บทที่ 1

บทนำ

ความเป็นมาของปัญหา

จากพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 (พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี, พ.ศ. 2546) ได้กำหนดเป้าหมายของการบริหารกิจการบ้านเมืองที่ดีว่า "ให้เป็นไปเพื่อประโยชน์สุขของประชาชนเกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ มีประสิทธิภาพและเกิดความคุ้มค่าในเชิงภารกิจของรัฐ ลดขั้นตอนการปฏิบัติงานที่เกิดจำเป็น ประชาชนได้รับการอำนวยความสะดวกและได้รับการตอบสนองความต้องการ รวมทั้งมีการประเมินผลการปฏิบัติงานอย่างสม่ำเสมอกัน" สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) จึงได้กำหนดให้การพัฒนาคุณภาพการบริหารจัดการภาครัฐ เป็นตัวชี้วัดหนึ่งในมิติด้านการพัฒนาองค์กร โดยกำหนดเป็นตัวชี้วัดเลือกในส่วนราชการระดับกรมในปีงบประมาณ พ.ศ. 2550 และกำหนดเป็นตัวชี้วัดบังคับในปีงบประมาณ พ.ศ. 2551 ซึ่งกระทรวงการคลัง และธนาคารแห่งประเทศไทยได้ผลักดันให้มีการจัดหาสถาบันเพื่อจัดอันดับเครดิตขึ้นให้แก่หน่วยงานภาครัฐ ได้แก่ บริษัท ไทยเรทติ้งแอนด์อินฟอร์เมชั่นเซอร์วิส จำกัด หรือทริส (TRIS) (ไทยเรทติ้งแอนด์อินฟอร์เมชั่นเซอร์วิส, 2551) เพื่อให้เป็นผู้จัดทำเกณฑ์ และประเมินผลการปฏิบัติงานของภาครัฐตามพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี ซึ่ง TRIS ได้มีการประเมินผลการปฏิบัติงานของหน่วยงานภาครัฐ และรัฐวิสาหกิจอย่างต่อเนื่อง อาทิ การนิคมอุตสาหกรรมแห่งประเทศไทย หน่วยงานราชการ ธนาคารออมสิน (ไทยเรทติ้งแอนด์อินฟอร์เมชั่นเซอร์วิส, 2551)

นับตั้งแต่มีการประกาศพระราชกฤษฎีกาและพระราชบัญญัติต่างๆ ตั้งแต่ พ.ศ. 2546 รวมทั้งมีการประเมินตลอดเรื่อยมาตั้งแต่ พ.ศ. 2546 นับแต่นั้นเป็นต้นมาได้มีการเพิ่มเติมเกณฑ์การประเมินในการตรวจสอบอย่างต่อเนื่อง โดยสาเหตุสำคัญมาจากการเพิ่มเติมข้อกำหนดกฎหมายของประเทศไทยหลายฉบับที่เกี่ยวข้อง อาทิ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 เมื่อวันที่ 10 มกราคม 2550 (พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ, พ.ศ. 2549) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เมื่อวันที่ 18 กรกฎาคม 2550 (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พ.ศ. 2550) และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในเดือนธันวาคม 2544 (คลังปัญญาไทย,

2551) ด้วยเหตุนี้เกณฑ์ที่ใช้ในการประเมินตรวจสอบมีการเพิ่มเติมและมุ่งเน้นด้านความเสี่ยงและ
ความมั่นคงปลอดภัยของสารสนเทศมากขึ้น เพื่อให้เกิดการประเมินและการปฏิบัติที่ดีในการ
ตรวจสอบจำเป็นต้องอาศัย "ระบบการบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ"
(Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001:2005
(International Organization for Standardization, พ.ศ. 2548) และมาตรฐาน NIST 800-30
Risk Management Guide for Information Technology System (National Institute of
Standards and Technology, พ.ศ. 2545) เข้ามาเป็นองค์ประกอบ ซึ่ง TRIS ก็ได้มีการเพิ่มเติม
หลักเกณฑ์การประเมินการบริหารความเสี่ยง เพื่อให้ครอบคลุมตามพระราชกฤษฎีกา และ
พระราชบัญญัติ โดยการประเมินประจำปีบัญชี 2550 และ 2551 ได้มีการกำหนดค่าเกณฑ์วัดโดย
ใช้การดำเนินงานตามมาตรฐาน ISO/IEC 27001:2005

ในการบริหารความเสี่ยงนั้น ขั้นตอนแรกจะต้องมีการประเมินความเสี่ยง ซึ่งการประเมิน
ความเสี่ยงจะมีการเปลี่ยนแปลงไปทุกปีตามเกณฑ์การประเมินที่มีการปรับปรุงอย่างต่อเนื่อง
ดังนั้นผู้วิจัยได้เล็งเห็นว่าถ้ามีการพัฒนาระบบสารสนเทศที่ดีมารองรับในการตรวจสอบการประเมิน
ความเสี่ยงให้เป็นไปตามมาตรฐานหรือเกณฑ์การประเมินที่เปลี่ยนแปลงไปทุกปี ซึ่งจะเป็น
ประโยชน์ต่อผู้ใช้งาน หรือหน่วยงานภาครัฐอื่น ๆ ที่อาจจะนำไปปรับใช้ได้ ผู้วิจัยจึงเห็นสมควรให้มี
การพัฒนาระบบบริหารข้อมูลเพื่อการประเมินความเสี่ยงด้านสารสนเทศนี้ขึ้น โดยการพัฒนาระบบ
ในครั้งนี้จะเน้นศึกษาในกรอบของหน่วยงานรัฐวิสาหกิจเป็นหลัก

จุดมุ่งหมายของการวิจัย

1. เพื่อศึกษากระบวนการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจ
2. เพื่อศึกษาการประเมินความเสี่ยงตามมาตรฐาน NIST SP 800-30
3. เพื่อศึกษาการประเมินความเสี่ยงตามมาตรฐาน TRIS
4. เพื่อศึกษากฎหมาย ข้อระเบียบที่เกี่ยวข้องกับหน่วยงานรัฐวิสาหกิจ
5. เพื่อพัฒนาระบบสารสนเทศเพื่อสนับสนุนการประเมินความเสี่ยงด้านสารสนเทศ
หน่วยงานรัฐวิสาหกิจ

ความสำคัญของการวิจัย

1. มีระบบสารสนเทศที่ใช้ในการบริหารข้อมูลเพื่อการประเมินความเสี่ยงอย่างเป็นระบบ
2. มีระบบสารสนเทศที่สามารถจัดทำรายงานผลการประเมินความเสี่ยงสำหรับใช้ในการ
ตรวจสอบของ TRIS

3. มีระบบสารสนเทศที่สามารถจัดทำรายงานผลการประเมินความเสี่ยง สำหรับนำไปกำหนดนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Information Security Policy)

4. เพื่อเป็นระบบสารสนเทศต้นแบบด้านการบริหารข้อมูล เพื่อการประเมินความเสี่ยงด้านสารสนเทศสำหรับนำไปปรับใช้กับหน่วยงานภาครัฐและรัฐวิสาหกิจอื่น ๆ

ขอบเขตของการวิจัย

การจัดทำโครงการนี้เป็นการศึกษาและพัฒนาระบบสารสนเทศ เพื่อใช้ในระบบสารสนเทศในการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจ โดยมีขอบเขตในการพัฒนา ดังต่อไปนี้

1. ขอบเขตในระดับหน่วยงาน

พัฒนาระบบสารสนเทศ เพื่อการประเมินความเสี่ยงด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจ

2. ขอบเขตในระดับกระบวนงาน

2.1 ส่วนของผู้ดูแลระบบ มีความสามารถดังต่อไปนี้

2.1.1 สร้าง Username และ Password

2.1.2 กำหนดสิทธิ์การใช้งาน

2.2 ส่วนของเจ้าหน้าที่ผู้ใช้งานระบบ มีความสามารถดังต่อไปนี้

2.2.1 บันทึกข้อมูล และจัดกลุ่มสินทรัพย์ทางเทคโนโลยีสารสนเทศ และการสื่อสาร

2.2.2 บันทึกภัยคุกคาม (Threat) และช่องโหว่ (Vulnerability) ของสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร

2.2.3 บันทึกค่าระดับความสำคัญของสินทรัพย์ ในแต่ละองค์ประกอบของการรักษาความมั่นคงปลอดภัยตามมาตรฐาน ISO27001 และ TRIS ได้แก่ ความลับ (Confidentiality) ความมั่นคงของข้อมูลสารสนเทศ(Integrity) และสภาพพร้อมใช้งาน (Availability)

2.2.4 ประมวลผลจัดระดับความเสี่ยง (Risk Value) ประเมินค่าระดับความเสี่ยง (Risk Assessment) ของสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร

2.2.5 จัดทำรายงานสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสารรายงานการประเมินผลความเสี่ยง (Risk Assessment)

2.3 ส่วนของผู้บริหาร สามารถเรียกดูรายงานสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร และรายงานการประเมินผลความเสี่ยง (Risk Assessment)

3. ขอบเขตในระดับการทำงาน

3.1 ส่วนของการบันทึกข้อมูล ได้แก่

3.1.1 การบันทึกข้อมูล และจัดกลุ่มสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร

3.1.2 การบันทึกภัยคุกคาม (Threat) และช่องโหว่ (Vulnerability) สินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร

3.1.3 การบันทึกค่าระดับความสำคัญของสินทรัพย์ในแต่ละองค์ประกอบของการรักษาความมั่นคงปลอดภัยตามมาตรฐาน ISO 27001 และ TRIS ได้แก่ ความลับ (Confidentiality) ความมั่นคงของข้อมูลสารสนเทศ (Integrity) และสภาพพร้อมใช้งาน (Availability)

3.2 ส่วนของรายงาน ได้แก่

3.2.1 รายงานสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร

3.2.2 รายงานการประเมินผลความเสี่ยง (Risk Assessment)

3.3 ส่วนของงานพิมพ์ข้อมูล ได้แก่

3.3.1 พิมพ์รายงานสินทรัพย์ทางเทคโนโลยีสารสนเทศและการสื่อสาร

3.3.2 พิมพ์รายงานการประเมินผลความเสี่ยง (Risk Assessment)

นิยามศัพท์เฉพาะ

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วยการรักษาคุณค่าพื้นฐาน สามประการ ได้แก่ การรักษาความลับ (Confidentiality) ความมั่นคงของข้อมูลสารสนเทศ (Integrity) และ ความพร้อมใช้งาน (Availability)

เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศและการสื่อสารข้อมูล ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสาร และสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

ความลับ (Confidentiality) หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

ความมั่นคงของข้อมูลสารสนเทศ (Integrity) หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

ความพร้อมใช้งาน (Availability) หมายถึง การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

การพิสูจน์ทราบ (Authentication) หมายถึง การตรวจสอบและการพิสูจน์สิทธิของการขอเข้าใช้ระบบของผู้ใช้บริการจากรายชื่อผู้มีสิทธิ สำหรับอุปกรณ์ ICT รวมถึงระบบงาน (Application) ทั้งหลาย

การพิสูจน์สิทธิ์ (Authorization) หมายถึง การตรวจสอบว่า บุคคล อุปกรณ์ ICT หรือระบบงาน (Application) นั้น ๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

ภัยคุกคาม (Threat) หมายถึง สิ่งที่เป็นไปได้ที่แหล่งกำเนิดภัยคุกคามจะกระทำต่อสิ่งที่ไม่มีความมั่นคง ความไม่มั่นคงคือความอ่อนแอของสิ่งหนึ่งทำให้ได้รับผลกระทบจากภายนอกได้ง่าย การพิจารณาความเป็นไปได้ของการเกิดภัยคุกคามจึงต้องพิจารณาจากแหล่งกำเนิดภัยคุกคาม ความอ่อนแอไม่มั่นคง และการควบคุมที่มีอยู่

ความเป็นไปได้ที่จะเกิดภัยคุกคาม (Likelihood) หมายถึง จุดอ่อนที่เกี่ยวข้องกับสินทรัพย์ ซึ่งอาจจะถูกคุกคามจากภัยต่าง ๆ ก่อให้เกิดการละเมิดความปลอดภัยที่ไม่พึงปรารถนาขึ้น ซึ่งส่งผลให้มีการสูญเสีย ความเสียหาย หรืออันตรายต่อธุรกิจ

สินทรัพย์ (Asset) หมายถึง อะไรก็ตามที่มีมูลค่า หรือมีผลกระทบต่อการให้บริการด้านสารสนเทศของหน่วยงานรัฐวิสาหกิจ (ISO/IEC 27001, พ.ศ. 2548)

ข้อมูล (Data) หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ไม่ว่าการสื่อความหมายนั้นจะทำโดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเทป ซีดี (CD) จานบันทึก (Hard disk) อุปกรณ์เก็บข้อมูลแบบพกพา (Handy/Thumb Drive) เอกสาร แฟ้ม รายงาน หนังสือ แผนที่ แผนผัง ภาพวาด ภาพถ่าย ฟิล์มบันทึกภาพ เทปเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือ กราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

การรักษาความมั่นคงปลอดภัยของข้อมูล (Information security) หมายถึง การป้องกันข้อมูลในบริบทของ การรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทน การรักษาความมั่นคงปลอดภัยของสารสนเทศได้

การประเมินความเสี่ยง (Risk assessment) หมายถึง กระบวนการโดยรวมของ การวิเคราะห์ความเสี่ยง (Risk Analysis) และการเปรียบเทียบการทบทวนความเสี่ยง (Risk Evaluation) (ISO/IEC 27001, พ.ศ. 2548)

การวิเคราะห์ความเสี่ยง (Risk Analysis) หมายถึง แผนการหรือรูปแบบในการบ่งชี้ สินทรัพย์ทางเทคโนโลยีสารสนเทศและการ และการวิเคราะห์ความเสี่ยง (ISO/IEC 27001, พ.ศ 2548)

การเปรียบเทียบการทบทวนความเสี่ยง (Risk Evaluation) หมายถึง ขั้นตอนของการ เปรียบเทียบการทบทวนจากการประเมินความเสี่ยง (ISO/IEC 27001, พ.ศ. 2548)

ความเสี่ยงที่ยอมรับได้ (Risk Acceptance) หมายถึง การยอมรับความเสี่ยง ถ้าความ เสี่ยงนั้นอยู่ในระดับที่ยอมรับได้ ซึ่งอาจไม่ต้องทำอะไรเพื่อจัดการความเสี่ยงก็ได้ แต่ต้องมีเหตุผลที่ ดีเพียงพอ

Control (**การควบคุม**) หมายถึง กิจกรรมควบคุมความเสี่ยงต้องทำอย่างไรบ้าง เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ต่ำสุดหรือยอมรับได้

ความเสี่ยงที่เหลืออยู่ (Residual Risk) หมายถึง ความเสี่ยงที่ยังคงหลงเหลืออยู่ หลังจากที่ได้มีการควบคุมความเสี่ยงนั้นๆ

นโยบายด้านความมั่นคงปลอดภัย (Security policy) หมายถึง นโยบายที่แสดง เป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบท ของความต้องการอย่างเป็นทางการขององค์กร รายละเอียดของวิธีการด้านความมั่นคงปลอดภัย ม้าจะอธิบายแยกไว้ในรายงานต่างหาก

มาตรฐาน (Standard) หมายถึง มาตรฐานที่บังคับใช้ในการปฏิบัติจริง เพื่อให้ได้ตาม วัตถุประสงค์หรือเป้าหมาย ในที่นี้หมายถึงมาตรฐาน ISO/IEC 27001 และมาตรฐาน NIST SP 800-30