บทที่ 5

บทสรุป

การวิจัยครั้งนี้เป็นการศึกษาข้อมูล และกระบวนการที่เกี่ยวข้องในการประเมินความเสี่ยงของหน่วยงานรัฐวิสาหกิจ เพื่อนำมาพัฒนาเป็นระบบสารสนเทศต้นแบบเพื่อสนับสนุนการบริหารข้อมูลเพื่อการประเมินความเสี่ยงของหน่วยงานรัฐวิสาหกิจ โดยผลการวิจัย และข้อเสนอแนะสามารถสรุปดังหัวข้อถัดไป

สรุปผลการวิจัย

ผู้วิจัยได้ทำการศึกษาข้อมูล และกระบวนการประเมินความเสี่ยงด้านสารสนเทศรวมทั้งกรรมวิธีมาตรฐานต่าง ๆ ที่นำมาใช้ในกระบวนการประเมินความเสี่ยง ซึ่งการวิจัยที่ได้จากวิเคราะห์สามารถสรุปได้ดังนี้

1. การศึกษากระบวนการประเมินความเสี่ยง ด้านสารสนเทศในปัจจุบัน ของหน่วยงานรัฐวิสาหกิจ

จากการศึกษา และวิเคราะห์กระบวนการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจ พบว่าหน่วยงานรัฐวิสาหกิจมีการประเมินความเสี่ยงด้านสารสนเทศ โดยยึดตามหลักเกณฑ์การประเมินการบริหารความเสี่ยง TRIS เป็นหลัก ซึ่ง TRIS ได้มีการเพิ่มเติมหลักเกณฑ์การประเมินการบริหารความเสี่ยง เพื่อให้ครอบคลุมตามพระราชกฤษฎีกา และพระราชบัญญัติ ต่าง ๆ โดยการประเมินประจำปีบัญชี 2550 และ 2551 ได้มีการกำหนดค่าเกณฑ์วัดโดยใช้การดำเนินงานตามมาตรฐาน ISO/IEC 27001:2005 ซึ่งผลลัพธ์ หรือระดับคะแนนที่ได้จากการประเมินถือเป็นหนึ่งในตัวชี้วัดการดำเนินงานของหน่วยงานรัฐวิสาหกิจ

ในการบริหารความเสี่ยงนั้น ขั้นตอนแรกจะต้องมีการประเมินความเสี่ยงและเมื่อทำการศึกษากระบวนการประเมินความเสี่ยงในปัจจุบันของหน่วยงาน ทำให้ทราบถึงปัญหาต่าง ๆ ต่อการใช้ข้อมูลการประเมินความเสี่ยงต่าง ๆ ในการจัดทำรายงานบริหารความเสี่ยงเพื่อใช้ในการประเมินของ TRIS โดยปัญหาอันเนื่องมาจากการที่ไม่มีการบริหารจัดการข้อมูลการประเมินความเสี่ยงที่เป็นระบบ รวมทั้งการที่ไม่มีการจัดเก็บข้อมูลเหตุการณ์ความเสี่ยงต่าง ๆ ที่เกิดขึ้นต่อสารสนเทศ

การพัฒนาระบบสารสนเทศ ผู้วิจัยได้ทำการศึกษาวิธีการประเมินความเสี่ยงเพื่อพัฒนาระบบสารสนเทศเพื่อสนับสนุนการประเมินความเสี่ยงสารสนเทศหน่วยงานรัฐวิสาหกิจ โดยใช้แนวทางของการประเมินความเสี่ยงของ National Institute of Standards and Technology (NIST SP 800-30) ซึ่งเป็นมาตรฐานในการจัดการความเสี่ยง (Risk Management Standards)

2. วิเคราะห์และออกแบบระบบ ผู้วิจัยได้จัดทำการออกแบบระบบงาน โดยใช้แผนภาพกระแสข้อมูล (Data Flow Diagram) เป็นเครื่องมือในการออกแบบระบบงาน เพื่อให้เห็นภาพรวมของระบบทั้งข้อมูลและขั้นตอนการทำงาน และแผนภาพความสัมพันธ์ระหว่างข้อมูล (Entity Relationship Diagram) ในการออกแบบระบบฐานข้อมูลที่มีการใช้งานของระบบ

3. การพัฒนาระบบสารสนเทศ ซึ่งใช้ภาษา Visual Basic โดยใช้การเชื่อมต่อระบบฐานข้อมูล Access ซึ่งได้แบ่งส่วนการใช้งานต่าง ๆ ดังนี้คือ

3.1 ส่วนผู้ใช้ที่มีสิทธิในฐานะผู้ดูแลระบบ

3.2 ส่วนผู้ใช้ที่มีสิทธิในฐานะเจ้าหน้าที่

3.3 ส่วนผู้ใช้ที่มีสิทธิในฐานะผู้บริหาร

3.4 ส่วนผู้ใช้ที่มีสิทธิในฐานะเรียกดูรายงาน

อภิปรายผล

1. จากการศึกษากระบวนการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจที่ผู้วิจัยได้ทำการศึกษานั้น พบว่าหน่วยงานรัฐวิสาหกิจมีการประเมินความเสี่ยงด้านสารสนเทศโดยยึดตามหลักเกณฑ์การประเมินการบริหารความเสี่ยง TRIS เป็นหลัก ซึ่งผลลัพธ์หรือระดับคะแนนที่ได้จากการประเมินของ TRIS ถือเป็นหนึ่งในตัวชี้วัดการดำเนินงานของหน่วยงานรัฐวิสาหกิจ ซึ่งในปัจจุบันกระบวนการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานข้างต้น ยังไม่มีระบบสารสนเทศเข้ามาช่วยในการประเมิน ซึ่งใช้การกรอกข้อมูลลงเอกสารแบบสอบถาม หรือแบบฟอร์มตามที่หน่วยงานกำหนดขึ้นมา ทำให้การจัดเก็บและการค้นหาข้อมูลที่ต้องการต่าง ๆ ทำได้ลำบากและไม่สะดวกรวดเร็ว ซึ่งจะส่งผลต่อระยะเวลาการจัดทำรายงานการประเมินความเสี่ยงที่ต้องใช้เวลานานขึ้น นอกจากนั้นหน่วยงานหากหน่วยงานมีการขยายตัวในอนาคตจะส่งผลต่อความต้องการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มากขึ้น ทำให้จำนวนสินทรัพย์ขององค์กรที่เยอะขึ้น ด้วยเหตุผลดังกล่าวหากไม่มีการบริหารจัดการข้อมูลและระบบสารสนเทศเพื่อสนับสนุนการทำงานของเจ้าหน้าที่อาจจะส่งผลต่อการดำเนินงานที่ล่าช้า และไม่ทันต่อความต้องการในการใช้ข้อมูลต่าง ๆ

2. ผลจากการศึกษาขั้นตอนของการประเมินความเสี่ยง ซึ่งหน่วยงานรัฐวิสาหกิจที่ผู้วิจัยได้ทำการศึกษานั้น มีการนำขั้นตอนในการประเมินความเสี่ยงตามมาตรฐาน NIST SP 800-30 มาใช้เป็นแนวทางปฏิบัติ ซึ่งมาตรฐาน NIST SP 800-30 นั้นจะเน้นเรื่องการบ่งชี้ภัยคุกคาม และช่องโหว่ (Threat and Vulnerability Identification) การตรวจสอบความเป็นไปได้ในการเกิดภัยคุกคาม (Likelihood Determination) การวิเคราะห์ผลกระทบ (Impact Analysis) และการเสนอวิธีการควบคุม (Control Recommendation) ซึ่งหมายความว่าต้องกำหนด ภัยคุกคามและช่องโหว่ของระบบให้ได้เสียก่อน จากนั้นจึงดูความเป็นไปได้ในการเกิดภัยคุกคาม ประกอบกับผลกระทบจากความเสี่ยงดังกล่าว ตลอดจนถึงวิธีการแก้ไขปัญหาของความเสี่ยงในรูปแบบต่าง ๆ ซึ่งในหน่วยงานรัฐวิสาหกิจแห่งนี้ได้นำเอามาตรฐานการควบคุม 11 หมวด (Annex A) ภายใต้มาตรฐาน ISO27001:2005 มาใช้เป็นวิธีการควบคุม และจากการนำขั้นตอนตามมาตรฐาน NIST SP 800-30 ดังกล่าวมาใช้พบว่าขั้นตอนตามมาตรฐาน NIST SP 800-30 สามารถนำมาปรับใช้ได้จริงกับการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจดังกล่าว

3. ปัจจุบันการประเมินความเสี่ยงตามมาตรฐาน TRIS จะมุ่งเน้นการประเมินใน 2 ส่วนหลัก คือ แผนแม่บทสารสนเทศขององค์กร และระบบสารสนเทศที่สนับสนุนระบบการบริหารหลักขององค์กร ซึ่งการประเมินจะมีการกำหนดค่าเกณฑ์วัดตามแผนงานมาตรฐาน ISO 27001:2005 และในแง่ของการบริหารความเสี่ยงนั้นจะมุ่งไปที่การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) ซึ่งปัจจุบันถือว่าเป็นความเสี่ยงที่มีนัยสำคัญสูงมากสำหรับทุกองค์กร โดย TRIS ได้มีการตั้งเกณฑ์การประเมินความเสี่ยงต่อระบบหลักที่ใช้งานด้านเทคโนโลยีสารสนเทศที่เกิดความเสียหาย และส่งผลกระทบในด้านต่างๆ อาทิ ด้านบุคคลที่ได้รับผลกระทบ ด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน และด้านมูลค่าความเสียหายโดยตรงของผู้ใช้บริการ ทั้งนี้การกำหนดเกณฑ์การประเมินความเสี่ยงขององค์กรในแต่ละองค์กร อาจมี การกำหนดเกณฑ์ที่มีความแตกต่างกันออกไป อันเนื่องมาจากการดำเนินธุรกิจที่มีความแตกต่างกันออกไป ซึ่งเกณฑ์การประเมินความเสี่ยงที่มีการกำหนดขึ้นโดย TRIS นั้นสามารถปรับเปลี่ยน หรือปรับปรุงให้สอดคล้องกับการดำเนินธุรกิจขององค์กรได้เช่นกัน เพียงแต่กรอบในการดำเนินการหรือกรรมวิธีที่จะใช้ในการประเมินความเสี่ยงหรือบริหารความเสี่ยงนั้น TRIS ได้แนะนำให้เป็นไปตามมาตรฐาน ISO 27001 เพื่อมุ่งเน้นให้องค์กรหรือหน่วยงานนั้นได้ผลลัพธ์สุดท้ายจากการได้รับมาตรฐานด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001:2005

4. จากการศึกษากฎหมาย ข้อระเบียบที่เกี่ยวข้องกับ หน่วยงานรัฐวิสาหกิจที่ผู้วิจัย ได้ทำการศึกษานั้น มีกฎหมายและพระราชกฤษฎีกาหลาย ๆ มาตราที่เกี่ยวข้องใน การดำเนินธุรกิจด้วยการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรซึ่งได้แก่

4.1 พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 ที่มุ่งเน้นเพื่อประโยชน์สุขของประชาชน เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ มีประสิทธิภาพ เกิดความคุ้มค่าในเชิงภารกิจของรัฐ ลดขั้นตอนการปฏิบัติงานที่เกินความจำเป็น

4.2 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอกนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

4.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่กำหนดให้ทุก ๆ หน่วยงานที่มีการใช้งานระบบเครือข่ายสื่อสารข้อมูล ต้องทำการเก็บข้อมูลจราจรทางคอมพิวเตอร์ และสามารถระบุตัวตนของผู้ใช้งานระบบเครือข่ายสื่อสารข้อมูลได้ เพื่อใช้สำหรับการตรวจสอบหาผู้กระทำผิดตามพระราชบัญญัติดังกล่าว

ด้วยกฎหมาย และข้อระเบียบต่าง ๆ ทำให้หน่วยงานจำเป็นต้องมีการตรวจสอบและบริหารจัดการการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานรัฐวิสาหกิจ ในด้านความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อเสนอแนะ

ระบบสารสนเทศเพื่อสนับสนุนการประเมินความเสี่ยงสารสนเทศหน่วยงานรัฐวิสาหกิจควรต้องมีการพัฒนาระบบในส่วนต่างๆเพิ่มเติมเพื่อให้เกิดความสมบูรณ์มากยิ่งขึ้น โดยสรุปสาระสำคัญได้ดังต่อไปนี้

1. การนำมูลค่าของสินทรัพย์ที่เป็นตัวเงิน มาคิดคำนวณหาความสำคัญ ของสินทรัพย์ เนื่องจากบางหน่วยงานที่มีการดำเนินงานธุรกิจที่มีความเกี่ยวข้องกับธุรกรรมทางการเงิน อาจจะนำเอามูลค่าของสินทรัพย์มาเป็นปัจจัยหลักในการพิจารณาถึงความสำคัญของสินทรัพย์ ซึ่งการปรับปรุงดังกล่าวจะทำให้ผลลัพธ์ของการประเมินความสำคัญของสินทรัพย์ มีความสอดคล้องต่อการดำเนินงานธุรกิจนั้น ๆ

2. การพัฒนาระบบเพิ่มเติมในส่วน ของการจัดทำรายงาน และสืบค้นข้อมูล เพื่อนำเสนอในรูปแบบต่าง ๆ

3. การพัฒนาระบบให้มีความสามารถในเชิงการรองรับผู้ใช้งานได้หลายๆ ช่องทางเพื่อเพิ่มศักยภาพในการทำงานของระบบ