ ขณะทำการพัฒนาไปจนถึงแล้วเสร็จ]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

10. **เป้าหมายกิจกรรม** (Milestone)

    [ระบุลำดับของกิจกรรมที่จะเกิดขึ้น ภายใต้ขอบเขตของระยะเวลาดำเนินการ]

11. **มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้** (Related Standard and Technology)

    [ระบุมาตรฐานต่างๆ ที่เกี่ยวข้องกับการทดสอบระบบและเทคโนโลยีที่ต้องการนำมาใช้]

12. **งบประมาณและทรัพยากรที่จำเป็นต้องใช้** (Budget and Resource)

    [กำหนดงบประมาณสำหรับการทดสอบระบบและระบุถึงทรัพยากรที่จำเป็นต้องใช้]

13. **สมาชิกผู้รับผิดชอบและบทบาทหน้าที่** (Role and Responsibility)

    [ระบุถึงสมาชิกภายใต้ทีมทดสอบระบบ รวมถึงระบุบทบาทหน้าที่ความรับผิดชอบให้กับสมาชิก]

14. **เอกสารที่เกี่ยวข้อง** (Related Documents)

    [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับแผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Testing Plan)	**สถานะรายงาน** [ขื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย [ลงนาม] [วัน เดือน ปี]
[ชื่อ-สกุล] วันที่ลงนาม
[ตำแหน่ง]

ตรวจสอบโดย [ลงนาม] [วัน เดือน ปี]
[ชื่อ-สกุล] วันที่ลงนาม
[ตำแหน่ง]

อนุมัติโดย [ลงนาม] [วัน เดือน ปี]
[ชื่อ-สกุล] วันที่ลงนาม
[ตำแหน่ง]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Training Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

(IAAC Training Plan)

ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

(IAAC Training Plan)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Training Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Training Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Training Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง กับระบบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **บทนำ** (Introduction)
   [ระบุรายละเอียดของบทนำ]

2. **วัตถุประสงค์ของการอบรม** (Objective's Training)
   [ระบุวัตถุประสงค์ของการจัดการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

3. **ขอบเขตของการอบรม** (Scope of Training)
   [กำหนดขอบเขตของการจัดการอบรม]

4. **เนื้อหาของการอบรม** (Information of Training)
   [ระบุถึงองค์ความรู้ของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศโดยสรุป ซึ่งต้องการนำเสนอให้ผู้เข้าอบรมได้รับทราบ]

5. **กำหนดการอบรม** (Agenda)
   [ระบุถึงกำหนดการโดยสรุป โดยแสดงถึงกิจกรรมต่างๆ ภายใต้ระยะเวลาของการเข้าอบรม]

6. **วันเวลาและสถานที่จัดการอบรม** (Time and Place)
   [ระบุวันเวลาและสถานที่ที่จัดการอบรม]

7. **เกณฑ์และระดับในการประเมินผลการอบรม** (Criteria and Level of Training Evaluation)
   [กำหนดเกณฑ์และระบุระดับเพื่อใช้สำหรับประเมินผลการจัดการอบรม โดยครอบคลุมทั้งองค์ประกอบของการจัดอบรม ความรับรู้ได้ของผู้เข้าอบรม รวมถึงทัศนคติของผู้เข้าอบรมที่มีต่อการจัดอบรม]

8. **ระยะเวลาดำเนินการ** (Period of Time)
   [ระบุช่วงระยะเวลาของการดำเนินการจัดการอบรม]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง กับระบบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

9. **เป้าหมายกิจกรรม** (Milestone)
   [ระบุลำดับของกิจกรรมที่จะเกิดขึ้น ภายใต้ขอบเขตของระยะเวลาดำเนินการ]

10. **มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้** (Related Standard and Technology)
    [ระบุมาตรฐานต่างๆ ที่เกี่ยวข้องกับการจัดการอบรมและเทคโนโลยีที่ต้องการนำมาใช้]

11. **งบประมาณและทรัพยากรที่จำเป็นต้องใช้** (Budget and Resource)
    [กำหนดงบประมาณสำหรับการจัดการอบรมและระบุถึงทรัพยากรที่จำเป็นต้องใช้]

12. **สมาชิกผู้รับผิดชอบและบทบาทหน้าที่** (Role and Responsibility)
    [ระบุถึงสมาชิกผู้รับผิดชอบการจัดการอบรม รวมถึงระบุบทบาทหน้าที่ความรับผิดชอบให้กับสมาชิก]

13. **เอกสารที่เกี่ยวข้อง** (Related Documents)
    [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับแผนการอบรม]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Training Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง กับระบบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Training Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้อง กับระบบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
ตรวจสอบโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
อนุมัติโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)		
ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

(IAAC Monitoring and Reviewing Plan)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]

สถานะเอกสาร : [ชื่อสถานะ]

จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการเฝ้าสังเกตและทวนสอบ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **บทนำ** (Introduction)
   [ระบุรายละเอียดของบทนำ]

2. **วัตถุประสงค์ของการเฝ้าสังเกตและทวนสอบระบบ** (Objective's Reviewing)
   [ระบุวัตถุประสงค์ของการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

3. **ขอบเขตของการเฝ้าสังเกตและทวนสอบระบบ** (Scope of Monitoring and Reviewing)
   [กำหนดขอบเขตของการเฝ้าสังเกตและทวนสอบระบบ]

4. **ตัวชี้วัดประสิทธิภาพ** (Effective Metric)
   [ระบุตัวชี้วัดสำหรับใช้ประเมินประสิทธิภาพการทำงานในด้านต่างๆ ของระบบ โดยมุ่งเน้นไปที่การควบคุมการเข้าถึงของแต่ละสินทรัพย์ประเภทสารสนเทศ]

5. **ค่าคาดหมาย** (Based Line)
   [ระบุค่าคาดหมายในแต่ละตัวชี้วัดของประสิทธิภาพของระบบที่ต้องการบรรลุ]

6. **ส่วนการทำงานที่ต้องการเฝ้าสังเกตและทวนสอบ** (Monitoring and Reviewing Part)
   [ระบุส่วนนำเข้าและออก ฟังก์ชันหรือส่วนการทำงานใดๆ ของระบบ รวมถึงความเสี่ยงของสินทรัพย์ประเภทสารสนเทศที่จะต้องทำการเฝ้าสังเกตและทวนสอบ ซึ่งต้องสอดคล้องกับตัวชี้วัดที่ได้ทำการระบุเอาไว้]

7. **ส่วนการทำงานที่ต้องการประเมินประสิทธิภาพ** (Measurement Part)
   [ระบุส่วนนำเข้าและออก ฟังก์ชันหรือส่วนการทำงานใดๆ ของระบบ รวมถึงความเสี่ยงของสินทรัพย์ประเภทสารสนเทศที่จะต้องการประเมินประสิทธิภาพ ซึ่งต้องสอดคล้องกับตัวชี้วัดที่ได้ทำการระบุเอาไว้]

แผนการเฝ้าสังเกตและทวนสอบ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

8. **วิธีการประเมินประสิทธิภาพ** (How to Measurement)
   [ระบุวิธีการประเมินประสิทธิภาพของระบบ ซึ่งต้องสอดคล้องกับตัวชี้วัดที่ได้ทำการระบุเอาไว้]

9. **ระยะเวลาดำเนินการ** (Period of Time)
   [ระบุช่วงระยะเวลาของการดำเนินการเฝ้าสังเกตและทวนสอบระบบ ภายหลังจากที่ระบบได้ผ่านการเข้าใช้งานจากผู้ใช้ในช่วงระยะเวลาหนึ่งๆ]

10. **เป้าหมายกิจกรรม** (Milestone)
    [ระบุลำดับของกิจกรรมที่จะเกิดขึ้น ภายใต้ขอบเขตของระยะเวลาดำเนินการ]

11. **มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้** (Related Standard and Technology)
    [ระบุมาตรฐานต่างๆ ที่เกี่ยวข้องกับการเฝ้าสังเกตและทวนสอบระบบและเทคโนโลยีที่ต้องการนำมาใช้]

12. **งบประมาณและทรัพยากรที่จำเป็นต้องใช้** (Budget and Resource)
    [กำหนดงบประมาณสำหรับการเฝ้าสังเกตและทวนสอบระบบและระบุถึงทรัพยากรที่จำเป็นต้องใช้]

13. **สมาชิกผู้รับผิดชอบและบทบาทหน้าที่** (Role and Responsibility)
    [ระบุถึงสมาชิกภายใต้ทีมเฝ้าสังเกตและทวนสอบระบบ รวมถึงระบุบทบาทหน้าที่ความรับผิดชอบให้กับสมาชิก]

14. **เอกสารที่เกี่ยวข้อง** (Related Documents)
    [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับแผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการเฝ้าสังเกตและทวนสอบ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

แผนการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Monitoring and Reviewing Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการเฝ้าสังเกตและทวนสอบ
ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
ตรวจสอบโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม
อนุมัติโดย	[ลงนาม] [ชื่อ-สกุล] [ตำแหน่ง]	[วัน เดือน ปี] วันที่ลงนาม

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)

ตัวแบบอ้างอิง : [ISO/IEC] 27001, 27002	**ระดับการใช้งาน** : [โครงการ]	**เวอร์ชั่น** : [1.0]
ชื่อโครงการ : [โครงการ.....]		

[ชื่อหน่วยงาน]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

(IAAC Improvement Plan)

[ชื่อโครงการ]

☒ เอกสารควบคุม ☐ เอกสารไม่ควบคุม

วันที่จัดทำเอกสาร : [วัน เดือน ปี]
สถานะเอกสาร : [ชื่อสถานะ]
จัดทำโดย : [ระบุส่วนงานหรือแผนกที่จัดทำ]

เอกสารฉบับนี้จัดทำขึ้นเพื่อเป็นส่วนหนึ่งของวิทยานิพนธ์ ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ปีการศึกษา 2553
ของนางสาวเมธยา ราชคมน์ รหัสประจำตัวนิสิต 507 04090 21
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

บันทึกการแก้ไข

เวอร์ชัน	แก้ไขครั้งที่	วันที่แก้ไข	รายละเอียด	แก้ไขโดย	ผู้อนุมัติ
[เลขที่]	[ครั้งที่]/[พ.ศ.]	[วัน เดือน ปี]	[หัวข้อ-รายละเอียดการแก้ไข]	[ชื่อ-สกุล]	[ชื่อ-สกุล]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

สารบัญ

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

1. **บทนำ** (Introduction)
   [ระบุรายละเอียดของบทนำ]

2. **วัตถุประสงค์ของการปรับปรุงระบบ** (Objective's Improvement)
   [ระบุวัตถุประสงค์ของการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

3. **ขอบเขตของการปรับปรุงระบบ** (Scope of Improvement)
   [กำหนดขอบเขตของการปรับปรุงระบบ]

4. **ความต้องการของการปรับปรุงระบบ** (Improvement Requirements)
   [ระบุถึงความต้องการของการกระทำและการป้องกันสำหรับปรับปรุงระบบ ซึ่งความต้องการดังกล่าวเป็นผลจากการวิเคราะห์การกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ]

5. **ส่วนการทำงานที่ต้องการปรับปรุง** (Improvement Part)
   [ระบุส่วนนำเข้าและออก ฟังก์ชันหรือส่วนการทำงานใดๆ ของระบบ รวมถึงความเสี่ยงของสินทรัพย์ประเภทสารสนเทศที่จะต้องทำการปรับปรุง]

6. **ระยะเวลาดำเนินการ** (Period of Time)
   [ระบุช่วงระยะเวลาของการดำเนินการปรับปรุงระบบ ภายหลังจากที่ระบบได้ผ่านการประเมินประสิทธิภาพเรียบร้อยแล้ว]

7. **เป้าหมายกิจกรรม** (Milestone)
   [ระบุลำดับของกิจกรรมที่จะเกิดขึ้น ภายใต้ขอบเขตของระยะเวลาดำเนินการ]

8. **มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้** (Related Standard and Technology)
   [ระบุมาตรฐานต่างๆ ที่เกี่ยวข้องกับการปรับปรุงระบบและเทคโนโลยีที่ต้องการนำมาใช้]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

9. **งบประมาณและทรัพยากรที่จำเป็นต้องใช้** (Budget and Resource)
   [กำหนดงบประมาณสำหรับการปรับปรุงระบบและระบุถึงทรัพยากรที่จำเป็นต้องใช้]

10. **สมาชิกผู้รับผิดชอบและบทบาทหน้าที่** (Role and Responsibility)
    [ระบุถึงสมาชิกภายใต้ทีมปรับปรุงระบบ รวมถึงระบุบทบาทหน้าที่ความรับผิดชอบให้กับสมาชิก]

11. **เอกสารที่เกี่ยวข้อง** (Related Documents)
    [ระบุถึงทุกๆ เอกสารที่มีความเกี่ยวข้องกับแผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ภาคผนวก ก – อภิธานศัพท์ (Definition)

ภาคผนวก ข – คำย่อและรัสพจน์ (Abbreviation and Acronym)

ภาคผนวก ค – เอกสารอ้างอิง (Reference)

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (IAAC Improvement Plan)	**สถานะรายงาน** [ชื่อสถานะ] **เวอร์ชันเอกสาร** [n]
[ชื่อโครงการ]	**เวอร์ชัน** [1.0]

แผนการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

จัดทำโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
ตรวจสอบโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	
อนุมัติโดย	[ลงนาม]	[วัน เดือน ปี]
	[ชื่อ-สกุล]	วันที่ลงนาม
	[ตำแหน่ง]	

เลขที่เอกสารอ้างอิง: [IAAC-INT-001-nn]	แบบฟอร์มรายนามสมาชิกทีมความมั่นคง	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายนามสมาชิกทีมความมั่นคง

ลำดับ	รหัสพนักงาน	ชื่อ - นามสกุล	ส่วนงาน	ตำแหน่งหน้าที่	ลายมือชื่อ
1	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
2	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
3	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
4	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
5	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
6	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
7	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
8	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
9	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
10	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
11	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
12	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
13	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
14	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
15	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
.	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
.	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
.	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
.	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]
.	[ระบุรหัส]	[ระบุชื่อ-นามสกุล]	[ระบุส่วนงาน]	[ระบุตำแหน่ง]	[ลงลายมือชื่อ]

เลขที่เอกสารอ้างอิง: [IAAC-RIK-001-nn]	แบบฟอร์มรายการสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]	ที่ต้องการการควบคุมการเข้าถึง	แก้ไขครั้งที่ 0

แบบฟอร์มรายการสินทรัพย์ประเภทสารสนเทศ ที่ต้องการการควบคุมการเข้าถึง

- **รหัสสินทรัพย์ประเภทสารสนเทศ :**

  .....

- **สินทรัพย์ประเภทสารสนเทศ :**

  .....

  .....

  .....

ลำดับ	ปัจจัยทางธุรกิจที่เกี่ยวข้อง	คำอธิบายความสัมพันธ์
1	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
2	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
3	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
4	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
5	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
.	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
.	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
.	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
.	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]
.	[ระบุปัจจัยทางธุรกิจ]	[ระบุคำอธิบาย]

เลขที่เอกสารอ้างอิง: [IAAC-RIK-002-nn]	แบบฟอร์มรายการคุณสมบัติด้านความมั่นคง	หน้า 1/1
รหัสโครงการ: [.....]	ของสินทรัพย์ประเภทสารสนเทศ	แก้ไขครั้งที่ 0

แบบฟอร์มรายการคุณสมบัติด้านความมั่นคง ของสินทรัพย์ประเภทสารสนเทศ

- **รหัสสินทรัพย์ประเภทสารสนเทศ :**

  .....

- **สินทรัพย์ประเภทสารสนเทศ :**

  .....

  .....

  .....

ลำดับ	คุณสมบัติด้านความมั่นคง	คำอธิบายความสัมพันธ์
1	[ระบุคุณสมบัติ]	[ระบุคำอธิบาย]
2	[ระบุคุณสมบัติ]	[ระบุคำอธิบาย]
3	[ระบุคุณสมบัติ]	[ระบุคำอธิบาย]
4	[ระบุคุณสมบัติ]	[ระบุคำอธิบาย]

หมายเหตุ : คุณสมบัติด้านความมั่นคง (Security Properties) โดยทั่วไปจะประกอบด้วย

- การรักษาความลับ (Confidentiality)
- ความบูรณาภาพ (Integrity)
- สภาพพร้อมใช้งาน (Availability)
- ภาระรับผิดชอบ (Accountability)

เลขที่เอกสารอ้างอิง: [IAAC-RIK-003-nn]	แบบฟอร์มการประเมินมูลค่า	หน้า 1/1
รหัสโครงการ: [.....]	ของสินทรัพย์ประเภทสารสนเทศ	แก้ไขครั้งที่ 0

แบบฟอร์มการประเมินมูลค่าของสินทรัพย์ประเภทสารสนเทศ

- **รหัสสินทรัพย์ประเภทสารสนเทศ :**

  .....

- **สินทรัพย์ประเภทสารสนเทศ :**

  .....
  .....
  .....

มูลค่า	ระดับมูลค่า	คำอธิบายความสัมพันธ์
มูลค่าด้านความมั่นคง	[ระบุระดับมูลค่า]	[ระบุคำอธิบาย]
มูลค่าด้านการเงิน	[ระบุระดับมูลค่า]	[ระบุคำอธิบาย]
มูลค่าทางด้านธุรกิจ	[ระบุระดับมูลค่า]	[ระบุคำอธิบาย]
มูลค่าโดยรวม	[ระบุระดับมูลค่า]	[ระบุคำอธิบาย]

หมายเหตุ : ระดับของมูลค่าของสินทรัพย์ประเภทสารสนเทศในด้านต่างๆ โดยทั่วไปแบ่งออกเป็น

- สูงที่สุด (Extreme)
- สูงมาก (Very High)
- สูง (High)
- ปานกลาง (Medium)
- น้อย (Low)
- เล็กน้อย (Negligible)

เลขที่เอกสารอ้างอิง: [IAAC-RIK-004-nn]	แบบฟอร์มการประเมินภัยคุกคาม	หน้า 1/1
รหัสโครงการ: [.....]	ของสินทรัพย์ประเภทสารสนเทศ	แก้ไขครั้งที่ 0

แบบฟอร์มการประเมินภัยคุกคามของสินทรัพย์ประเภทสารสนเทศ

- **รหัสสินทรัพย์ประเภทสารสนเทศ :**

  .....

- **สินทรัพย์ประเภทสารสนเทศ :**

  .....
  .....
  .....

ลำดับ	ภัยคุกคาม	ระดับความเป็นไปได้	ผลกระทบจากภัยคุกคาม
1	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
2	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
3	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
4	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
5	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
.	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
.	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
.	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
.	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]
.	[ระบุภัยคุกคาม]	[ระบุความเป็นไปได้]	[ระบุผลกระทบ]

หมายเหตุ : ระดับของความเป็นไปได้ที่จะเกิดภัยคุกคามใดๆ ขึ้นกับสินทรัพย์ประเภทสารสนเทศ โดยทั่วไปแบ่งออกเป็น

- สูงที่สุด (Extreme)
- สูงมาก (Very High)
- สูง (High)
- ปานกลาง (Medium)
- น้อย (Low)
- เล็กน้อย (Negligible)

เลขที่เอกสารอ้างอิง: [IAAC-RIK-005-nn]	แบบฟอร์มการประเมินภาวะเสี่ยง	หน้า 1/1
รหัสโครงการ: [.....]	ของสินทรัพย์ประเภทสารสนเทศ	แก้ไขครั้งที่ 0

แบบฟอร์มการประเมินภาวะเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

- **รหัสสินทรัพย์ประเภทสารสนเทศ :**

  .....

- **สินทรัพย์ประเภทสารสนเทศ :**

  .....
  .....
  .....

ลำดับ	ภาวะจุดอ่อน	ระดับความรุนแรง	คำอธิบายความสัมพันธ์
1	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
2	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
3	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
4	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
5	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
.	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
.	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
.	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
.	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]
.	[ระบุจุดอ่อน]	[ระบุความรุนแรง]	[ระบุคำอธิบาย]

หมายเหตุ : ระดับความรุนแรงของภาวะจุดอ่อนในแต่ละสินทรัพย์ประเภทสารสนเทศ โดยทั่วไปแบ่งออกเป็น

- สูงที่สุด (Extreme)
- สูงมาก (Very High)
- สูง (High)
- ปานกลาง (Medium)
- น้อย (Low)
- เล็กน้อย (Negligible)

เลขที่เอกสารอ้างอิง: [IAAC-RIK-006-nn]	แบบฟอร์มการกำหนดค่าความเสี่ยง	หน้า 1/1
รหัสโครงการ: [.....]	ของสินทรัพย์ประเภทสารสนเทศ	แก้ไขครั้งที่ 0

แบบฟอร์มการกำหนดค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

ลำดับ	รหัสสินทรัพย์	สินทรัพย์สารสนเทศ	ค่าความเสี่ยง	ระดับค่าความเสี่ยง	คำอธิบาย
1	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
2	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
3	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
4	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
5	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
6	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
7	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
8	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
9	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
10	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
.	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
.	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
.	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
.	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]
.	[ระบุรหัส]	[ระบุสินทรัพย์]	[ระบุค่าความเสี่ยง]	[ระบุค่าความเสี่ยง]	[ระบุคำอธิบาย]

<u>หมายเหตุ</u>: สามารถแบ่งระดับค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ โดยที่ให้ M แทนค่าความเสี่ยงที่คำนวณได้ และ S แทน M/6

- สูงที่สุด (Extreme) : 5S+1 ถึง 6S
- สูงมาก (Very High) : 4S+1 ถึง 5S
- สูง (High) : 3S+1 ถึง 4S
- ปานกลาง (Medium) : 2S+1 ถึง 3S
- น้อย (Low) : S+1 ถึง 2S
- เล็กน้อย (Negligible) : 1 ถึง S

เลขที่เอกสารอ้างอิง: [IAAC-RIK-007-nn]	แบบฟอร์มการกำหนดแนวคิดความมั่นคงของสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มการกำหนดแนวคิดความมั่นคงของสินทรัพย์ประเภทสารสนเทศ

รหัสสินทรัพย์ประเภทสารสนเทศ :	**สินทรัพย์ประเภทสารสนเทศ** :

ความสำคัญทางธุรกิจ : ☐ สูง ☐ กลาง ☐ ต่ำ

.....

.....

การรักษาความลับ (Confidentiality)

การป้องกัน (Detection) : ☐ สูง ☐ กลาง ☐ ต่ำ

.....

.....

การทวนหา (Prevention) : ☐ สูง ☐ กลาง ☐ ต่ำ

.....

.....

ความบูรณาภาพ (Integrity)

การป้องกัน (Detection) : ☐ สูง ☐ กลาง ☐ ต่ำ

.....

.....

การทวนหา (Prevention) : ☐ สูง ☐ กลาง ☐ ต่ำ

.....

.....

การตอบสนอง (Response) : ☐ สูง ☐ กลาง ☐ ต่ำ

.....

.....

เลขที่เอกสารอ้างอิง: [IAAC-RIK-007-nn]	แบบฟอร์มการกำหนดแนวคิดความมั่นคงของสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

สภาพพร้อมใช้งาน (Availability)
การป้องกัน (Detection) : ☐ สูง ☐ กลาง ☐ ต่ำ ....
การทวนหา (Prevention) : ☐ สูง ☐ กลาง ☐ ต่ำ ....
การตอบสนอง (Response) : ☐ สูง ☐ กลาง ☐ ต่ำ ....
ภาระรับผิดชอบ (Accountability)
การป้องกัน (Detection) : ☐ สูง ☐ กลาง ☐ ต่ำ ....
การตอบสนอง (Response) : ☐ สูง ☐ กลาง ☐ ต่ำ ....

เลขที่เอกสารอ้างอิง: [IAAC-AC-001-nn]	แบบฟอร์มรายการเข้าถึงสินทรัพย์	หน้า 1/1
รหัสโครงการ: [.....]	ประเภทสารสนเทศแบบให้อำนาจ	แก้ไขครั้งที่ 0

แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภทสารสนเทศแบบให้อำนาจ

- **รหัสสินทรัพย์ประเภทสารสนเทศ :**

  .....

- **สินทรัพย์ประเภทสารสนเทศ :**

  .....

  .....

  .....

สิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	สิทธิในการเข้าถึง	คำอธิบายความสัมพันธ์
1	[ระบุสิทธิ]	[ระบุคำอธิบาย]
2	[ระบุสิทธิ]	[ระบุคำอธิบาย]
3	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]

ผู้ใช้งานที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	ผู้ใช้งาน/กลุ่มผู้ใช้งาน	หมายเหตุ
1	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
2	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
3	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]

แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภทสารสนเทศเชิงบทบาท

- **บทบาท : .....**
  .....
- **รหัสสินทรัพย์ประเภทสารสนเทศ :**
  .....
- **สินทรัพย์ประเภทสารสนเทศ :**
  .....
  .....
  .....

สิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	สิทธิในการเข้าถึง	คำอธิบายความสัมพันธ์
1	[ระบุสิทธิ]	[ระบุคำอธิบาย]
2	[ระบุสิทธิ]	[ระบุคำอธิบาย]
3	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]

ผู้ใช้งานที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	ผู้ใช้งาน/กลุ่มผู้ใช้งาน	หมายเหตุ
1	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
2	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
3	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]

เลขที่เอกสารอ้างอิง: [IAAC-AC-003-nn]	แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภท	หน้า 1/1
รหัสโครงการ: [.....]	สารสนเทศแบบความมั่นคงหลายระดับ	แก้ไขครั้งที่ 0

แบบฟอร์มรายการเข้าถึงสินทรัพย์ประเภทสารสนเทศ แบบความมั่นคงหลายระดับ

- **บทบาท :** .....
  .....
- **ระดับบทบาท (ถ้ามี)** :
  ☐ อย่างมากที่สุด ☐ สูงมาก ☐ สูง ☐ ต่ำ ☐ ซึ่งไม่สำคัญ
- **รหัสสินทรัพย์ประเภทสารสนเทศ :**
  .....
- **สินทรัพย์ประเภทสารสนเทศ :**
  .....
  .....
- **ระดับสินทรัพย์ประเภทสารสนเทศ (ถ้ามี)** :
  ☐ อย่างมากที่สุด ☐ สูงมาก ☐ สูง ☐ ต่ำ ☐ ซึ่งไม่สำคัญ

สิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	สิทธิในการเข้าถึง	คำอธิบายความสัมพันธ์
1	[ระบุสิทธิ]	[ระบุคำอธิบาย]
2	[ระบุสิทธิ]	[ระบุคำอธิบาย]
3	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]

ผู้ใช้งานที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	ผู้ใช้งาน/กลุ่มผู้ใช้งาน	หมายเหตุ
1	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
2	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
3	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]
.	[ระบุผู้ใช้งาน]	[ระบุหมายเหตุ]

เลขที่เอกสารอ้างอิง: [IAAC-AC-004-nn]	แบบฟอร์มรายการกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

- **บทบาท :** .....
  .....
- **ระดับบทบาท (ถ้ามี)** :
  ☐ อย่างมากที่สุด ☐ สูงมาก ☐ สูง ☐ ต่ำ ☐ ซึ่งไม่สำคัญ
- **รหัสสินทรัพย์ประเภทสารสนเทศ :**
  .....
- **สินทรัพย์ประเภทสารสนเทศ :**
  .....
  .....
- **ระดับสินทรัพย์ประเภทสารสนเทศ (ถ้ามี)** :
  ☐ อย่างมากที่สุด ☐ สูงมาก ☐ สูง ☐ ต่ำ ☐ ซึ่งไม่สำคัญ

สิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ลำดับ	สิทธิในการเข้าถึง	คำอธิบายความสัมพันธ์
1	[ระบุสิทธิ]	[ระบุคำอธิบาย]
2	[ระบุสิทธิ]	[ระบุคำอธิบาย]
3	[ระบุสิทธิ]	[ระบุคำอธิบาย]
.	[ระบุสิทธิ]	[ระบุคำอธิบาย]

กฎหรือข้อบังคับของการตรวจสอบการเข้าถึง

ลำดับ	ชื่อกลุ่มของกฎหรือข้อบังคับ	กฎหรือข้อบังคับ	หมายเหตุ
1	[ระบุชื่อกลุ่ม]	[ระบุกฎหรือข้อบังคับ]	
2	[ระบุชื่อกลุ่ม]	[ระบุกฎหรือข้อบังคับ]	
3	[ระบุชื่อกลุ่ม]	[ระบุกฎหรือข้อบังคับ]	

เลขที่เอกสารอ้างอิง: [IAAC-PN-001-nn]	แบบฟอร์มรายการจัดการ	หน้า 1/1
รหัสโครงการ: [.....]	ความเสี่ยงโครงการ	แก้ไขครั้งที่ 0

แบบฟอร์มรายการจัดการความเสี่ยงของการพัฒนาระบบ

ความเสี่ยงโครงการ
▪ **ประเภทของความเสี่ยง :** ☐ การบริหารจัดการการพัฒนาระบบ ☐ องค์กร ☐ เทคนิคของการพัฒนา ☐ ส่วนภายนอกที่มีความเกี่ยวข้อง [เพิ่มเติม]..... ..... ▪ **ความเสี่ยง :** ....
▪ **ระดับของความเสี่ยง :** ☐ สูงมาก ☐ มาก ☐ ปานกลาง ☐ น้อย
▪ **ระดับโอกาสในการเกิดความเสี่ยง :** ☐ สูงมาก ☐ มาก ☐ ปานกลาง ☐ น้อย
▪ **ระดับความรุนแรงของผลกระทบ :** ☐ สูงมาก ☐ มาก ☐ ปานกลาง ☐ น้อย

<u>การจัดการความเสี่ยงโครงการ</u>

▪ **วิธีการจัดการความเสี่ยง :**

☐ หลีกเลี่ยง ☐ ยอมรับ ☐ ทำให้ลดลง ☐ ถ่ายโอน

[เพิ่มเติม].....

.....

เลขที่เอกสารอ้างอิง: [IAAC-PN-001-nn]	แบบฟอร์มรายการจัดการ	หน้า 1/1
รหัสโครงการ: [.....]	ความเสี่ยงโครงการ	แก้ไขครั้งที่ 0

- **การจัดการความเสี่ยง :**

.....
.....
.....
.....
.....
.....
.....
.....
.....

- **สิ่งที่คาดว่าจะได้รับ :**

.....
.....
.....
.....
.....
.....
.....

- **งบประมาณและทรัพยากรที่จำเป็นต้องใช้ :**

.....
.....
.....
.....
.....
.....
.....

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IM-001-nn]	แบบฟอร์มรายงานผลการประเมินการอบรมผู้ใช้งาน/สมาชิกทีมการทำงานและผู้ที่เกี่ยวข้องกับการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [……..……]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานผลการประเมินการอบรมผู้ใช้งาน/ เจ้าหน้าที่ดำเนินการและผู้ที่เกี่ยวข้องกับ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการอบรม ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

- **ผลการประเมินการอบรม :**

  ……
  ……
  ……

- **อภิปรายและสรุปผลการประเมินการอบรม :**

  ……
  ……
  ……

- **ข้อจำกัดของการอบรม :**

  ……
  ……

- **แนวทางเสนอแนะและการแก้ไขปรับปรุง :**

  ……
  ……

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IM-002-nn]	แบบฟอร์มรายงานความก้าวหน้า การพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานความก้าวหน้าการพัฒนา ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

รายงานครั้งที่ : n

== ข้อมูลระบบ ==

ชื่อระบบ : _____

เวอร์ชันระบบ : [_____]

รายงานสถานะ : _____

_____

สิ่งส่งมอบ

ลำดับ	กิจกรรม	วันที่มอบหมาย	วันที่คาดว่าจะแล้วเสร็จ	ผู้รับผิดชอบ	หมายเหตุ
1	[ระบุกิจกรรม]	[ระบุวันที่]	[ระบุวันที่]	[ระบุผู้รับผิดชอบ]	
2	[ระบุกิจกรรม]	[ระบุวันที่]	[ระบุวันที่]	[ระบุผู้รับผิดชอบ]	
3	[ระบุกิจกรรม]	[ระบุวันที่]	[ระบุวันที่]	[ระบุผู้รับผิดชอบ]	

คำแนะนำและความต้องการเพื่อการตัดสินใจ

ลำดับ	กิจกรรม	วันที่มอบหมาย	วันที่คาดว่าจะแล้วเสร็จ	ผู้รับผิดชอบ	หมายเหตุ
1	[ระบุกิจกรรม]	[ระบุวันที่]	[ระบุวันที่]	[ระบุผู้รับผิดชอบ]	
2	[ระบุกิจกรรม]	[ระบุวันที่]	[ระบุวันที่]	[ระบุผู้รับผิดชอบ]	
3	[ระบุกิจกรรม]	[ระบุวันที่]	[ระบุวันที่]	[ระบุผู้รับผิดชอบ]	

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IM-003-nn]	แบบฟอร์มรายงานความเปลี่ยนแปลงของการพัฒนาการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานความเปลี่ยนแปลงของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

รายงานครั้งที่ : n

== ข้อมูลระบบ ==

ชื่อระบบ : _____

เวอร์ชันระบบ : [_____]

รายงานสถานะ : _____

_____

ข้อมูลการเปลี่ยนแปลง
กิจกรรมหรืองานที่ต้องการจะเปลี่ยนแปลง : ....
รายละเอียดของสิ่งที่ต้องการให้เปลี่ยนแปลง : ....
เหตุผลที่จำเป็นต้องเปลี่ยน : ....
ความสำคัญ : ☐ สูง ☐ กลาง ☐ ต่ำ
ผลกระทบถ้าไม่ได้ทำการเปลี่ยนแปลง : ....

เลขที่เอกสารอ้างอิง: [IAAC-IM-003-nn]	แบบฟอร์มรายงานความเปลี่ยนแปลงของการพัฒนาการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

การวิเคราะห์ผลกระทบจากการเปลี่ยน

ผลกระทบกับความต้องการของโครงการ : ☐ ในขอบเขต ☐ นอกขอบเขต

ผลกระทบต่อวัตถุประสงค์ของโครงการ :

.....

.....

.....

ผลกระทบต่อโครงสร้างของโครงการ :

.....

.....

.....

ผลกระทบต่อการส่งมอบโครงการ :

.....

.....

.....

ผลกระทบต่อความเสี่ยงของโครงการ :

.....

.....

.....

ผลกระทบต่อกำหนดการของโครงการ :

.....

.....

.....

ผลกระทบต่องบประมาณของโครงการ :

.....

.....

.....

ข้อเสนอแนะ :

.....

.....

เลขที่เอกสารอ้างอิง: [IAAC-IM-003-nn]	แบบฟอร์มรายงานความเปลี่ยนแปลงของการพัฒนาการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

รายละเอียดของการเปลี่ยนแปลง	
ผลการอนุมัติ : ☐ อนุมัติ ☐ ผ่อนผัน ☐ ไม่อนุมัติ	วันที่อนุมัติ
ผู้ตัดสินใจ : ☐ เจ้าของโครงการ ☐ ผู้ดูแลโครงการ ☐ อื่นๆ	**ลายเซ็นต์ :**
เหตุผลการตัดสินใจ *:*	

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IM-006-nn]	แบบฟอร์มรายการกรณีทดสอบสำหรับใช้ทดสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [……..……]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการกรณีทดสอบสำหรับใช้ทดสอบ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการทดสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

ระดับการทดสอบ : ☐ Acceptance ☐ System ☐ Integration ☐ Unit

……

……

กรณีทดสอบ: [ระบุฟังก์ชันการทำงาน]

รหัสกรณีทดสอบ	ชื่อการทดสอบ	ข้อมูลนำเข้า	ค่าคาดหวัง	ค่าจริง	หมายเหตุ
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุข้อมูลนำเข้า]	[ระบุค่าคาดหวัง]	[ระบุค่าจริง]	

เลขที่เอกสารอ้างอิง: [IAAC-IM-005-nn]	แบบฟอร์มรายงานผลการทดสอบ ระบบการควบคุมการเข้าถึง สินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [……..…..]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานผลการทดสอบ
ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

รายงานครั้งที่ : n

== ข้อมูลแผนการทดสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

ผู้รับผิดชอบ	
วันที่เริ่มทดสอบ	**วันที่สิ้นสุดการทดสอบ**
ชื่อระบบ	**เวอร์ชัน**

ระดับการทดสอบ : ☐ Acceptance ☐ System ☐ Integration ☐ Unit

……

……

ผลการทดสอบ

สถานะ Red / Amber / Green (RAG)	[ระบุสถานะ]
รายละเอียดสถานะ : …… ……	
การรับรองคุณภาพภายหลังจากการทดสอบ : …… ……	

วัตถุประสงค์ของการทดสอบ	**เป้าหมาย**	**ผลลัพธ์**
การทดสอบตามความต้องการของระบบ	100%	
การทดสอบตามข้อผิดพลาดที่กำหนดไว้	100%	

เลขที่เอกสารอ้างอิง: [IAAC-IM-005-nn]	แบบฟอร์มรายงานผลการทดสอบ ระบบการควบคุมการเข้าถึง สินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [……..…..]		แก้ไขครั้งที่ 0

สรุปผลการทดสอบ

รหัสกรณีทดสอบ	ชื่อการทดสอบ	ฟังก์ชันการทำงาน	ผลการทดสอบ (ผ่าน/ไม่ผ่าน)	ระดับความรุนแรง	หมายเหตุ
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	
[ระบุรหัส]	[ระบุการทดสอบ]	[ระบุฟังก์ชัน]	[ระบุผลทดสอบ]	[ระบุระดับ]	

เลขที่เอกสารอ้างอิง: [IAAC-MR-001-nn]	แบบฟอร์มรายงานผลการเฝ้าสังเกตและทวนสอบระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานผลการเฝ้าสังเกตและทวนสอบ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

ผู้รับผิดชอบ	
วันที่เริ่มเฝ้าสังเกตและทวนสอบ	**วันที่สิ้นสุดการเฝ้าสังเกตและทวนสอบ**
ชื่อระบบ	**เวอร์ชัน**

ส่วนที่ทำการเฝ้าสังเกตและทวนสอบ :	**ข้อมูลที่ทำการเฝ้าสังเกตและทวนสอบ :**
ผลการเฝ้าสังเกตและทวนสอบ :	
สรุปผลการเฝ้าสังเกตและทวนสอบ :	

เลขที่เอกสารอ้างอิง: [IAAC-MR-002-nn]	แบบฟอร์มรายงานผลการประเมินประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานผลการประเมินประสิทธิภาพของ ระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

ผู้รับผิดชอบ	
วันที่เริ่มประเมิน	**วันที่สิ้นสุดการประเมิน**
ชื่อระบบ	**เวอร์ชัน**

ส่วนที่ต้องการทำการประเมิน :	**ข้อมูลที่ต้องการทำการประเมิน :**
ตัวชี้วัดประสิทธิภาพ :	
ผลการประเมิน :	
วิเคราะห์ผลการประเมิน เมื่อเทียบกับค่าคาดหมาย (Based Line) :	
สรุปผลการประเมิน : **ระดับการยอมรับ :** ☐ มากที่สุด ☐ มาก ☐ ปานกลาง ☐ น้อย	

เลขที่เอกสารอ้างอิง : [IAAC-MR-002-nn]	**[ชื่อแฟ้ม.นามสกุล]**	**วันที่พิมพ์ [วัน เดือน ปี]**

เลขที่เอกสารอ้างอิง: [IAAC-MR-003-nn]	แบบฟอร์มรายงานผลการปรับ แผนการเฝ้าสังเกตและทวนสอบระบบ	หน้า 1/1
รหัสโครงการ: [……..……]		แก้ไขครั้งที่ 0

แบบฟอร์มรายงานผลการปรับ แผนการเฝ้าสังเกตและทวนสอบระบบ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

- **หัวข้อภายในแผนที่ต้องการปรับเปลี่ยน :**

  ……
  ……
  ……
  ……
  ……
  ……
  ……
  ……

- **รายละเอียดของการปรับเปลี่ยน :**

  ……
  ……
  ……
  ……
  ……
  ……
  ……
  ……

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-MR-004-nn]	แบบฟอร์มรายการการกระทำและเหตุการณ์ที่ซึ่งส่งผลต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการการกระทำและเหตุการณ์ที่ซึ่งส่งผลต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

การกระทำ (Action)

ลำดับ	การกระทำ	ระดับความรุนแรง	ผลต่อประสิทธิภาพ	รายละเอียด
1	[ระบุการกระทำ]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]
2	[ระบุการกระทำ]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]
3	[ระบุการกระทำ]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]
.	[ระบุการกระทำ]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]

เหตุการณ์ (Event)

ลำดับ	เหตุการณ์	ระดับความรุนแรง	ผลต่อประสิทธิภาพ	รายละเอียด
1	[ระบุเหตุการณ์]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]
2	[ระบุเหตุการณ์]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]
3	[ระบุเหตุการณ์]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]
.	[ระบุเหตุการณ์]	[ระบุระดับ]	[ระบุผลกระทบ]	[ระบุรายละเอียด]

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IMP-001-nn]	แบบฟอร์มวิเคราะห์การกรทำและเหตุการณ์ที่ซึ่งส่งผลกระทบต่อประสิทธิภาพของระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มวิเคราะห์การกระทำและเหตุการณ์ที่ซึ่งส่งผลต่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

== ข้อมูลแผนการปรับปรุงระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

รายละเอียดการกระทำหรือเหตุการณ์ :

.....

.....

สาเหตุที่การกระทำหรือเหตุการณ์นั้น มีผลกระทบต่อประสิทธิภาพของระบบ :

.....

.....

ระดับการยอมรับ : ☐ มากที่สุด ☐ มาก ☐ ปานกลาง ☐ น้อย

วิเคราะห์ผลของการยอมรับ

.....

.....

.....

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง : [IAAC-IMP-001-nn]	[ชื่อแฟ้ม.นามสกุล]	วันที่พิมพ์ [วัน เดือน ปี]

เลขที่เอกสารอ้างอิง: [IAAC-IMP-002-nn]	แบบฟอร์มรายการการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการการกระทำและการป้องกันสำหรับการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

== ข้อมูลแผนการปรับปรุงระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

รายละเอียดการกระทำหรือเหตุการณ์ :

.....

.....

.....

การกระทำ (Corrective Action) **หรือการป้องกัน** (Preventive Action) *:*

ระดับความสำคัญ : ☐ มากที่สุด ☐ มาก ☐ ปานกลาง ☐ น้อย

.....

.....

.....

ส่วนการทำงานของระบบที่ต้องการปรับปรุง *:*

.....

.....

.....

ลงนามผู้รับผิดชอบ : _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IMP-003-nn]	แบบฟอร์มข้อเสนอแนะของผู้ที่เกี่ยวข้องต่อการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มข้อเสนอแนะของผู้ที่เกี่ยวข้องต่อการปรับปรุงระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

== ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

== ข้อมูลแผนการปรับปรุงระบบ ==

ชื่อแผน : _____

เวอร์ชันแผน : [_____]

รายละเอียดการกระทำหรือการป้องกัน :

.....

.....

วัตถุประสงค์ของข้อเสนอแนะ :

.....

.....

ระดับความสำคัญ : ☐ มากที่สุด ☐ มาก ☐ ปานกลาง ☐ น้อย

ข้อเสนอแนะ :

.....

.....

.....

ลงนามผู้รับผิดชอบ : _____

(_____)

[ระบุส่วนงาน]

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-VF-001-nn]	แบบฟอร์มรายการทวนสอบข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการทวนสอบข้อกำหนด การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

- **ตำแหน่งข้อผิดพลาด :**
  - ☐ กำหนดความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น
  - ☐ ข้อกำหนดวิธีการการควบคุมการเข้าถึง
  - ☐ ข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน

  [เพิ่มเติม].....
  .....
- **ระดับของข้อผิดพลาด :**
  ☐ วิกฤต ☐ มาก ☐ ปานกลาง ☐ น้อย
- **ข้อผิดพลาด :**
  .....
  .....
  .....
- **สาเหตุของข้อผิดพลาด เมื่อเทียบกับหลักความมั่นคงของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ :**
  .....
  .....
- **แนวทางเสนอแนะการแก้ไข :**
  .....
  .....

ลงนามผู้ทวนสอบ: _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-VF-002-nn]	แบบฟอร์มรายการทวนสอบข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยยึดนโยบายและกลยุทธ์เป็นหลัก	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการทวนสอบข้อกำหนดการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ โดยยึดนโยบายและกลยุทธ์เป็นหลัก

- **ตำแหน่งข้อผิดพลาด :**
  - ☐ ข้อกำหนดความเสี่ยงของสินทรัพย์ประเภทสารสนเทศและการป้องกันรักษาความเสี่ยงนั้น
  - ☐ ข้อกำหนดวิธีการการควบคุมการเข้าถึง
  - ☐ ข้อกำหนดของการออกแบบและใช้งานรหัสผ่าน

  [เพิ่มเติม].....
  .....
- **ระดับของข้อผิดพลาด :**

  ☐ วิกฤต ☐ มาก ☐ ปานกลาง ☐ น้อย
- **ข้อผิดพลาด :**

  .....
  .....
  .....
- **สาเหตุของข้อผิดพลาด เมื่อเทียบกับนโยบายและกลยุทธ์การควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ :**

  .....
  .....
- **แนวทางเสนอแนะการแก้ไข :**

  .....
  .....

ลงนามผู้ทวนสอบ: _____

(_____)

วัน / เดือน / ปี

เลขที่เอกสารอ้างอิง: [IAAC-IM-004-nn]	แบบฟอร์มรายการตรวจสอบความครบถ้วนของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [.....]		แก้ไขครั้งที่ 0

แบบฟอร์มรายการตรวจสอบความครบถ้วนของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ความครบถ้วนของความต้องการต่อผลิตภัณฑ์ (Product Checklist)

ลำดับ	รายละเอียด	Y/N or Developing	หมายเหตุ
Functional Requirements			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
Non-Functional Requirement s			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	

ความครบถ้วนของกิจกรรมที่ต้องทำในแต่ละเฟสการทำงาน (Project Manager Checklist)

ลำดับ	รายละเอียด	Y/N or Developing	หมายเหตุ
Project Initiation			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	

เลขที่เอกสารอ้างอิง: [IAAC-IM-004-nn]	แบบฟอร์มรายการตรวจสอบความครบถ้วนของการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ	หน้า 1/1
รหัสโครงการ: [……..…..]		แก้ไขครั้งที่ 0

ลำดับ	รายละเอียด	Y/N or Developing	หมายเหตุ
Project Planning			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
Project Execution			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
Project Monitoring and Control			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
Project Closure			
1	[ระบุรายละเอียด]	[ระบุสถานะ]	
2	[ระบุรายละเอียด]	[ระบุสถานะ]	
3	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	
.	[ระบุรายละเอียด]	[ระบุสถานะ]	

ภาคผนวก ง
โครงสร้างตารางข้อมูล

ตารางข้อมูลของเครื่องมือสนับสนุนกระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ มีทั้งหมด 57 ตาราง ซึ่งสามารถสรุปได้ดังตารางที่ ง.1 ทั้งนี้โครงสร้างของตารางข้อมูลทั้งหมดสามารถแสดงได้ดังตารางที่ ง.2 - ง.58

ตารางที่ ง.1 สรุปตารางข้อมูลของเครื่องมือสนับสนุนกระบวนการ

ลำดับ	ชื่อตาราง	คำอธิบาย
1	iaac_team	ข้อมูลผู้ใช้งานระบบ
2	iaac_position	ข้อมูลบทบาทภายในระบบ
3	iaac_phase	ข้อมูลเมนูขั้นตอนหลัก
4	iaac_subphase	ข้อมูลเมนูขั้นตอนย่อย
5	iaac_authentication	ข้อมูลบทบาทของผู้ใช้งานระบบ
6	iaac_uploadfile	ข้อมูลเอกสารสนับสนุนกระบวนการ
7	iaac_inititation	ข้อมูลเริ่มต้นกระบวนการ
8	iaac_policy	ข้อมูลนโยบายกระบวนการ
9	iaac_strategy	ข้อมูลกลยุทธ์กระบวนการ
10	iaac_riskassessment	ข้อมูลการประเมินความเสี่ยง
11	iaac_residualrisk	ข้อมูลการจัดการความเสี่ยงที่คงเหลือ
12	iaac_asset	ข้อมูลสินทรัพย์ประเภทสารสนเทศ
13	iaac_assetcategoty	ข้อมูลหมวดหมู่ของสินทรัพย์ประเภทสารสนเทศ
14	iaac_classificationlevel	ข้อมูลการจำแนกสินทรัพย์ประเภทสารสนเทศ
15	iaac_businessfactor	ข้อมูลปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ
16	iaac_businessfactor_asset	ข้อมูลปัจจัยทางธุรกิจของสินทรัพย์ประเภทสารสนเทศ
17	iaac_securityproperty_asset	ข้อมูลคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
18	iaac_threat	ข้อมูลภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ
19	iaac_vulnerability	ข้อมูลจุดอ่อนที่ถูกใช้โดยภัยคุกคาม
20	iaac_riskvalue	ข้อมูลมูลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
21	iaac_risktreatment	ข้อมูลการป้องกันรักษาความเสี่ยงของสินทรัพย์สารสนเทศ
22	iaac_acselection_factor	ข้อมูลปัจจัยในการเลือกใช้โมเดลวิธีการควบคุมการเข้าถึง
23	iaac_user	ข้อมูลผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.1 สรุปตารางข้อมูลของเครื่องมือสนับสนุนกระบวนการ (ต่อ)

ลำดับ	ชื่อตาราง	คำอธิบาย
24	iaac_usergroup	ข้อมูลกลุ่มผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
25	iaac_clearancelevel	ข้อมูลระดับของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
26	iaac_role	ข้อมูลบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
27	iaac_assetrole	ข้อมูลความสัมพันธ์ระหว่างสินทรัพย์ประเภทสารสนเทศและบทบาท
28	iaac_right	ข้อมูลสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
29	iaac_authorization	ข้อมูลกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
30	iaac_authorizationgroup	ข้อมูลกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
31	iaac_referencemonitor	ข้อมูลความสัมพันธ์ระหว่างบทบาทและกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์สารสนเทศ
32	iaac_passwordrequirements	ข้อมูลความต้องการของการออกแบบและใช้งานรหัสผ่าน
33	iaac_passworddesign	ข้อมูลการออกแบบและใช้งานรหัสผ่าน
34	iaac_review	ข้อมูลการตรวจสอบข้อกำหนดกระบวนการ
35	iaac_reviewpolicy	ข้อมูลการตรวจสอบข้อกำหนดกระบวนการเมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ
36	iaac_systemplan	ข้อมูลแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
37	iaac_riskmanagement	ข้อมูลการจัดการความเสี่ยงของการพัฒนาระบบ
38	iaac_progressreporting	ข้อมูลความก้าวหน้าของการพัฒนาระบบ
39	iaac_changemanagement	ข้อมูลการเปลี่ยนแปลงของการพัฒนาระบบ
40	iaac_systemchecklist	ข้อมูลรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ
41	iaac_testplan	ข้อมูลแผนการทดสอบระบบ
42	iaac_testresult	ข้อมูลผลการทดสอบระบบ
43	iaac_testrecord	ข้อมูลบันทึกการทดสอบระบบ
44	iaac_trainingplan	ข้อมูลแผนการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง

ตารางที่ ง.1 สรุปตารางข้อมูลของเครื่องมือสนับสนุนกระบวนการ (ต่อ)

ลำดับ	ชื่อตาราง	คำอธิบาย
45	iaac_trainingsummery	ข้อมูลผลการประเมินการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง
46	iaac_monitoringplan	ข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ
47	iaac_monitoringresult	ข้อมูลผลการเฝ้าสังเกตและทวนสอบระบบ
48	iaac_measurementresult	ข้อมูลผลการวัดประสิทธิภาพของระบบ
49	iaac_monitoring_measure	ข้อมูลความสัมพันธ์ระหว่างข้อมูลการเฝ้าสังเกตและทวนสอบระบบและข้อมูลการวัดประสิทธิภาพของระบบ
50	iaac_matric	ข้อมูลตัวชี้วัดประสิทธิภาพของระบบ
51	iaac_measurement_matric	ข้อมูลความสัมพันธ์ระหว่างการวัดประสิทธิภาพระบบและตัวชี้วัด
52	iaac_changingplan_result	ข้อมูลผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบ
53	iaac_actionevent	ข้อมูลการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
54	iaac_improvementplan	ข้อมูลแผนการปรับปรุงระบบ
55	iaac_actionevent_accepted	ข้อมูลผลการวิเคราะห์การยอมรับของการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
56	iaac_correctivepreventive	ข้อมูลการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
57	iaac_stakeholdersuggetion	ข้อมูลข้อเสนอแนะต่อการกระทำและการป้องกันสำหรับการปรับปรุงระบบของผู้ที่เกี่ยวข้องกับกระบวนการ

ตารางที่ ง.2 โครงสร้างตารางข้อมูลผู้ใช้งานระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
team_id	varchar(10)	รหัสผู้ใช้งานระบบ
team_username	varchar(30)	ชื่อผู้ใช้งานระบบ
team_password	varchar(10)	รหัสผ่าน
team_repassword	varchar(10)	การยืนยันรหัสผ่าน
team_title	varchar(5)	คำนำหน้าชื่อ
team_firstname	varchar(50)	ชื่อ
team_lastname	varchar(50)	นามสกุล
team_address	text	ที่อยู่
team_telnum	varchar(15)	เบอร์โทรศัพท์

ตารางที่ ง.2 โครงสร้างตารางข้อมูลผู้ใช้งานระบบ (ต่อ)

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
team_mobilenum	varchar(15)	เบอร์โทรศัพท์มือถือ
team_email	varchar(50)	อีเมล
team_department	varchar(100)	หน่วยงาน
team_skill	text	ข้อมูลทักษะหรือความชำนาญ
team_experience	text	ข้อมูลประสบการณ์
team_createdate	varchar(15)	วันที่สร้างข้อมูล
team_createby	varchar(50)	ผู้สร้างข้อมูล
position_id	int (2)	บทบาทภายในระบบ

ตารางที่ ง.3 โครงสร้างตารางข้อมูลบทบาทภายในระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
position_id	int (2)	รหัสบทบาท
position_name	varchar(100)	ชื่อบทบาทภายในระบบ

ตารางที่ ง.4 โครงสร้างตารางข้อมูลเมนูขั้นตอนหลัก

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
phase_id	int (2)	รหัสขั้นตอนหลัก
phase_name	varchar(100)	ชื่อขั้นตอนหลัก

ตารางที่ ง.5 โครงสร้างตารางข้อมูลเมนูขั้นตอนย่อย

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
subphase_id	int (2)	รหัสขั้นตอนย่อย
subphase_name	varchar(100)	ชื่อขั้นตอนย่อย
phase_id	int (2)	รหัสขั้นตอนหลัก

ตารางที่ ง.6 โครงสร้างตารางข้อมูลบทบาทของผู้ใช้งานระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
authentication_id	int (2)	รหัสบทบาทของผู้ใช้งาน
position_id	int (2)	รหัสบทบาท
subphase_id	int (2)	รหัสขั้นตอนย่อย

ตารางที่ ง.7 โครงสร้างตารางข้อมูลเอกสารสนับสนุนกระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
upload_id	int (5)	รหัสเอกสารสนับสนุน
upload_documentcategory	varchar(50)	หมวดหมู่เอกสารสนับสนุน
upload_documenttype	varchar(50)	ประเภทเอกสารสนับสนุน
upload_documentversion	varchar(10)	เวอร์ชันของเอกสารสนับสนุน
upload_title	varchar(255)	หัวเรื่องของเอกสารสนับสนุน
upload_description	text	คำอธิบายเอกสารสนับสนุน
upload_filename	varchar(50)	ชื่อไฟล์เอกสารสนับสนุน
upload_filetype	varchar(30)	ประเภทของไฟล์เอกสารสนับสนุน
upload_filesize	int (10)	ขนาดของไฟล์เอกสารสนับสนุน
upload_path	text	ที่อยู่ของไฟล์เอกสารสนับสนุน
upload_createdate	varchar(15)	วันที่อัพโหลดเอกสารสนับสนุน
upload_createby	varchar(50)	ผู้ที่อัพโหลดเอกสารสนับสนุน
subphase_id	int (2)	รหัสขั้นตอนย่อย

ตารางที่ ง.8 โครงสร้างตารางข้อมูลเริ่มต้นกระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
inititation_abstract	text	ที่มาและความสำคัญของกระบวนการ
inititation_scope	text	ขอบเขตของกระบวนการ
inititation_goal	text	เป้าหมายของกระบวนการ
inititation_mission	text	พันธกิจของกระบวนการ
inititation_createdate	varchar(15)	วันที่สร้างข้อมูล
inititation_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.9 โครงสร้างตารางข้อมูลนโยบายกระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
policy_detail	text	รายละเอียดนโยบายของกระบวนการ
policy_concern1	text	ความสอดคล้องต้องกันของการควบคุมการเข้าถึงกับการจัดแบ่งประเภทสินทรัพย์ประเภทสารสนเทศขององค์กร
policy_concern2	text	จัดการสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.9 โครงสร้างตารางข้อมูลนโยบายกระบวนการ (ต่อ)

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
policy_concern3	text	กฎข้อบังคับของการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
policy_concern4	text	ความต้องการของการอนุญาตให้เข้าถึงสินทรัพย์ประเภทสารสนเทศ
policy_concern5	text	การจัดการการถอนสิทธิการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
policy_createdate	varchar(15)	วันที่สร้างข้อมูล
policy_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.10 โครงสร้างตารางข้อมูลกลยุทธ์กระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
strategy_gap	text	ความเหมือนและต่างระหว่างนโยบายกระบวนการและกลยุทธ์องค์กรด้านการจัดการความเสี่ยง
strategy_detail	text	รายละเอียดกลยุทธ์กระบวนการ
strategy_process	text	กระบวนการการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
strategy_createdate	varchar(15)	วันที่สร้างข้อมูล
strategy_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.11 โครงสร้างตารางข้อมูลการประเมินความเสี่ยง

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
riskassessment_method	text	วิธีการของการประเมินความเสี่ยง
riskassessment_criteria	text	เกณฑ์ของการยอมรับความเสี่ยง
riskassessment_acceptedlevel	text	ระดับของการยอมรับความเสี่ยง
riskassessment_createdate	varchar(15)	วันที่สร้างข้อมูล
riskassessment_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.12 โครงสร้างตารางข้อมูลการจัดการความเสี่ยงที่คงเหลือ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
residualrisk_management	text	การจัดการความเสี่ยงที่คงเหลือ
residualrisk_criteria	text	เกณฑ์ในการยอมรับความเสี่ยงที่คงเหลือ
residualrisk_acceptedlevel	text	ระดับในการยอมรับความเสี่ยงที่คงเหลือ
residualrisk_impaction	text	ผลกระทบที่มีต่อองค์กรที่คาดว่าจะเกิดขึ้น ซึ่งเกิดจากความเสี่ยงที่คงเหลือ
residualrisk_createdate	varchar(15)	วันที่สร้างข้อมูล
residualrisk_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.13 โครงสร้างตารางข้อมูลสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ
asset_name	varchar(150)	ชื่อสินทรัพย์ประเภทสารสนเทศ
asset_description	text	คำอธิบายสินทรัพย์ประเภทสารสนเทศ
asset_svalue	int(5)	มูลค่าด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
asset_svalue_description	text	คำอธิบายมูลค่าด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
asset_fvalue	int(5)	มูลค่าด้านการเงินของสินทรัพย์ประเภทสารสนเทศ
asset_fvalue_description	text	คำอธิบายมูลค่าด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
asset_bvalue	int(5)	มูลค่าทางด้านธุรกิจของสินทรัพย์ประเภทสารสนเทศ
asset_bvalue_description	text	คำอธิบายมูลค่าด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
asset_overallvalue	int(5)	มูลค่าโดยรวมของสินทรัพย์ประเภทสารสนเทศ
asset_createdate	varchar(15)	วันที่สร้างข้อมูล
asset_createby	varchar(50)	ผู้สร้างข้อมูล
assetcategoty_id	int(5)	รหัสหมวดหมู่ของสินทรัพย์ประเภทสารสนเทศ
class_id	int(5)	รหัสการจำแนกสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.14 โครงสร้างตารางข้อมูลหมวดหมู่ของสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
assetcategoty_id	int(3)	รหัสหมวดหมู่ของสินทรัพย์ประเภทสารสนเทศ
assetcategoty_name	varchar(100)	หมวดหมู่ของสินทรัพย์ประเภทสารสนเทศ
assetcategoty_description	text	คำอธิบายหมวดหมู่ของสินทรัพย์ประเภทสารสนเทศ
assetcategoty_createdate	varchar(15)	วันที่สร้างข้อมูล
assetcategoty_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.15 โครงสร้างตารางข้อมูลการจำแนกสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
class_id	int(3)	รหัสการจำแนกสินทรัพย์ประเภทสารสนเทศ
class_name	varchar(100)	การจำแนกสินทรัพย์ประเภทสารสนเทศ
class_description	text	คำอธิบายการจำแนกสินทรัพย์ประเภทสารสนเทศ
class_createdate	varchar(15)	วันที่สร้างข้อมูล
class_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.16 โครงสร้างตารางข้อมูลปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
businessfactor_id	int(3)	รหัสปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ
businessfactor_name	varchar(100)	ปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ
businessfactor_description	text	คำอธิบายปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ
businessfactor _createdate	varchar(15)	วันที่สร้างข้อมูล
businessfactor _createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.17 โครงสร้างตารางข้อมูลปัจจัยทางธุรกิจของสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
businessfactorasset_id	int (5)	รหัสปัจจัยทางธุรกิจของสินทรัพย์ประเภทสารสนเทศ
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ
businessfactor_id	int(3)	รหัสปัจจัยทางธุรกิจที่มีผลต่อสินทรัพย์ประเภทสารสนเทศ
description	text	คำอธิบายปัจจัยทางธุรกิจของสินทรัพย์ประเภทสารสนเทศ
createdate	varchar(15)	วันที่สร้างข้อมูล
createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.18 โครงสร้างตารางข้อมูลคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
securitypropertyasset_id	int (5)	รหัสคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ
securityproperty	varchar(100)	คุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
description	text	อธิบายคุณสมบัติด้านความมั่นคงของสินทรัพย์ประเภทสารสนเทศ
impaction	text	ผลกระทบที่มีต่อองค์กร เมื่อเกิดการสูญเสียคุณสมบัติด้านความมั่นคงนั้นๆ
createdate	varchar(15)	วันที่สร้างข้อมูล
createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.19 โครงสร้างตารางข้อมูลภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
threat_id	varchar(10)	รหัสภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ
threat_action	text	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ
threat_likelihood	int (5)	ระดับความถี่ของภัยคุกคาม
threat_consequence	text	ผลกระทบที่มีต่อองค์กรเมื่อภัยคุกคามใดๆ เกิดขึ้น
threat_createdate	varchar(15)	วันที่สร้างข้อมูล
threat_createby	varchar(50)	ผู้สร้างข้อมูล
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.20 โครงสร้างตารางข้อมูลจุดอ่อนที่ถูกใช้โดยภัยคุกคาม

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
vulnerability_id	varchar(10)	รหัสจุดอ่อนที่ถูกใช้โดยภัยคุกคาม
vulnerability_action	text	จุดอ่อนที่จะถูกใช้โดยภัยคุกคาม
vulnerability_serverity	int (5)	ระดับความรุนแรงเมื่อถูกภัยคุกคามใดๆ โจมตีจุดอ่อน
vulnerability_description	text	คำอธิบายเพิ่มเติม
vulnerability_createdate	varchar(15)	วันที่สร้างข้อมูล
vulnerability_createby	varchar(50)	ผู้สร้างข้อมูล
threat_id	varchar(10)	รหัสภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.21 โครงสร้างตารางข้อมูลมูลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
riskvalue_id	int (5)	รหัสมูลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ
riskvalue	int(5)	มูลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
description	text	คำอธิบายมูลค่าความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
createdate	varchar(15)	วันที่สร้างข้อมูล
createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.22 โครงสร้างตารางข้อมูลการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
treatment_id	int (5)	รหัสการป้องกันรักษาความเสี่ยงของสินทรัพย์ประเภทสารสนเทศ
treatment_businesspriority	int(5)	ลำดับความสำคัญทางธุรกิจของสินทรัพย์ประเภทสารสนเทศ
confidentiality_detection	int(5)	ระดับการป้องกันของการรักษาความลับ
confidentiality_prevention	int(5)	ระดับการทวนหาของการรักษาความลับ
confidentiality_description	text	คำอธิบายการป้องกันรักษาของคุณสมบัติด้านความมั่นคง-การรักษาความลับ
integrity_detection	int(5)	ระดับการป้องกันของความบูรณาภาพ
integrity_prevention	int(5)	ระดับการทวนหาของความบูรณาภาพ
integrity_response	int(5)	ระดับการตอบสนองความบูรณาภาพ
integrity_description	text	คำอธิบายการป้องกันรักษาของคุณสมบัติด้านความมั่นคง-ความบูรณาภาพ
availability_detection	int(5)	ระดับการป้องกันของสภาพพร้อมใช้งาน
availability_prevention	int(5)	ระดับการทวนหาของสภาพพร้อมใช้งาน
availability_response	int(5)	ระดับการตอบสนองสภาพพร้อมใช้งาน
availability_description	text	คำอธิบายการป้องกันรักษาของคุณสมบัติด้านความมั่นคง-สภาพพร้อมใช้งาน
accountability_detection	int(5)	ระดับการป้องกันของภาระรับผิดชอบ
accountability_response	int(5)	ระดับการตอบสนองภาระรับผิดชอบ
accountability_description	text	คำอธิบายการป้องกันรักษาของคุณสมบัติด้านความมั่นคง-ภาระรับผิดชอบ
treatment_createdate	varchar(15)	วันที่สร้างข้อมูล
treatment_createby	varchar(50)	ผู้สร้างข้อมูล
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.23 โครงสร้างตารางข้อมูลปัจจัยในการเลือกใช้โมเดลวิธีการควบคุมการเข้าถึง

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
acselection_factor	text	ปัจจัยในการเลือกใช้โมเดลการควบคุมการเข้าถึง
acselection_model	text	โมเดลการควบคุมการเข้าถึงที่ได้เลือกใช้
acselection_reason	text	เหตุผลของการเลือกใช้โมเดลการควบคุมการเข้าถึงนั้นๆ
acselection_createdate	varchar(15)	วันที่สร้างข้อมูล
acselection_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.24 โครงสร้างตารางข้อมูลผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
user_id	varchar(10)	รหัสผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
user_title	varchar(5)	คำนำหน้าชื่อ
user_firstname	varchar(50)	ชื่อ
user_lastname	varchar(50)	นามสกุล
user_telnum	varchar(15)	เบอร์โทรศัพท์
user_mobilenum	varchar(15)	เบอร์โทรศัพท์มือถือ
user_email	varchar(50)	อีเมล
user_department	varchar(100)	หน่วยงาน
user_createdate	varchar(15)	วันที่สร้างข้อมูล
user_createby	varchar(50)	ผู้สร้างข้อมูล
usergroup_id	int(3)	รหัสกลุ่มผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
clearance_id	int(3)	รหัสระดับของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
role_id	int(3)	รหัสบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.25 โครงสร้างตารางข้อมูลกลุ่มผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
usergroup_id	int(3)	รหัสกลุ่มผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
usergroup_name	varchar(100)	กลุ่มผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
usergroup_description	text	คำอธิบายกลุ่มผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
usergroup_createdate	varchar(15)	วันที่สร้างข้อมูล
usergroup_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.26 โครงสร้างตารางข้อมูลระดับของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
clearance_id	int(3)	รหัสระดับของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
clearance_name	varchar(100)	ระดับของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
clearance_description	text	คำอธิบายระดับของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
clearance_createdate	varchar(15)	วันที่สร้างข้อมูล
clearance_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.27 โครงสร้างตารางข้อมูลบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์สารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
role_id	int(3)	รหัสบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
role_name	varchar(100)	บทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
role_description	text	คำอธิบายบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
role_createdate	varchar(15)	วันที่สร้างข้อมูล
role_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.28 โครงสร้างตารางข้อมูลความสัมพันธ์ระหว่างสินทรัพย์ประเภทสารสนเทศและบทบาท

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
assetrole_id	int(5)	รหัสความสัมพันธ์ระหว่างสินทรัพย์ประเภทสารสนเทศและบทบาท
role_id	int(3)	รหัสบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
asset_id	varchar(10)	รหัสสินทรัพย์ประเภทสารสนเทศ
description	text	คำอธิบายความสัมพันธ์
createdate	varchar(15)	วันที่สร้างข้อมูล
createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.29 โครงสร้างตารางข้อมูลสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
right_id	int(3)	รหัสสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
right_name	varchar(100)	สิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
right_description	text	คำอธิบายสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
right_createdate	varchar(15)	วันที่สร้างข้อมูล
right_createby	varchar(50)	ผู้สร้างข้อมูล
role_id	int(3)	รหัสบทบาทของผู้ใช้ที่มีสิทธิในการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.30 โครงสร้างตารางข้อมูลกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
rule_id	int(5)	รหัสกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
rule_detail	text	รายละเอียดกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
rule_description	text	คำอธิบายกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
rule_createdate	varchar(15)	วันที่สร้างข้อมูล
rule_createby	varchar(50)	ผู้สร้างข้อมูล
authorizationgroup_id	int(3)	รหัสกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ตารางที่ ง.31 โครงสร้างตารางข้อมูลกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
authorizationgroup_id	int(3)	รหัสกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
authorizationgroup_name	varchar(100)	กลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
authorizationgroup_description	text	คำอธิบายกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
authorizationgroup_createdate	varchar(15)	วันที่สร้างข้อมูล
authorizationgroup_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.32 โครงสร้างตารางข้อมูลความสัมพันธ์ระหว่างบทบาทและกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
reference_id	int(5)	รหัสความสัมพันธ์ระหว่างบทบาทและกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
authorizationgroup_id	int(3)	รหัสกลุ่มของกฎหรือข้อบังคับของการตรวจสอบการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
assetrole_id	int(5)	รหัสความสัมพันธ์ระหว่างสินทรัพย์ประเภทสารสนเทศและบทบาท
reference_description	text	คำอธิบายความสัมพันธ์
reference_createdate	varchar(15)	วันที่สร้างข้อมูล
reference_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.33 โครงสร้างตารางข้อมูลความต้องการของการออกแบบและใช้งานรหัสผ่าน

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
password_scope	text	ขอบเขตของการออกแบบและใช้งานรหัสผ่าน
password_factor	text	ปัจจัยที่มีผลต่อการกำหนดความต้องการของการออกแบบและใช้งานรหัสผ่าน
password_requirements	text	ความต้องการของการออกแบบและใช้งานรหัสผ่าน
password_createdate	varchar(15)	วันที่สร้างข้อมูล
password_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.34 โครงสร้างตารางข้อมูลการออกแบบและใช้งานรหัสผ่าน

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
design_composition	text	ลักษณะตัวอักษรที่จะใช้ในรหัสผ่าน
design_length	text	ความยาวของรหัสผ่าน
design_lifetime	text	อายุการใช้งานของรหัสผ่าน
design_source	text	ที่มาของรหัสผ่าน
design_ownership	text	บุคคลที่มีสิทธิในการใช้งานรหัสผ่าน
design_distribution	text	วิธีการในการส่งรหัสผ่านให้ผู้ใช้งาน
design_storage	text	วิธีการในการจัดเก็บรหัสผ่าน
design_entry	text	วิธีการในการกรอกรหัสผ่าน
design_transmission	text	วิธีการในการถ่ายโอนรหัสผ่านเพื่อใช้ในการทวนสอบ
design_authentication_period	text	ระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน
design_others	text	กำหนดการออกแบบและใช้งานรหัสผ่านอื่นๆ
design_createdate	varchar(15)	วันที่สร้างข้อมูล
design_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.35 โครงสร้างตารางข้อมูลการตรวจสอบข้อกำหนดกระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
review_id	varchar(10)	รหัสการตรวจสอบข้อกำหนดกระบวนการ
review_fault	text	ข้อผิดพลาดที่เกิดขึ้น
review_faultcause	text	สาเหตุของการเกิดข้อผิดพลาด
review_faultlevel	varchar(10)	ระดับของข้อผิดพลาด
review_faultaddress	text	ตำแหน่งของข้อผิดพลาด
review_faultdescription	text	คำอธิบายข้อผิดพลาด
review_faultfixing	text	การแก้ไขข้อผิดพลาด
review_createdate	varchar(15)	วันที่สร้างข้อมูล
review_createby	varchar(50)	ผู้สร้างข้อมูล
subphase_id	int (2)	รหัสขั้นตอนย่อย

ตารางที่ ง.36 โครงสร้างตารางข้อมูลการตรวจสอบข้อกำหนดกระบวนการเมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
reviewpolicy_id	varchar(10)	รหัสการตรวจสอบข้อกำหนดกระบวนการเมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ
reviewpolicy_fault	text	ข้อผิดพลาดที่เกิดขึ้นเมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ
reviewpolicy_faultcause	text	สาเหตุของการเกิดข้อผิดพลาด
reviewpolicy_faultlevel	varchar(10)	ระดับของข้อผิดพลาด
reviewpolicy_faultaddress	text	ตำแหน่งของข้อผิดพลาด
reviewpolicy_faultdescription_withpolicy	text	คำอธิบายข้อผิดพลาดเมื่อเทียบกับนโยบายและกลยุทธ์กระบวนการ
reviewpolicy_faultfixing	text	การแก้ไขข้อผิดพลาด
reviewpolicy_createdate	varchar(15)	วันที่สร้างข้อมูล
reviewpolicy_createby	varchar(50)	ผู้สร้างข้อมูล
subphase_id	int (2)	รหัสขั้นตอนย่อย

ตารางที่ ง.37 โครงสร้างตารางข้อมูลแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
systemplan_version	varchar(15)	เวอร์ชันแผนการพัฒนาระบบ
systemplan_systemname	varchar(255)	ชื่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
systemplan_systemversion	varchar(20)	เวอร์ชันระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
systemplan_objective	text	วัตถุประสงค์ของการพัฒนาระบบ
systemplan_scope	text	ขอบเขตของการพัฒนาระบบ
systemplan_methodology	text	ระเบียบวิธีการของการพัฒนาระบบ
systemplan_wbs	text	โครงสร้างของกิจกรรมที่เกิดขึ้นในการพัฒนาระบบ
systemplan_pbs	text	โครงสร้างของผลิตภัณฑ์ที่เกิดขึ้นในการพัฒนาระบบ

ตารางที่ ง.37 โครงสร้างตารางข้อมูลแผนการพัฒนาระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ (ต่อ)

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
systemplan_period	varchar(30)	ระยะเวลาของการพัฒนาระบบ
systemplan_milestone	text	เป้าหมายกิจกรรมของการพัฒนาระบบ
systemplan_tecnology	text	มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้
systemplan_responsibility	text	สมาชิกผู้รับผิดชอบและบทบาทหน้าที่
systemplan_budget	text	งบประมาณและทรัพยากรที่จำเป็นต้องใช้
systemplan_createdate	varchar(15)	วันที่สร้างข้อมูล
systemplan_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.38 โครงสร้างตารางข้อมูลการจัดการความเสี่ยงของการพัฒนาระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
risk_id	varchar(10)	รหัสความเสี่ยงของการพัฒนาระบบ
risk_type	varchar(20)	ประเภทความเสี่ยงของการพัฒนาระบบ
risk_detail	text	รายละเอียดความเสี่ยงของการพัฒนาระบบ
risk_description	text	คำอธิบายความเสี่ยงของการพัฒนาระบบ
risk_level	varchar(10)	ระดับของความเสี่ยงของการพัฒนาระบบ
risk_opportunitylevel	varchar(10)	ระดับโอกาสของการเกิดความเสี่ยงของการพัฒนาระบบ
risk_affectationlevel	varchar(10)	ระดับผลกระทบของความเสี่ยงเมื่อเกิดขึ้น
risk_method	varchar(30)	วิธีการจัดการความเสี่ยง
risk_management	text	การจัดการความเสี่ยง
risk_benefit	text	สิ่งที่ได้จากการจัดการความเสี่ยง
risk_budget	text	ต้นทุนสำหรับใช้ในการจัดการความเสี่ยง
risk_createdate	varchar(15)	วันที่สร้างข้อมูล
risk_createby	varchar(50)	ผู้สร้างข้อมูล
systemplan_version	varchar(15)	เวอร์ชันแผนการพัฒนาระบบ

ตารางที่ ง.39 โครงสร้างตารางข้อมูลความก้าวหน้าของการพัฒนาระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
progress_id	varchar(10)	รหัสความก้าวหน้าของการพัฒนาระบบ
progress_activity	text	กิจกรรมของการพัฒนาระบบ
progress_startdate	varchar(15)	วันที่เริ่มพัฒนากิจกรรม
progress_stopdate	varchar(15)	วันที่สิ้นสุดการพัฒนากิจกรรม
progress_undertaker	varchar(50)	ผู้รับผิดชอบการพัฒนากิจกรรม
progress_description	text	คำอธิบายเพิ่มเติมของการพัฒนากิจกรรม
additional_activity	text	กิจกรรมเสนอแนะเพิ่มเติม
additional_stratdate	varchar(15)	วันที่เริ่มพัฒนากิจกรรมเสนอแนะ
additional_stopdate	varchar(15)	วันที่สิ้นสุดการพัฒนากิจกรรมเสนอแนะ
additional_undertaker	varchar(50)	ผู้รับผิดชอบการพัฒนากิจกรรมเสนอแนะ
additional_description	text	คำอธิบายเพิ่มเติมของการพัฒนากิจกรรมเสนอแนะ
progress_createdate	varchar(15)	วันที่สร้างข้อมูล
progress_createby	varchar(50)	ผู้สร้างข้อมูล
systemplan_version	varchar(15)	เวอร์ชันแผนการพัฒนาระบบ

ตารางที่ ง.40 โครงสร้างตารางข้อมูลการเปลี่ยนแปลงของการพัฒนาระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
change_id	varchar(10)	รหัสการเปลี่ยนแปลงของการพัฒนาระบบ
change_activity	text	การเปลี่ยนแปลงของการพัฒนาระบบ
change_description	text	คำอธิบายการเปลี่ยนแปลงของการพัฒนาระบบ
change_reason	text	สาเหตุการเปลี่ยนแปลงของการพัฒนาระบบ
change_priority	varchar(10)	ระดับความสำคัญของการเปลี่ยนแปลงของการพัฒนาระบบ
change_impaction_withoutchange	text	ผลกระทบถ้าไม่ได้ทำการเปลี่ยนแปลง
change_impaction_requirements	text	ผลกระทบต่อความต้องการของโครงการ
change_impaction_objective	text	ผลกระทบต่อวัตถุประสงค์ของโครงการ
change_impaction_structure	text	ผลกระทบต่อโครงสร้างของโครงการ
change_impaction_deliver	text	ผลกระทบต่อการส่งมอบโครงการ

ตารางที่ ง.40 โครงสร้างตารางข้อมูลการเปลี่ยนแปลงของการพัฒนาระบบ (ต่อ)

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
change_impaction_risk	text	ผลกระทบต่อความเสี่ยงของโครงการ
change_impaction_schedule	text	ผลกระทบต่อกำหนดการของโครงการ
change_impaction_budget	text	ผลกระทบต่องบประมาณของโครงการ
change_recommendation	text	ข้อเสนอแนะเพิ่มเติม
change_approval	varchar(15)	ผลการอนุมัติ
change_approvalundertaker	varchar(50)	ผู้อนุมัติ
change_approvaldate	varchar(15)	วันที่อนุมัติ
change_approvalreason	text	เหตุผลของการตัดสินใจ
change_createdate	varchar(15)	วันที่สร้างข้อมูล
change_createby	varchar(50)	ผู้สร้างข้อมูล
risk_id	varchar(10)	รหัสความเสี่ยงของการพัฒนาระบบ

ตารางที่ ง.41 โครงสร้างตารางข้อมูลรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
checklist_id	varchar(10)	รหัสรายการตรวจสอบ
checklist_type	varchar(100)	ประเภทของรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ
checklist_subtype	varchar(100)	ประเภทย่อยของรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ
checklist_detail	text	รายละเอียดของรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ
checklist_status	char(1)	สถานะของรายการตรวจสอบความครบถ้วนของการพัฒนาระบบ
checklist_description	text	คำอธิบายของรายการตรวจสอบ
checklist_createdate	varchar(15)	วันที่สร้างข้อมูล
checklist_createby	varchar(50)	ผู้สร้างข้อมูล
systemplan_version	varchar(15)	เวอร์ชันแผนการพัฒนาระบบ

ตารางที่ ง.42 โครงสร้างตารางข้อมูลแผนการทดสอบระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
testplan_version	varchar(15)	เวอร์ชันแผนการทดสอบระบบ
testplan_systemname	varchar(255)	ชื่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
testplan_systemversion	varchar(20)	เวอร์ชันระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
testplan_objective	text	วัตถุประสงค์ของการทดสอบระบบ
testplan_scope	text	ขอบเขตของการทดสอบระบบ
testplan_methodology	text	ระเบียบวิธีที่ใช้ในการทดสอบระบบ
testplan_criteriatest	text	เกณฑ์ของการทดสอบ
testplan_acceptedlevel	text	ระดับของการยอมรับ
testplan_function_needtotest	text	ส่วนการทำงานที่ต้องการทดสอบ
testplan_testproduct	text	ผลิตภัณฑ์ที่ได้จากการทดสอบ
testplan_period	varchar(30)	ระยะเวลาของการทดสอบระบบ
testplan_milestone	text	เป้าหมายกิจกรรมของการทดสอบระบบ
testplan_tecnology	text	มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้
testplan_responsibility	text	สมาชิกผู้รับผิดชอบและบทบาทหน้าที่
testplan_budget	text	งบประมาณและทรัพยากรที่จำเป็นต้องใช้
testplan_createdate	varchar(15)	วันที่สร้างข้อมูล
testplan_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.43 โครงสร้างตารางข้อมูลผลการทดสอบระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
testresult_id	varchar(10)	รหัสผลการทดสอบระบบ
testresult_testinglevel	varchar(100)	ระดับของการทดสอบระบบ
testresult_RAGstatus	varchar(10)	สถานะ RAG ของการทดสอบระบบ
testresult_RAGdescription	text	คำอธิบายสถานะ RAG
testresult_qualityassurance	text	คำอธิบายคุณภาพของการทดสอบระบบ
testresult_successfully_testrequirements	varchar(10)	ความสำเร็จของการทดสอบตามความต้องการของระบบ

ตารางที่ ง.43 โครงสร้างตารางข้อมูลผลการทดสอบระบบ (ต่อ)

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
testresult_successfully_testfixed	varchar(10)	ความสำเร็จของการทดสอบตามข้อผิดพลาดที่กำหนดไว้
testresult_startdate	varchar(15)	วันที่เริ่มทดสอบระบบ
testresult_stopdate	varchar(15)	วันที่สิ้นสุดการทดสอบระบบ
testresult_createdate	varchar(15)	วันที่สร้างข้อมูล
testresult_createby	varchar(50)	ผู้สร้างข้อมูล
testplan_version	varchar(15)	เวอร์ชันแผนการทดสอบระบบ

ตารางที่ ง.44 โครงสร้างตารางข้อมูลบันทึกการทดสอบระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
testcase_id	varchar(10)	รหัสกรณีทดสอบ
testcase _detail	text	ชื่อการทดสอบ
testcase _function	text	ฟังก์ชันการทำงานที่ต้องการทดสอบ
testcase _testresult	char(1)	ผลของการทดสอบ
testcase _criticallevel	varchar(10)	ระดับความรุนแรงของข้อผิดพลาด
testcase _testdescription	text	คำอธิบายของการทดสอบ
testcase _createdate	varchar(15)	วันที่สร้างข้อมูล
testcase _createby	varchar(50)	ผู้สร้างข้อมูล
testresult_id	varchar(10)	รหัสผลการทดสอบระบบ

ตารางที่ ง.45 โครงสร้างตารางข้อมูลแผนการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
trainingplan_version	varchar(15)	เวอร์ชันแผนการอบรมผู้ใช้งาน/เจ้าหน้าที่และผู้ที่เกี่ยวข้อง
trainingplan_type	varchar(100)	ประเภทของแผนการอบรม
trainingplan_objective	text	วัตถุประสงค์ของการอบรม
trainingplan_scope	text	ขอบเขตของการอบรม
trainingplan_knowledge	text	เนื้อหาหรือองค์ความรู้ของการอบรม
trainingplan_agenda	text	กำหนดการอบรม

ตารางที่ ง.45 โครงสร้างตารางข้อมูลแผนการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง (ต่อ)

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
trainingplan_place	text	วันเวลาและสถานที่ของการจัดการอบรม
trainingplan_evaluation	text	เกณฑ์และระดับของการประเมินการอบรม
trainingplan_period	varchar(30)	ระยะเวลาของการอบรม
trainingplan_milestone	text	เป้าหมายกิจกรรมของการอบรม
trainingplan_technology	text	มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้
trainingplan_responsibility	text	สมาชิกผู้รับผิดชอบและบทบาทหน้าที่
trainingplan_budget	text	งบประมาณและทรัพยากรที่จำเป็นต้องใช้
trainingplan_createdate	varchar(15)	วันที่สร้างข้อมูล
trainingplan_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.46 โครงสร้างตารางข้อมูลผลการประเมินการอบรมผู้ใช้งาน/เจ้าหน้าที่ดำเนินการกระบวนการและผู้ที่เกี่ยวข้อง

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
trainingsum_id	int(3)	รหัสผลการประเมินการอบรม
trainingsum_result	text	ผลการประเมินการอบรม
trainingsum_summery	text	สรุปผลการประเมินการอบรม
trainingsum_limitation	text	ข้อจำกัดของการอบรม
trainingsum_suggestion	text	แนวทางการเสนอแนะและการแก้ไขปรับปรุงการอบรม
trainingsum_createdate	varchar(15)	วันที่สร้างข้อมูล
trainingsum_createby	varchar(50)	ผู้สร้างข้อมูล
trainingplan_version	varchar(15)	เวอร์ชันแผนการอบรมผู้ใช้งาน/เจ้าหน้าที่และผู้ที่เกี่ยวข้อง

ตารางที่ ง.47 โครงสร้างตารางข้อมูลแผนการเฝ้าสังเกตและทวนสอบระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ
monitoringplan_systemname	varchar(255)	ชื่อระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
monitoringplan_systemversion	varchar(20)	เวอร์ชันระบบการควบคุมการเข้าถึงสินทรัพย์ประเภทสารสนเทศ
monitoringplan_objective	text	วัตถุประสงค์ของการเฝ้าสังเกตและทวนสอบระบบ
monitoringplan_scope	text	ขอบเขตของการเฝ้าสังเกตและทวนสอบระบบ
monitoringplan_monitoringpart	text	ส่วนการทำงานที่ต้องการเฝ้าสังเกตและทวนสอบ
monitoringplan_measurementpart	text	ส่วนการทำงานที่ต้องการวัดประสิทธิภาพ
monitoringplan_howto_measure	text	วิธีการวัดประสิทธิภาพของระบบ
monitoringplan_period	varchar(30)	ระยะเวลาของการเฝ้าสังเกตและทวนสอบระบบ
monitoringplan_milestone	text	เป้าหมายกิจกรรมของเฝ้าสังเกตและทวนสอบระบบ
monitoringplan_technology	text	มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้
monitoringplan_responsibility	text	สมาชิกผู้รับผิดชอบและบทบาทหน้าที่
monitoringplan_budget	text	งบประมาณและทรัพยากรที่จำเป็นต้องใช้
monitoringplan_createdate	varchar(15)	วันที่สร้างข้อมูล
monitoringplan_createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.48 โครงสร้างตารางข้อมูลผลการเฝ้าสังเกตและทวนสอบระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
monitoring_id	varchar(10)	รหัสผลการเฝ้าสังเกตและทวนสอบระบบ
monitoring_part	text	ส่วนการทำงานที่ต้องการเฝ้าสังเกตและทวนสอบ
monitoring_data	text	ข้อมูลที่ต้องการเฝ้าสังเกตและทวนสอบ
monitoring_result	text	ผลของการเฝ้าสังเกตและทวนสอบระบบ
monitoring_summery	text	สรุปผลการเฝ้าสังเกตและทวนสอบระบบ
monitoring_startdate	varchar(15)	วันที่เริ่มการเฝ้าสังเกตและทวนสอบระบบ
monitoring_stopdate	varchar(15)	วันที่สิ้นสุดการเฝ้าสังเกตและทวนสอบระบบ
monitoring_createdate	varchar(15)	วันที่สร้างข้อมูล
monitoring_createby	varchar(50)	ผู้สร้างข้อมูล
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ

ตารางที่ ง.49 โครงสร้างตารางข้อมูลผลการวัดประสิทธิภาพของระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
measure_id	varchar(10)	รหัสผลการวัดประสิทธิภาพของระบบ
measure_part	text	ส่วนการทำงานที่ต้องการวัดประสิทธิภาพ
measure_data	text	ข้อมูลที่ต้องการวัดประสิทธิภาพ
measure_result	text	ผลของการวัดประสิทธิภาพของระบบ
measure_baselineanalysis	text	การวิเคราะห์เมื่อเทียบกับค่าคาดหมาย
measure_acceptedlevel	varchar(10)	ระดับของการยอมรับ
measure_summery	text	สรุปผลการวัดประสิทธิภาพของระบบ
measure_startdate	varchar(15)	วันที่เริ่มการวัดประสิทธิภาพของระบบ
measure_stopdate	varchar(15)	วันที่สิ้นสุดการวัดประสิทธิภาพของระบบ
measure_createdate	varchar(15)	วันที่สร้างข้อมูล
measure_createby	varchar(50)	ผู้สร้างข้อมูล
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ

ตารางที่ ง.50 โครงสร้างตารางข้อมูลความสัมพันธ์ระหว่างข้อมูลการเฝ้าสังเกตและทวนสอบระบบและข้อมูลการวัดประสิทธิภาพของระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
monitormeasure_id	int(5)	รหัสความสัมพันธ์ระหว่างข้อมูลการเฝ้าสังเกตและทวนสอบระบบและข้อมูลการวัดประสิทธิภาพของระบบ
monitoring_id	varchar(10)	รหัสผลการเฝ้าสังเกตและทวนสอบระบบ
measure_id	varchar(10)	รหัสผลการวัดประสิทธิภาพของระบบ
description	text	คำอธิบายความสัมพันธ์
createdate	varchar(15)	วันที่สร้างข้อมูล
createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.51 โครงสร้างตารางข้อมูลตัวชี้วัดประสิทธิภาพของระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
matric_id	varchar(10)	รหัสตัวชี้วัดประสิทธิภาพของระบบ
matric_type	varchar(100)	ประเภทของตัวชี้วัดประสิทธิภาพของระบบ
matric_name	text	ชื่อตัวชี้วัดประสิทธิภาพของระบบ
matric_description	text	คำอธิบายตัวชี้วัดประสิทธิภาพของระบบ
matric_baseline	text	ค่าคาดหมายของตัวชี้วัดประสิทธิภาพของระบบ
matric_createdate	varchar(15)	วันที่สร้างข้อมูล
matric_createby	varchar(50)	ผู้สร้างข้อมูล
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ

ตารางที่ ง.52 โครงสร้างตารางข้อมูลความสัมพันธ์ระหว่างการวัดประสิทธิภาพของระบบและตัวชี้วัด

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
measurematric_id	int(5)	รหัสความสัมพันธ์ระหว่างการวัดประสิทธิภาพของระบบและตัวชี้วัด
measure_id	varchar(10)	รหัสผลการวัดประสิทธิภาพของระบบ
matric_id	varchar(10)	รหัสตัวชี้วัดประสิทธิภาพของระบบ
description	text	คำอธิบายความสัมพันธ์
createdate	varchar(15)	วันที่สร้างข้อมูล
createby	varchar(50)	ผู้สร้างข้อมูล

ตารางที่ ง.53 โครงสร้างตารางข้อมูลผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
changing_id	int(3)	รหัสผลการปรับแผนการเฝ้าสังเกตและทวนสอบระบบ
changing_topic	varchar(255)	หัวข้อที่ต้องการปรับเปลี่ยน
changing_detail	text	รายละเอียดของการปรับแผนการเฝ้าสังเกตและทวนสอบระบบ
changing_createdate	varchar(15)	วันที่สร้างข้อมูล
changing_cretateby	varchar(50)	ผู้สร้างข้อมูล
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ

ตารางที่ ง.54 โครงสร้างตารางข้อมูลการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
actionevent_id	varchar(10)	รหัสการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
actionevent_type	varchar(50)	ประเภทของการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
actionevent_detail	text	รายละเอียดการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
actionevent_description	text	คำอธิบายการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
actionevent_criticallevel	varchar(10)	ระดับความรุนแรง
actionevent_effectiveimpaction	text	ผลกระทบต่อประสิทธิภาพของระบบ
actionevent_createdate	varchar(15)	วันที่สร้างข้อมูล
actionevent_createby	varchar(50)	ผู้สร้างข้อมูล
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ

ตารางที่ ง.55 โครงสร้างตารางข้อมูลแผนการปรับปรุงระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
improvementplan_version	varchar(15)	เวอร์ชันแผนการปรับปรุงระบบ
improvementplan_objective	text	วัตถุประสงค์ของการปรับปรุงระบบ
improvementplan_scope	text	ขอบเขตของการปรับปรุงระบบ
improvementplan_improvement	text	วิธีการปรับปรุง
improvementplan_improvementpart	text	ส่วนการทำงานใดๆ ที่ต้องการทำการปรับปรุง
improvementplan_period	varchar(30)	ระยะเวลาของการปรับปรุงระบบ
improvementplan_milestone	text	เป้าหมายกิจกรรมของการปรับปรุงระบบ
improvementplan_technology	text	มาตรฐานที่เกี่ยวข้องและเทคโนโลยีที่นำมาใช้
improvementplan_responsibility	text	สมาชิกผู้รับผิดชอบและบทบาทหน้าที่
improvementplan_budget	text	งบประมาณและทรัพยากรที่จำเป็นต้องใช้
improvementplan_createdate	varchar(15)	วันที่สร้างข้อมูล
improvementplan_createby	varchar(50)	ผู้สร้างข้อมูล
monitoringplan_version	varchar(15)	เวอร์ชันแผนเฝ้าสังเกตและทวนสอบระบบ

ตารางที่ ง.56 โครงสร้างตารางข้อมูลผลการวิเคราะห์การยอมรับของการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
accepted_id	int(3)	รหัสผลการวิเคราะห์การยอมรับของการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
accepted_effectivereason	text	สาเหตุที่การกระทำหรือเหตุการณ์นั้นส่งผลกระทบต่อประสิทธิภาพของระบบ
accepted_level	varchar(10)	ระดับของการยอมรับ
accepted_analysis	text	การวิเคราะห์ผลการยอมรับ
accepted_createdate	varchar(15)	วันที่สร้างข้อมูล
accepted_createby	varchar(50)	ผู้สร้างข้อมูล
improvementplan_version	varchar(15)	เวอร์ชันแผนการปรับปรุงระบบ
actionevent_id	varchar(10)	รหัสการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ

ตารางที่ ง.57 โครงสร้างตารางข้อมูลการกระทำและการป้องกันสำหรับการปรับปรุงระบบ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
correctivepreventive_id	varchar(10)	รหัสการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
correctivepreventive_type	varchar(50)	ประเภทของการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
correctivepreventive_detail	text	รายละเอียดของการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
correctivepreventive_priority	varchar(10)	ระดับความสำคัญ
correctivepreventive_part	text	ส่วนการทำงานที่ต้องการปรับปรุงแก้ไข
correctivepreventive_startdate	varchar(15)	วันที่เริ่มการปรับปรุงแก้ไข
correctivepreventive_stopdate	varchar(15)	วันที่สิ้นสุดการปรับปรุงแก้ไข
correctivepreventive_budget	text	งบประมาณที่จำเป็นต้องใช้สำหรับการปรับปรุงแก้ไข
correctivepreventive_createdate	varchar(15)	วันที่สร้างข้อมูล
correctivepreventive_createby	varchar(50)	ผู้สร้างข้อมูล
accepted_id	int(3)	รหัสผลการวิเคราะห์การยอมรับของการกระทำและเหตุการณ์ที่ส่งผลกระทบต่อประสิทธิภาพของระบบ

ตารางที่ ง.58 โครงสร้างตารางข้อมูลข้อเสนอแนะต่อการกระทำและการป้องกันสำหรับการปรับปรุงระบบของผู้ที่เกี่ยวข้องกับกระบวนการ

ชื่อสดมภ์	ประเภทข้อมูล	คำอธิบาย
suggestion_id	int(3)	รหัสข้อเสนอแนะต่อการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
suggestion_objective	text	วัตถุประสงค์ของการเสนอแนะต่อการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
suggestion_priority	varchar(10)	ระดับความสำคัญ
suggestion_detail	text	รายละเอียดของข้อเสนอแนะต่อการกระทำและการป้องกันสำหรับการปรับปรุงระบบ
suggestion_createdate	varchar(15)	วันที่สร้างข้อมูล
suggestion_createby	varchar(50)	ผู้สร้างข้อมูล
correctivepreventive_id	varchar(10)	รหัสการกระทำและการป้องกัน

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวเมธยา ราชคมน์ เกิดเมื่อวันที่ 30 มกราคม พ.ศ. 2528 สำเร็จการศึกษาระดับปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ จากคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร ในปีการศึกษา 2549 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2550

ขณะที่ศึกษานั้น ผู้วิจัยได้ร่วมทำบทความกับอาจารย์ที่ปรึกษา ซึ่งมีบทความที่ได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงานประชุมวิชาการทั้งระดับชาติและนานาชาติ รวมทั้งสิ้น 2 บทความ โดยมีรายละเอียดดังต่อไปนี้

1) บทความวิชาการเรื่อง “การออกแบบกระบวนการการควบคุมการเข้าถึงสินทรัพย์สารสนเทศโดยใช้แบบรูปความมั่นคง (A Design of Process Model for Information Assets Access Control using Security Patterns)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทางวิทยาศาสตร์และวิศวกรรมคอมพิวเตอร์ระดับชาติ ครั้งที่ 13 (The13th National Computer Science and Engineering Conference: NCSEC 2009)” ระหว่างวันที่ 4 - 6 พฤศจิกายน 2552 ณ โรงแรม มนเฑียร ริเวอร์ไซต์ กรุงเทพฯ ประเทศไทย

2) บทความวิชาการเรื่อง “A Process Model Design and Tool Support for Information Assets Access Control using Security Patterns” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการร่วมสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมซอฟต์แวร์ ครั้งที่ 8 (The 8th International Joint Conference on Computer Science and Software Engineering: JCSSE 2011)” ระหว่างวันที่ 11 - 13 พฤษภาคม 2554 ณ คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล วิทยาเขตศาลายา นครปฐม ประเทศไทย