บทที่ 3
การออกแบบขั้นตอนการดำเนินงาน

งานวิจัยนี้มีแนวคิดที่จะนำเสนอขั้นตอนวิธีการดำเนินงานของกระบวนการตรวจสอบการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ชัดเจน เพื่อเป็นแนวทางให้ผู้ตรวจสอบปฏิบัติตามได้โดยง่าย รวมถึงออกแบบและพัฒนาระบบเพื่อช่วยอำนวยความสะดวกให้กับผู้ตรวจสอบในการดำเนินการตรวจสอบศูนย์สารสนเทศของธนาคารโดยอ้างอิงจากกรอบงานโคบิต ซึ่งระบบที่พัฒนาขึ้นจะมีฟังก์ชันการทำงานดังต่อไปนี้

3.1 **การวางแผนการตรวจสอบประจำปี** (Project Planning)

เนื่องจากธนาคารแห่งประเทศไทยจะมีการออกกฎระเบียบให้กับธนาคารพาณิชย์ทุกแห่งว่าอย่างน้อยในแต่ละปีธนาคารควรจะทำการตรวจสอบเกี่ยวกับเรื่องใดบ้าง ดังนั้นระบบจะช่วยอำนวยความสะดวกให้กับผู้ตรวจสอบโดยจะมีการให้คะแนนกับศูนย์สารสนเทศต่าง ๆ ทั้งหมด ซึ่งจะให้คะแนนกับศูนย์สารสนเทศที่เกี่ยวข้องกับเรื่องที่ธนาคารแห่งประเทศไทยกำหนดมากกว่าศูนย์สารสนเทศที่ไม่เกี่ยวข้อง โดยอาจจะมีปัจจัยอื่น ที่เป็นตัวกำหนดคะแนนของแต่ละศูนย์สารสนเทศร่วมด้วย เช่น ใช้ข้อมูลจากประวัติการตรวจสอบโดยดูความถี่ของการตรวจสอบ ถ้าศูนย์สารสนเทศใดที่มีความถี่น้อยก็จะให้คะแนนมากกว่าศูนย์สารสนเทศที่มีความถี่มาก (เพราะมีแนวโน้มที่การควบคุมจะไม่มีประสิทธิภาพที่ดีเพียงพอ) หรือ ศูนย์สารสนเทศใดที่ถือว่าเป็นระบบงานหลักของธนาคาร (Core System) ก็จะมีคะแนนที่มากกว่าศูนย์สารสนเทศที่ไม่ใช่ระบบงานหลัก เป็นต้น

ระบบจะนำเสนอข้อมูลในรูปแบบของตารางอันดับพร้อมทั้งมีการประมาณระยะเวลาที่จะต้องใช้ในการตรวจสอบแต่ละศูนย์ด้วย (คำนวณโดยใช้ข้อมูลสถิติเดิมจากประวัติการตรวจสอบที่ผ่านมา)

3.2 **การประเมินความเสี่ยง** (Risk Assessment)

ในขั้นตอนของการประเมินความเสี่ยงนั้นมีปัจจัยที่ใช้ในการประเมินความเสี่ยงอยู่ 2 ส่วนด้วยกันคือ

ปัจจัยที่หนึ่ง **ผลกระทบทางธุรกิจ** (Business Impact) หมายถึง มูลค่าของความเสียหายที่เกิดขึ้นของแต่ละเหตุการณ์ที่เกิด โดยวิเคราะห์จากองค์ประกอบหลาย ๆ ด้าน เช่น ตามปริมาณความเสียหาย ตามระยะเวลาในการแก้ไข หรือตามปริมาณของจำนวนลูกค้า เป็นต้น

ปัจจัยที่สอง **โอกาสเกิด** (Likelihood) หมายถึง ความเป็นไปได้ที่จะเกิดเหตุการณ์นั้น ๆ ซึ่งโอกาสเกิดจะมีมากหรือน้อยเพียงใดต้องพิจารณาจากการควบคุมเป็นหลัก กล่าวคือ หากมีการควบคุมที่ดีโอกาสที่จะเกิดเหตุการณ์ที่จะสร้างความเสียหายก็ย่อมน้อยลง

ระบบจะช่วยอำนวยความสะดวกให้กับผู้ใช้งานโดยจะจัดเตรียมโครงร่าง (Template) ที่ใช้สำหรับคำนวณคะแนนของการประเมินความเสี่ยง ซึ่งมีหลักในการคำนวณ 2 รูปแบบเพื่อให้ผู้ใช้งานสามารถเลือกใช้ได้ตามความเหมาะสม ดังนี้

รูปแบบที่ 1 การประเมินความเสี่ยงแบบทั่วไป ซึ่งมีหลักในการคำนวนดังนี้

(ผลกระทบ x โอกาสเกิด) - การควบคุมที่มีอยู่

รูปแบบที่ 2 การประเมินความเสี่ยงแบบถ่วงน้ำหนัก ซึ่งมีหลักในการคำนวณดังนี้

((ผลกระทบ x โอกาสเกิด) - การควบคุมที่มีอยู่) x น้ำหนัก

คะแนนต่างๆเหล่านี้ผู้ใช้งานจะเป็นผู้ใส่ข้อมูลเข้าทั้งหมดแล้วระบบจะทำการคำนวนออกมาเป็นคะแนนให้พร้อมทั้งทำการจัดเรียงอันดับตามหัวข้อการควบคุมที่มีคะแนนสูงที่สุดถึงหัวข้อการควบคุมที่มีคะแนนต่ำที่สุด ซึ่งผู้ใช้งานสามารถเลือกหัวข้อการควบคุมที่จะใช้ในการตรวจสอบของแต่ละศูนย์สารสนเทศได้เองตามที่ต้องการ

3.3 การจัดการเอกสารที่ใช้ในการตรวจสอบ (Audit Document Management)

เป็นการอำนวยความสะดวกให้กับผู้ใช้งานในด้านของเอกสาร โดยเอกสารการตรวจสอบที่ระบบมีการจัดเตรียมไว้ให้ได้แก่ โปรแกรมการตรวจสอบ (Audit Program) รายการของเอกสารที่ต้องใช้ในการตรวจสอบ (Request Document) และข้อแนะนำในการตรวจสอบ (Audit Guideline) ของทุก ๆ หัวข้อการควบคุม (โดยข้อมูลที่ปรากฏอยู่ในเอกสารต่าง ๆ จะอ้างอิงมาจากข้อมูลของการตรวจสอบปีล่าสุด) ซึ่งระบบจะทำหน้าที่เป็นตัวควบคุมการเรียกใช้งานเอกสารการตรวจสอบดังกล่าว ดังนั้นผู้ตรวจสอบจะสามารถเข้าถึงและแก้ไขได้เฉพาะหัวข้อการควบคุมที่ตนได้รับมอบหมายเท่านั้น

3.4 ประวัติการตรวจสอบของศูนย์สารสนเทศ (Audit History)

ระบบจะช่วยอำนวยความสะดวกให้กับผู้ตรวจสอบในส่วนของการเรียกดูประวัติของการตรวจสอบของปีที่ผ่าน ๆ มา โดยระบบจะสร้างให้อยู่ในรูปแบบของแผนภูมิต้นไม้ (Tree view) โดยเมื่อผู้ใช้เลือกปีที่ต้องการจะปรากฏรายละเอียดของปีนั้น ๆ ว่ามีการตรวจสอบศูนย์สารสนเทศใดบ้าง และเมื่อทำการเลือกศูนย์สารสนเทศที่ต้องการแล้วจะปรากฏหัวข้อการควบคุมทั้งหมดที่ใช้

ตรวจในปีนั้น ๆ เมื่อทำการเลือกหัวข้อการตรวจสอบที่ต้องการแล้วระบบจะแสดง เกณฑ์ที่ใช้ในการตรวจสอบ รายการเอกสารที่ต้องใช้ในการตรวจสอบ ข้อแนะนำในการตรวจสอบ

3.5 **การจัดการประเด็นปัญหา** (Issue Management)

ระบบจะทำการจัดเก็บประเด็นปัญหา (Issue) ต่าง ๆ ที่ผู้ตรวจสอบทำการตรวจพบ โดยจะทำการแบ่งตามศูนย์สารสนเทศที่ทำการตรวจสอบ เพื่อทำหน้าที่ในการคอยตรวจสอบติดตามการแก้ไขประเด็นปัญหาของฝ่ายงานที่เกี่ยวข้อง ว่าได้มีการแก้ไขตามที่ผู้ตรวจสอบแนะนำไปครบถ้วนหรือไม่ โดยระบบจะทำการจัดเก็บรายละเอียดต่าง ๆ ดังนี้ เป็นประเด็นเรื่องอะไร ของศูนย์สารสนเทศใด วันที่ตรวจพบ ระดับความรุนแรง ผู้รับผิดชอบในการสั่งการ (Issue Owner) ผู้รับผิดชอบในการดำเนินการ (Action Owner) และ กำหนดการในการแก้ไข (Target Date) เป็นต้น

ผู้รับผิดชอบในการสั่งการ หมายถึง ประธานคณะเจ้าหน้าที่ซึ่งเป็นผู้บริหารสูงสุดในสายงาน ถือเป็นผู้รับผิดชอบหลักในการกำหนดนโยบาย แนวทางแก้ไข รวมถึงการสั่งการและมอบหมายให้ **ผู้รับผิดชอบในการดำเนินการ** ทำการแก้ไขปรับปรุงประเด็นดังกล่าว เพื่อให้องค์กรสามารถทำงานได้อย่างมีประสิทธิภาพ

การทำงานนี้จะช่วยอำนวยความสะดวกให้กับผู้ตรวจสอบได้โดยผู้ตรวจสอบสามารถเข้ามาเรียกดูรายการของประเด็นปัญหา (ทั้งที่แก้ไขเสร็จแล้วและที่ยังไม่ได้ดำเนินการ) หรือ แก้ไขข้อมูลเมื่อฝ่ายงานที่เกี่ยวข้องได้ดำเนินการแก้ไขเรียบร้อยแล้ว เพื่อให้ผู้ตรวจสอบสามารถมั่นใจได้ว่าประเด็นปัญหาต่าง ๆ ที่ตรวจสอบพบจะถูกดำเนินการแก้ไขได้หมดโดยไม่ตกหล่น

3.6 **การระบุความเสี่ยง** (Risk Database)

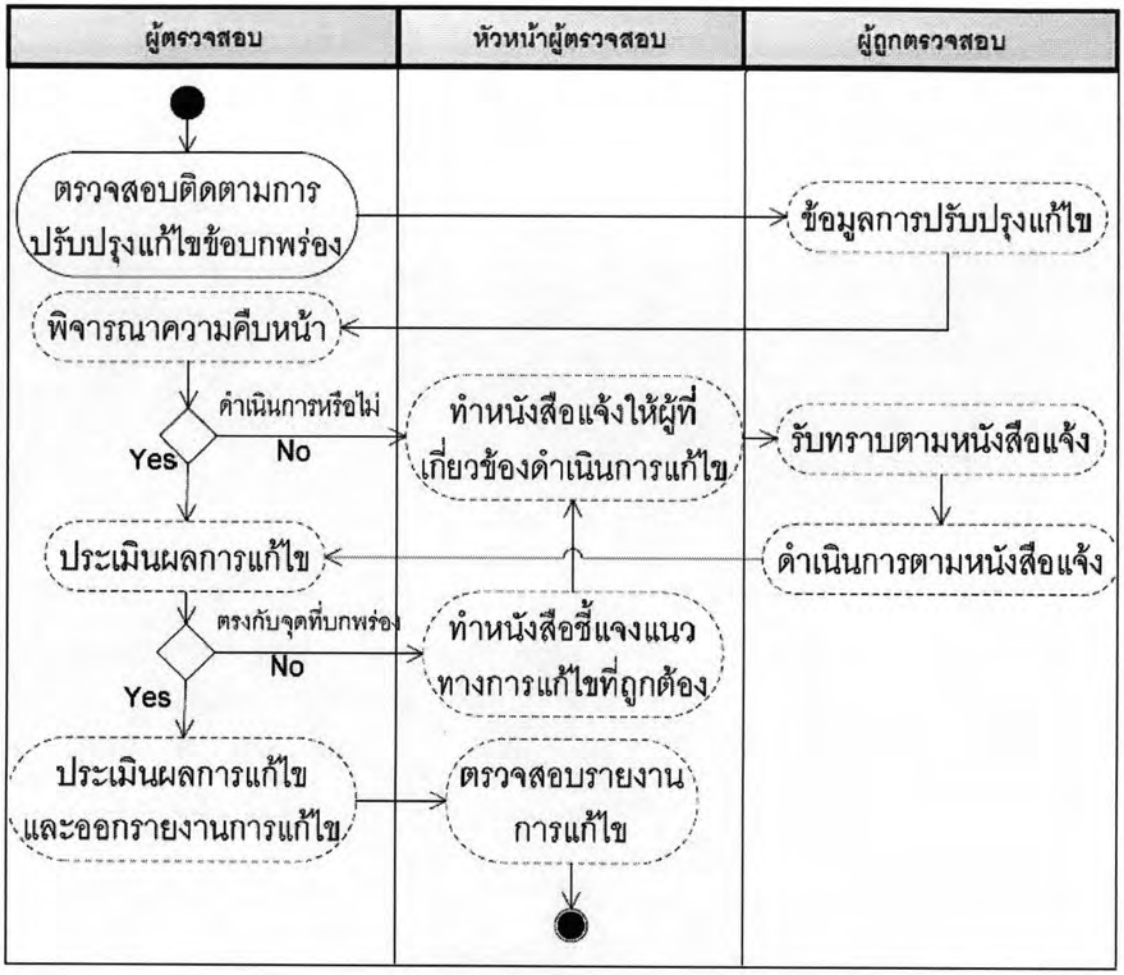
ระบบสามารถทำการจัดเก็บข้อมูลของความเสี่ยงต่าง ๆ ที่สามารถเกิดขึ้นได้ภายในองค์กร โดยระบบจะจัดเก็บรายละเอียดของความเสี่ยงต่าง ๆ ไว้ ซึ่งประกอบด้วยรายละเอียดดังต่อไปนี้ ชื่อความเสี่ยง คำอธิบายโดยละเอียดของความเสี่ยง ส่งผลกระทบต่อผู้ที่มีส่วนเกี่ยวข้อง (Stakeholder) ใดบ้าง ส่งผลกระทบต่อเป้าหมายของผู้ที่มีส่วนเกี่ยวข้องส่วนใดบ้าง ก่อให้เกิดความเสียหายแก่องค์กรอย่างไรบ้าง และ มีวิธีป้องกันหรือควบคุมได้อย่างไร

รูปแบบในการนำเสนอข้อมูลความเสี่ยงนี้ระบบจะนำเสนอในรูปแบบของตารางที่มีความสัมพันธ์เชื่อม ต่อกัน โดยจะนำทฤษฎีของ Riskit Method มาประยุกต์ใช้ เพื่อแสดงให้ผู้ตรวจสอบเห็นและเข้าใจถึงรายละเอียดและความสัมพันธ์กันของข้อมูลต่างได้โดยง่าย โดยแสดงเป็นแผนภาพ ทั้งนี้ผู้ตรวจสอบสามารถทำการค้นถาม (Query) สร้าง (Create) แก้ไข (Modify) และลบ (Delete) ข้อมูลความเสี่ยงต่าง ๆ ได้ เพื่อให้ข้อมูลดังกล่าวมีความถูกต้องครบถ้วนและสามารถนำไปใช้ประโยชน์ในการตรวจสอบได้

จากการศึกษากระบวนการตรวจสอบการควบคุมภายด้านเทคโนโลยีสารสนเทศ ผู้วิจัยได้ทำการสรุปและออกแบบขั้นตอนการดำเนินงานของกระบวนการตรวจสอบการควบคุมภายใน ดังรูปที่ 4 โดยขั้นตอนการดำเนินงานนี้จะแสดงการไหลของข้อมูลและกระบวนการทำงานอย่างเป็นลำดับขั้นตอน พร้อมทั้งยังระบุหน้าที่หรือการกระทำต่าง ๆ ของผู้ที่เกี่ยวข้องทั้งหมดอย่างชัดเจน และยังสามารถแสดงถึงเอกสารหรือข้อมูลต่าง ๆ ที่ถูกสร้างขึ้นจากขั้นตอนการทำงานดังกล่าว (แทนด้วยสัญลักษณ์สี่เหลี่ยม)

นอกจากขั้นตอนการดำเนินการหลักของกระบวนการตรวจสอบที่ได้กล่าวไว้ข้างต้นแล้ว งานวิจัยนี้ยังได้นำเสนอกระบวนการที่ใช้ในการตรวจสอบและติดตามการปรับปรุงแก้ไขประเด็นปัญหา (Issue) ที่ตรวจพบ อีกกระบวนการหนึ่งดังรูปที่ 5 เพื่อเป็นเครื่องมือที่ผู้ตรวจสอบใช้ในการติดตามประเด็นปัญหาที่ตรวจพบ ว่าผู้ที่รับผิดชอบในการแก้ไขได้ดำเนินการแก้ไขแล้วหรือไม่

รูปที่ 4 แผนภาพกิจกรรมของกระบวนการตรวจสอบการควบคุมภายใน



รูปที่ 5 แผนภาพกิจกรรมการตรวจสอบติดตามการแก้ไขข้อบกพร่อง