บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

การพัฒนาระบบการประเมินความเสี่ยงด้านสารสนเทศ เพื่อช่วยในการประเมินและวิเคราะห์ ความเสี่ยง ภัยคุกคาม และช่องโหว่ต่าง ๆ ที่มีผลต่อข้อมูลสารสนเทศหรือระบบเทคโนโลยีสารสนเทศและการสื่อสาร ผู้พัฒนาได้ทำการศึกษาหลักทฤษฎีต่าง ๆ และเทคโนโลยีที่เกี่ยวข้อง พร้อมแหล่งข้อมูลที่มีความจำเป็นในการพัฒนาระบบสารสนเทศ โดยมีรายละเอียดดังต่อไปนี้

1. พระราชกฤษฎีว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546
2. พระราชกฤษฎีกากำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549
3. หลักเกณฑ์การประเมินการบริหารความเสี่ยง TRIS ประจำปีบัญชี 2550 และ 2551
4. การบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001:2005
5. การประเมินความเสี่ยง (Risk Assessment) ตามมาตรฐาน NIST SP 800-30
6. งานวิจัยที่เกี่ยวข้อง

พระราชกฤษฎีว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546

สืบเนื่องจากพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ โดยที่มีการปฏิรูประบบราชการเพื่อให้การปฏิบัติงานของส่วนราชการตอบสนองต่อการพัฒนาประเทศและให้บริการแก่ประชาชนได้อย่างมีประสิทธิภาพยิ่งขึ้น ซึ่งการบริหารราชการและการปฏิบัติหน้าที่ของส่วนราชการนี้ ต้องใช้วิธีการบริหารกิจการบ้านเมืองที่ดีเพื่อให้การบริหารราชการแผ่นดินเป็นไปเพื่อประโยชน์สุขของประชาชน เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ มีประสิทธิภาพ เกิดความคุ้มค่าในเชิงภารกิจของรัฐ ลดขั้นตอนการปฏิบัติงานที่เกินความจำเป็น และประชาชนได้รับการอำนวยความสะดวกและได้รับการตอบสนองความต้องการ รวมทั้งมีการประเมินผลการปฏิบัติราชการอย่างสม่ำเสมอ และเนื่องจากมาตรา 3/1 แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2534 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ 5) พ.ศ. 2545 บัญญัติให้การกำหนดหลักเกณฑ์และวิธีการในการปฏิบัติราชการและการสั่งการให้ส่วนราชการ และข้าราชการ

ปฏิบัติราชการเพื่อให้เกิดการบริหารกิจการบ้านเมืองที่ดีกระทำโดยตราเป็นพระราชกฤษฎีกา จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549

สืบเนื่องจากพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 (พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ, พ.ศ. 2549) ที่ได้มีการประกาศในราชกิจจานุเบกษาแล้วนั้น ทำให้พระราชกฤษฎีกาฉบับดังกล่าวมีผลบังคับใช้กับหน่วยงานภาครัฐที่มีการให้บริการการทำธุรกรรมทางอิเล็กทรอนิกส์ ว่าต้องมีหน้าที่ในการปฏิบัติตามหลักเกณฑ์และวิธีการของพระราชกฤษฎีกาฉบับนี้ อาทิ การจัดทำเอกสารในรูปของข้อมูลอิเล็กทรอนิกส์ต้องอยู่ในรูปที่เหมาะสมสามารถแสดงหรืออ้างอิงในภายหลังและยังคงความครบถ้วนของข้อความในรูปแบบอิเล็กทรอนิกส์ได้การกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ การกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะหรือรูปแบบลายมือชื่ออิเล็กทรอนิกส์ และการกำหนดวิธีแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อเป็นหลักฐานว่าได้มีการดำเนินการทางอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่ง โดยการทำธุรกรรมทางอิเล็กทรอนิคส์ภาครัฐ นี้มีเพื่อช่วยส่งเสริมให้หน่วยงานรัฐใช้เทคโนโลยีสารสนเทศในการปฏิบัติงาน เพิ่มศักยภาพในการให้บริการแก่ประชาชน มีทางเลือกให้แก่ประชาชนในการเข้าใช้บริการจากหน่วยงานของรัฐอาทิ ธนาคารแห่งประเทศไทย กรมสรรพากร กรมศุลกากร ตลาดหลักทรัพย์แห่งประเทศไทย สำนักเลขาธิการผู้แทนราษฎร ซึ่งความหมายของหน่วยงานรัฐตามพ.ร.บ.ธุรกรรมฯ ได้แก่

1. กระทรวง ทบวง กรม ส่วนราชการ ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น
2. รัฐวิสาหกิจที่ตั้งขึ้นโดย พ.ร.บ. หรือ พ.ร.ฎ.
3. นิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ

ในการรักษาความมั่นคงปลอดภัย อย่างน้อยต้องเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีการสำรองข้อมูล และสภาพพร้อมใช้งาน และทำแผนฉุกฉิน รวมถึงการตรวจสอบ และประเมินความเสี่ยงอย่างสม่ำเสมอ เพื่อความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นข้อมูลที่สำคัญ ในอนาคตการติดต่อกับทางภาครัฐจะมีความสะดวกมากขึ้น เนื่องมาจากการใช้เทคโนโลยีเข้ามาช่วยในการทำงานจัดเก็บเอกสารต่างๆ รวมไปถึงการประสานงานกับภาครัฐผ่านทางอินเทอร์เน็ต ทำให้สามารถลดระยะเวลาในการติดต่อกับทางภาครัฐลงได้มาก ซึ่งจากพระราชกฤษฎีกากำหนด

หลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ, พ.ศ. 2549) สามารถสรุปกิจกรรมหลัก ๆ ได้ดังนี้

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)
2. การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ (Business Continuity Planning & Disaster Recovery Planning)
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

หลักเกณฑ์การประเมินการบริหารความเสี่ยง TRIS ประจำปีบัญชี 2550 และ 2551

บริษัท TRIS ได้มีการจัดสัมมนาการชี้แจงหลักเกณฑ์การประเมิน การบริหารความเสี่ยงประจำปีบัญชี 2550 และ 2551 เมื่อวันที่ 29 พฤศจิกายน 2550 (ไทยเรทติ้งแอนด์อินฟอร์เมชั่นเซอร์วิส, 2551) โดยการประเมินการบริหารจัดการสารสนเทศมีการประเมินใน 2 ส่วนหลัก คือ แผนแม่บทสารสนเทศขององค์กร และระบบสารสนเทศที่สนับสนุนระบบการบริหารหลักๆ ขององค์กร อาทิ ระบบสารสนเทศที่สนับสนุนการบริหารทรัพยากรบุคคล ซึ่งการประเมินโดยกำหนดค่าเกณฑ์วัดจะดำเนินงานตามแผนงาน ISO 27001 ในแง่ของการบริหารความเสี่ยงนั้น โดยมุ่งไปที่การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) ซึ่งปัจจุบัน ถือว่าเป็นความเสี่ยงที่มีนัยสำคัญสูงมากสำหรับทุกองค์กร โดย TRIS ได้มีการตั้งเกณฑ์การประเมินระบบหลักที่ใช้ ICT เกิดความเสียหาย และส่งผลกระทบในด้านต่าง ๆ แสดงตามตาราง 1 ถึง 3

ตาราง 1 แสดงด้านบุคคลที่ได้รับผลกระทบ

คำอธิบาย	ระดับความสำคัญ
กระทบผู้ใช้จำนวนประมาณน้อยกว่า 10,000 คน	ต่ำ
กระทบผู้ใช้จำนวนประมาณ 10,000 – 100,000 คน	กลาง
กระทบผู้ใช้จำนวนประมาณมากกว่า 100,000 คน	สูง

ตาราง 2 แสดงด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน

คำอธิบาย	ระดับความสำคัญ
ไม่ได้รับผลกระทบด้านความเจ็บป่วย	ต่ำ
หากบาดเจ็บ หรือป่วย 1 คน	กลาง
หากเสียชีวิตเพียง 1 คน	สูง

ตาราง 3 แสดงด้านมูลค่าความเสียหายโดยตรงของผู้ใช้บริการ

คำอธิบาย	ระดับความสำคัญ
หากเสียหายทางธุรกิจต่อวันมูลค่าประมาณ 1 ล้านบาท	ต่ำ
หากเสียหายทางธุรกิจต่อวันมูลค่าระหว่างประมาณ 1 – 100 ล้านบาท	กลาง
หากเสียหายทางธุรกิจต่อวันมูลค่าเกินกว่า 100 ล้านบาท	สูง

นอกจากนี้เกณฑ์การประเมินด้าน Information Technology Governance (ITG) เพื่อรองรับ พรบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งการดำเนินการตาม พรบ. ดังกล่าว TRIS ได้มีการแนะนำให้ดำเนินงานตาม 11 หมวด ของมาตรฐาน ISO 27001 ทั้งนี้เพื่อหวังผลในการได้รับการรับรอง ISO 27001

การบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) **ตามมาตรฐาน** ISO/IEC 27001:2005

มาตรฐาน ISO27001:2005 เป็นมาตรฐานเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งจะกำหนดความต้องการเกี่ยวกับการจัดทำระบบให้มีความมั่นคงปลอดภัย โดยมีวัตถุประสงค์เพื่อช่วยให้องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ ทั้งนี้มาตรฐานดังกล่าวสามารถนำมาใช้ได้กับทุกๆ ประเภทขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยไม่ว่าจะเป็นองค์กรขนาดใหญ่หรือขนาดย่อมก็ตาม

ระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ เป็นส่วนหนึ่งในระบบบริหารจัดการขององค์กร ซึ่งมีพื้นฐานมาจากแนวทางการจัดการความเสี่ยงของธุรกิจ (Business Risk Approach) มีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ (Information) รวมทั้งทรัพย์สินอื่นๆ ที่มีความสำคัญขององค์กร ในอันที่จะสร้าง ดำเนินการ นำมาใช้ ตรวจสอบ วัดผล ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารความมั่นคงปลอดภัย เพื่อให้องค์กรรอดพ้นจากภัยคุกคามต่างๆ โดยใช้หลักการ Plan-Do-Check-Act (PDCA Model) ตามมาตรฐาน ISO 27001 โดยมีรายละเอียดดังนี้

1. Plan (**การวางนโยบาย**)

การจัดสร้างนโยบาย จุดประสงค์ กระบวนการ และขั้นตอนสำหรับ ISMS นั้นมีความสำคัญเป็นอย่างยิ่งในการจัดการแก้ไขปัญหาความเสี่ยงที่อาจเกิดขึ้น และยังมีความสำคัญต่อการพัฒนาศักยภาพของระบบรักษาความปลอดภัยของข้อมูล ส่งผลตรงต่อนโยบายและจุดประสงค์หลักขององค์กร ดังนั้นในขั้นตอนการวางนโยบาย จะเป็นการกำหนดขอบเขต วิเคราะห์และประเมินผลของปัญหา คัดเลือกวิธีและขั้นตอนในการแก้ไขปัญหาความเสี่ยวที่อาจจะเกิดขึ้น

2. Do (**จัดสร้างและปฏิบัติการ**)

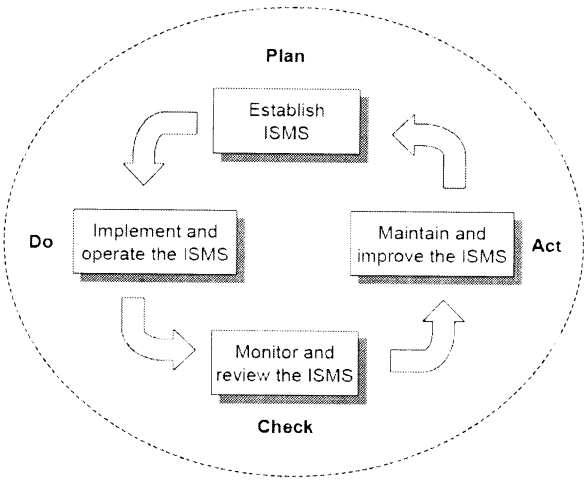
การจัดสร้างและปฏิบัติการสำหรับ ISMS ในขั้นตอนนี้จะเป็นการวงนโยบาย การควบคุม กำหนดขั้นตอนและกระบวนการ ดังนั้นในขั้นตอนการจัดสร้างและปฏิบัติการ จะเป็นการกำหนดแผนแก้ไขปัญหาความเสี่ยง จัดสร้างแผนแก้ไขปัญหาความเสี่ยงเพื่อนำไปสู่การคัดสรรเครื่องมือในการจัดการและควบคุมความเสี่ยง รวมทั้งการติดตั้งเครื่องมือในการจัดการและควบคุมความเสี่ยงที่คัดเลือกไว้

3. Check (**ค้นหาและตรวจสอบ**)

การเข้าถึง และการนำส่วนต่างๆ ที่สามารถนำไปปรับใช้ได้ไม่ว่าจะเป็นการตรวจสอบประสิทธิภาพของผลการทำงานของนโยบาย วัตถุประสงค์ และประสบการณ์ที่ตรงกับความเป็นจริง แล้วรายงานสู่ระบบจัดการเพื่อตรวจสอบ หลักการจัดทำ ISMS แล้ว

4. Act (**ดูแลและพัฒนา**)

ขั้นตอนนี้เป็นขั้นตอนสำหรับการปรับปรุงแก้ไข และป้องกันการทำงานที่ถูกรายงานจากการตรวจสอบของขั้นตอนค้นหาและตรวจสอบ เพื่อใช้ในการพัฒนาศักยภาพของการจัดทำ ISMS ทั้งนี้เพื่อสร้างความมั่นใจในการจัดทำ ISMS ทำงานอย่างมีเสถียรภาพ จึงมีความจำเป็นอย่างยิ่งที่จะต้องทำให้ระบบมีความทันสมัยอยู่ตลอดเวลา



ภาพ 1 แสดงหลักการ Plan-Do-Check-Act (PDCA Model)

จากหลักการของ PDCA Model ในระหว่างขั้นตอน Plan (การวางนโยบาย) และ Do (จัดสร้างและปฏิบัติการ) ซึ่งจะเป็นขั้นตอนในการกำหนดขอบเขต วิเคราะห์ และประเมินความเสี่ยงที่เกิดขึ้น รวมทั้งการกำหนดแผนแก้ไขปัญหาความเสี่ยงนั้น โดยในขั้นตอนที่กล่าวมาจะมุ่งเน้นในการประเมินความเสี่ยงเพื่อให้ได้มาซึ่งผลลัพธ์ของความเสี่ยงนั้นที่มีผลกระทบต่อสินทรัพย์นั้นๆ ขององค์กร นอกจากหลักการของ PDCA Model กระบวนการตรวจสอบและการสร้างความมั่นคงปลอดภัยสารสนเทศ ยังมีการใช้วัตถุประสงค์การควบคุม (Control Objectives) ซึ่งอยู่ภายใต้มาตรฐาน ISO27001:2005 ซึ่งประกอบไปด้วย 11 หมวดโดยมีรายละเอียดดังนี้

ตาราง 4 แสดงวัตถุประสงค์การควบคุม (Control Objectives)

หมายเลขอ้างอิง	คำอธิบาย	วัตถุประสงค์
A.5	นโยบายความมั่นคงปลอดภัย (Security Policy)	เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรเพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

ตาราง 4 (ต่อ)

หมายเลขอ้างอิง	คำอธิบาย	วัตถุประสงค์
A.6	โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)	เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
A.7	การบริหารจัดการทรัพย์สินขององค์กร (Asset management)	เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้
A.8	ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)	เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้ทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่
A.9	การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก
A.10	การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)	เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย และ รักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

ตาราง 4 (ต่อ)

หมายเลขอ้างอิง	คำอธิบาย	วัตถุประสงค์
A.11	การควบคุมการเข้าถึง (Access control)	เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ
A.12	การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)	เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ และป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์
A.13	การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)	เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
A.14	การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)	เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

ตาราง 4 (ต่อ)

หมายเลขอ้างอิง	คำอธิบาย	วัตถุประสงค์
A.15	การปฏิบัติตามข้อกำหนด (Compliance)	เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร และเพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

การประเมินความเสี่ยง (Risk Assessment) ตามมาตรฐาน NIST SP 800-30

National Institute of Standards and Technology หรือ NIST เป็นองค์กรในการจัดทำมาตรฐานด้านเทคโนโลยีของประเทศสหรัฐอเมริการ NIST ได้มีการจัดทำมาตรฐาน NIST SP 800-30 (Risk Management Guide for Information Technology Systems) ซึ่งมาตรฐานดังกล่าวได้มีการกำหนดกรรมวิธีในการประเมินความเสี่ยงซึ่งเป็นกระบวนการแรกในวิธีการบริหารจัดการความเสี่ยง องค์กรทั้งหลายมักใช้การประเมินความเสี่ยงในการตรวจสอบขอบเขตของความเสี่ยง และภัยคุกคามที่สัมพันธ์กับระบบสารสนเทศรวมไปถึงช่วงชีวิตของการพัฒนาระบบ (SDLC: System Development Life Cycle) ผลที่ได้จากกระบวนการนี้ช่วยให้สามารถหาวิธีการควบคุมที่เหมาะสมสำหรับการลดหรือกำจัดความเสี่ยงที่เกิดขึ้น

ความเสี่ยงเป็นเหตุการณ์ที่เกิดขึ้นที่ไม่เป็นไปตามความคาดหวัง มีโอกาสที่จะเกิดเหตุการณ์ใดๆ ซึ่งก่อให้เกิดภัยคุกคามในระบบที่มีช่องโหว่ในการปกป้อง กับความรุนแรงของผลกระทบที่จะเกิดขึ้นจากภัยคุกคามนั้น ในการตรวจสอบโอกาสในการเกิดเหตุการณ์หรือภัยคุกคามใดๆ ในอนาคตที่มีผลต่อระบบข้อมูลขององค์กรนั้นจะต้องวิเคราะห์จากช่องโหว่ และวิธีการควบคุมของระบบ ในขณะที่ผลกระทบที่เกิดขึ้นจะพิจารณาที่ความรุนแรง ซึ่งกรรมวิธีในการประเมินความเสี่ยงตามมาตรฐาน NIST SP 800-30 จะวิธีการประเมินความเสี่ยงอยู่ 9 ขั้นตอนซึ่งมีรายละเอียดต่อไปนี้

1. การอธิบายลักษณะของระบบ (System Characterization)

   การประเมินความเสี่ยงในระบบข้อมูลสารสนเทศ ขั้นตอนแรกคือการระบุขอบเขตใน

การพิจารณา ซึ่งจะต้องคำนึงถึงจำนวนทรัพยากรและข้อมูลข่าวสารที่มีอยู่ในระบบ การอธิบายลักษณะระบบข้อมูลสารสนเทศจะต้องกำหนดขอบเขตในการประเมินความเสี่ยง จำแนกขอบเขตการให้สิทธิในการทำงาน และเตรียมข้อมูลที่มีผลต่อความเสี่ยง โดยการอธิบายลักษณะของระบบจะจำแนกออกเป็น 2 ส่วนหลักซึ่งได้แก่

1.1 ข้อมูลที่สัมพันธ์กับระบบ (System-Related Information)

การระบุความเสี่ยงในระบบข้อมูลสารสนเทศต้องอาศัยความเข้าใจในสภาพแวดล้อมของกระบวนการภายในระบบ ผู้ที่มีหน้าที่ในการประเมินความเสี่ยงต้องรวบรวมข้อมูลที่สัมพันธ์กับระบบทั้งหมดก่อน ซึ่งปกติสามารถจำแนกประเภทได้ดังนี้

1.1.1 อุปกรณ์ฮาร์ดแวร์

1.1.2 ซอฟแวร์

1.1.3 การเชื่อมต่อระบบทั้งภายในและภายนอกระบบ

1.1.4 ข้อมูลและข่าวสาร

1.1.5 บุคคลผู้ที่ดูแลและใช้งานระบบ

1.1.6 พันธกิจของระบบ อาทิ กระบวนการที่ทำโดยระบบข้อมูลสารสนเทศ

1.1.7 ความสำคัญของข้อมูลและระบบ อาทิ คุณค่าของระบบหรือความสำคัญที่มีต่อองค์กร

1.1.8 ระดับการปกป้องข้อมูลและระบบ

1.2 เทคนิคการรวบรวมข้อมูล (Information Gathering Techniques) เทคนิคที่สามารถนำมาใช้ประกอบไปด้วย 3 ส่วนหลักได้แก่

1.2.1 ส่วนแบบสอบถาม (Questionnaire) ในการรวบรวมข้อมูลที่เกี่ยวข้องผู้ที่ทำการประเมินความเสี่ยงสามารถปรับปรุงแบบสอบถาม ซึ่งเกี่ยวข้องกับการบริหารและการควบคุมการปฏิบัติงานที่วางแผนหรือถูกนำไปใช้กับระบบข้อมูลสารสนเทศได้ แบบสอบถามนี้ควรจะสามารถใช้ได้ทั้งกับบุคคลที่มีความรู้ทางด้านเทคนิคและบุคคลที่มีความรู้ด้านการบริหารจัดการที่ทำงานเกี่ยวข้องกับระบบข้อมูลสารสนเทศ นอกจากนี้แบบสอบถามยังสามารถนำไปใช้ในกรณีที่มีการสัมภาษณ์ได้อีกด้วย

1.2.2 ส่วนการสัมภาษณ์ตามสถานที่จริง (On-site Interviews) การสัมภาษณ์บุคคลที่มีหน้าที่ดูแลหรือบริหารระบบข้อมูลสารสนเทศทำให้ผู้ประเมินความเสี่ยงสามารถรวบรวมข้อมูลที่มีประโยชน์ได้อย่างเต็มที่ การเข้าไปตามสถานที่จริงทำให้ผู้ประเมินความเสี่ยงสามารถ

สังเกตและรวบรวมข้อมูลเกี่ยวกับลักษณะทางกายภาพ สภาพแวดล้อม และการรักษาความปลอดภัยในเชิงปฏิบัติของระบบข้อมูลสารสนเทศได้

1.2.3 การตรวจเอกสาร (Document Review) เอกสารนโยบายบริษัท เอกสารเกี่ยวกับระบบ และเอกสารที่เกี่ยวกับการรักษาความปลอดภัยสามารถนำมาใช้เป็นข้อมูลที่ดีในการประเมินได้

2. การบ่งชี้ภัยคุกคาม (Threat Identification)

ภัยคุกคาม คือ สิ่งที่เป็นไปได้ที่แหล่งกำเนิดภัยคุกคามจะกระทำต่อสิ่งที่ไม่มีความมั่นคง ความไม่มั่นคงคือความอ่อนแอของสิ่งหนึ่งทำให้ได้รับผลกระทบจากภายนอกได้ง่าย การพิจารณาความเป็นไปได้ของการเกิดภัยคุกคามจึงต้องพิจารณาจากแหล่งกำเนิดภัยคุกคาม ความอ่อนแอไม่มั่นคง และการควบคุมที่มีอยู่

การบ่งชี้แหล่งกำเนิดภัยคุกคาม(Threat-Source Identification) เป้าหมายของขั้นตอนนี้ คือระบุแหล่งกำเนิดของภัยคุกคามและประมวลผลเป็นรายชื่อภัยคุกคามที่มีผลต่อระบบข้อมูลสารสนเทศเพื่อนำมาใช้ในการประเมิน แหล่งกำเนิดของภัยคุกคามโดยทั่วไปสามารถแบ่งออกเป็น 3 ประเภทดังนี้

2.1 ประเภทแรก ภัยคุกคามโดยธรรมชาติ (Natural Threats) อาทิ น้ำท่วม แผ่นดินไหว และพายุ

2.2 ประเภทสอง ภัยคุกคามโดยมนุษย์ (Human Threats) ทั้งการกระทำที่เกิดจากความไม่ตั้งใจและการกระทำผิดโดยเจตนา

2.3 ประเภทสาม ภัยคุกคามจากสภาพแวดล้อม (Environment Threats) อาทิ ระบบไฟฟ้าขัดข้อง มลภาวะ และสารเคมีรั่วไหล

3. การบ่งชี้ความไม่มั่นคง (Vulnerability Identification)

การวิเคราะห์ภัยคุกคามที่มีต่อระบบข้อมูลสารสนเทศ ต้องมีการวิเคราะห์ความอ่อนแอไม่มั่นคงของสภาพแวดล้อมของระบบ เป้าหมายของขั้นตอนนี้คือการพัฒนารายการความไม่มั่นคงของระบบที่ทำให้ระบบมีโอกาสได้รับภัยคุกคาม

4. การวิเคราะห์การควบคุม (Control Analysis)

เป้าหมายของขั้นตอนนี้เพื่อวิเคราะห์การควบคุมที่องค์กรใช้อยู่หรือที่วางแผนไว้เพื่อลดหรือกำจัดโอกาสที่จะเกิดภัยคุกคาม การวัดระดับโอกาสที่จะเกิดความเสี่ยงซึ่งบ่งชี้ถึงความเป็นไปได้ที่ระบบจะไม่มีความมั่นคงสามารถทำได้เมื่ออยู่ในสภาพแวดล้อมที่มีภัยคุกคาม เช่น โอกาสเกิดความเสี่ยงจะต่ำ ถ้าแหล่งกำเนิดภัยคุกคามมีความสามารถต่ำในการสร้างผลกระทบ

หรือเมื่อองค์กรมีวิธีการควบคุมและรักษาความปลอดภัยที่มีประสิทธิภาพมากพอที่จะลด หรือกำจัดอันตรายที่จะเกิดขึ้น

5. การตรวจสอบโอกาสในการเกิดภัยคุกคาม (Likelihood Determination)

การวัดระดับโอกาสที่จะเกิดความเสี่ยงซึ่งบ่งชี้ถึงความเป็นไปได้ที่ระบบจะไม่มีความมั่นคงสามารถทำได้เมื่ออยู่ในสภาพแวดล้อมที่มีภัยคุกคาม ปัจจัยที่ต้องพิจารณาได้แก่

5.1 ความสามารถของแหล่งกำเนิดภัยคุกคามในการก่อให้เกิดความเสี่ยง

5.2 ธรรมชาติของความไม่มั่นคงที่ก่อให้เกิดความเสี่ยง

5.3 ความมีประสิทธิภาพของวิธีการควบคุมที่มีอยู่

โอกาสที่ระบบเกิดความไม่มั่นคงเนื่องจากแหล่งกำเนิดภัยคุกคามสามารถอธิบายได้ด้วยระดับของความเป็นไปได้อาทิ ระดับสูง ระดับปานกลาง และระดับต่ำ แต่ละระดับความเป็นไปได้มีคำนิยามดังตาราง 5

ตาราง 5 แสดงนิยามของระดับความเป็นไปได้ (Likelihood Definitions)

ระดับความสำคัญ	คำอธิบาย
สูง	แหล่งกำเนิดภัยคุกคามมีความสามารถสูงในการกระตุ้นและก่อให้เกิดความเสี่ยงต่อระบบและวิธีการควบคุมที่มีอยู่ไม่มีประสิทธิภาพ
ปานกลาง	แหล่งกำเนิดภัยคุกคามมีความสามารถพอที่จะก่อให้เกิดความเสี่ยงต่อระบบได้ แต่ระบบมีการควบคุมที่มีประสิทธิภาพทำให้สามารถป้องกันระบบจากความไม่มั่นคงที่เกิดขึ้นจากภัยคุกคามได้
ต่ำ	แหล่งกำเนิดภัยคุกคามไม่สามารถสร้างความเสี่ยงให้แก่ระบบได้ หรือวิธีการควบคุมความปลอดภัยของระบบมีประสิทธิภาพสูง สามารถรักษาความมั่นคงของระบบได้ดี

6. การวิเคราะห์ผลกระทบ (Impact Analysis)

อีกขั้นตอนหนึ่งในการวัดระดับความเสี่ยงคือการตรวจสอบผลกระทบต่อระบบเมื่อเกิดภัยคุกคามขึ้น การวิเคราะห์ผลกระทบนำไปสู่การจัดลำดับผลกระทบโดยพิจารณาจากข้อมูลขององค์กร ซึ่งก็ขึ้นอยู่กับการประเมินความสำคัญและผลกระทบในการเปลี่ยนแปลงของสินทรัพย์ทั้งหลายทั้งในเชิงปริมาณหรือเชิงคุณภาพ หากไม่สามารถหาข้อมูลรายงานขององค์กรได้

ผลกระทบในการต่อการเปลี่ยนแปลงของระบบและข้อมูลสามารถตรวจสอบได้จากระดับการป้องกัน เพื่อดูแลรักษาระบบและข้อมูลให้สามารถใช้งานได้เมื่อต้องการ รวมไปถึงความน่าเชื่อถือและความถูกต้องแม่นยำของระบบและข้อมูลด้วย อย่างไรก็ตาม ในการวิเคราะห์ผลกระทบต้องอาศัยความร่วมมือของเจ้าของข้อมูลและระบบ

ผลกระทบจะประกอบไปด้วยผลกระทบที่จับต้องได้สามารถวัดปริมาณได้ในรูปของรายได้ที่สูญเสียไป หรือต้นทุนในการซ่อมแซมระบบที่เพิ่มขึ้น ส่วนผลกระทบที่ไม่สามารถวัดปริมาณได้ก็สามารถอธิบายด้วยการวัดเป็นระดับของความรุนแรงที่มีต่อระบบอาทิ ระดับสูง ปานกลาง และ ต่ำ นิยามของแต่ละระดับดังตาราง 6

ตาราง 6 แสดงนิยามของระดับของความรุนแรง (Impact Definitions)

ระดับความสำคัญ	คำอธิบาย
ผลกระทบระดับสูง	ความไม่มั่นคงของระบบส่งผลให้เกิดการสูญเสียทรัพย์สินและทรัพยากรหลักขององค์กรจำนวนมาก หรือเป็นอันตรายร้ายแรงต่อพันธกิจหรือชื่อเสียงขององค์กร หรือส่งผลให้เกิดการสูญเสียชีวิตหรือบาดเจ็บสาหัส
ผลกระทบระดับปานกลาง	ความไม่มั่นคงของระบบส่งผลให้เกิดการสูญเสียทรัพย์สินและทรัพยากรขององค์กร หรือส่งผลต่อพันธกิจหรือชื่อเสียงขององค์กร หรือส่งผลให้เกิดการบาดเจ็บ
ผลกระทบระดับต่ำ	ความไม่มั่นคงของระบบส่งผลให้เกิดการสูญเสียทรัพย์สินและทรัพยากรขององค์กรเล็กน้อย หรือส่งผลต่อพันธกิจหรือชื่อเสียงขององค์กรบ้างเล็กน้อย

7. การตรวจสอบความเสี่ยง (Risk Determination)

การตรวจสอบความเสี่ยงจะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงจะใช้มาตรฐานเมตริกซ์ระดับความเสี่ยง (Risk-Level Matrix) ซึ่งสูตรวัดความเสี่ยงได้จากผลคูณของโอกาสเกิดความเสี่ยง (Likelihood) กับ ความรุนแรงของความเสี่ยง (Impact) ที่ระบบได้รับ

จากภัยคุกคามนั้น เมตริกซ์ระดับความเสี่ยงสามารถมีได้หลายขนาดแล้วแต่ความต้องการของแต่ละองค์กรอาทิ เมตริกซ์ 3 x 3 และเมตริกซ์ 4 x 4

ตัวอย่างในที่นี้ใช้เมตริกซ์ 3x3 จากโอกาสเกิดภัยคุกคาม 3 ระดับ (สูง ปานกลาง และต่ำ) โดยผลกระทบของภัยคุกคาม 3 ระดับ (สูง ปานกลาง และต่ำ) แสดงได้ดังตาราง 7 แสดงค่าความเป็นไปได้ของระดับโอกาสเกิดภัยคุกคามมีค่าเป็น 1 เมื่อเป็นระดับสูง มีค่าเป็น 0.5 เมื่อเป็นระดับปานกลาง และมีค่าเป็น 0.1 เมื่อเป็นระดับต่ำ และค่าของระดับความรุนแรงของผลกระทบจากภัยคุกคามมีค่าเป็น 100 เมื่อเป็นระดับสูง มีค่าเป็น 50 เมื่อเป็นระดับปานกลาง และมีค่าเป็น 10 เมื่อเป็นระดับต่ำตามลำดับ

ตาราง 7 แสดงเมตริกซ์ระดับความเสี่ยง 3x3

โอกาสการเกิดความเสี่ยง (Likelihood)	ความรุนแรงของความเสี่ยง (Impact)		
	ต่ำ (10)	ปานกลาง (50)	สูง (100)
สูง (1.0)	ต่ำ 10 x 1.0 = 10	ปานกลาง 50 x 1.0 = 50	สูง 100 x 1.0 = 100
ปานกลาง (0.5)	ต่ำ 10 x 0.5 = 5	ปานกลาง 50 x 0.5 = 25	ปานกลาง 100 x 0.5 = 50
ต่ำ (0.1)	ต่ำ 10 x 0.1 = 1	ต่ำ 50 x 0.1 = 5	ต่ำ 100 x 0.1 = 10

ระดับความเสี่ยง (Risk Level) จากเมตริกซ์ระดับความเสี่ยงมีการกำหนดสเกลของความเสี่ยง จากเมตริกซ์ตัวอย่างกำหนดให้ระดับความเสี่ยงสูงมีค่าตั้งแต่ 50–100 ระดับความเสี่ยงปานกลางมีค่าตั้งแต่ 10-50 และระดับความเสี่ยงต่ำมีค่าต่ำกว่า 50 ในแต่ละระดับความเสี่ยงมีคำอธิบายและสิ่งที่ต้องปฏิบัติดังตาราง 8

ตาราง 8 แสดงนิยามของระดับของความเสี่ยงและสิ่งที่ต้องปฏิบัติ (Risk Scale and Necessary Actions)

ระดับความเสี่ยง	คำอธิบาย
ระดับความเสี่ยงสูง	จำเป็นต้องได้รับการแก้ไขอย่างเร่งด่วน ระบบที่ดำเนินอยู่อาจจะยังคงปฏิบัติงานตามปกติแต่จะต้องนำแผนการแก้ไขมาใช้ทันทีที่เป็นไปได้
ระดับความเสี่ยงปานกลาง	ควรมีการแก้ไขและแผนการควบคุมควรได้รับการปรับปรุงแล้วนำมาใช้ ความเสี่ยงเป็นฟังก์ชันของโอกาสที่จะเกิดเหตุการณ์ใดๆ ซึ่งก่อให้เกิดภัยคุกคามในระบบที่มีความอ่อนแอในการปกป้อง กับความรุนแรงของผลกระทบที่จะเกิดขึ้นจากภัยคุกคามนั้น
ระดับความเสี่ยงต่ำ	ระบบควรได้รับการตรวจสอบเพื่อให้แน่ใจว่าแผนการควบคุมที่มีอยู่จะสามารถแก้ไขปัญหาและรับมือกับความเสี่ยงได้

8. การเสนอวิธีการควบคุม (Control Recommendation)

การควบคุมภายในองค์กรช่วยลดระดับความเสี่ยงที่จะเกิดกับระบบข้อมูลสารสนเทศและข้อมูลอื่นๆ ขององค์กรให้อยู่ในระดับที่สามารถยอมรับได้ การเสนอวิธีการควบคุมเป็นผลจากกระบวนการประเมินความเสี่ยงและเป็นการเตรียมข้อมูลสำหรับกระบวนการลดระดับความเสี่ยง

9. การจัดทำเอกสารสรุปผล (Results Documentation)

เมื่อการประเมินความเสี่ยงเสร็จสมบูรณ์แล้ว ต้องมีการรวบรวมข้อมูลที่เกี่ยวข้องทั้งหมดและจัดทำเอกสารสรุป รายงานการประเมินความเสี่ยงเป็นรายงานที่นำไปใช้ร่วมกับการบริหารจัดการ เพื่อประกอบการตัดสินใจต่างๆ ขององค์กร

งานวิจัยที่เกี่ยวข้อง

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้มีการจัดทำคู่มือการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2549 – 2551 เป็นเอกสารที่จัดทำขึ้นเพื่อประกอบโครงการจัดทำแผนแม่บทการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ซึ่งได้กำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของประเทศ ให้อยู่ในระดับมาตรฐานสากล โดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว ร่างแผนแม่บทความมั่นคงปลอดภัยด้านไอซีทีแห่ง

ชาติฯ จะช่วยจัดตั้งรูปแบบและลำดับความสำคัญในบริบทของความมั่นคงปลอดภัยด้านไอซีทีเมื่อ
คำนึงถึงสถานการณ์ ปัจจุบันและการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องทั้งหลาย ทั้งที่จะเกิดต่อ
ภาคประชาชน ภาคเอกชนและภาครัฐบาล หลังจากที่ประกาศใช้แผนแม่บท แล้วต้องการที
จะจัดให้มีกรอบการทำงานและเครื่องมือที่จำเป็นอย่างพอเพียง เพื่อที่จะสนับสนุนกิจกรรมต่าง ๆ ที่
จะเกิดขึ้นของแผนฏิบัติการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในระดับองค์กรต่อไป

แผนบริหารจัดการความเสี่ยงตามคู่มือการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2549 - 2551 เพื่อที่จะจัดการความเสี่ยงที่มี ผลต่อระบบ ICT ในสิ่งแวดล้อมที่เป็นอยู่ตามที่ได้กำหนดไว้ตามความต้องการของนโยบายความมั่นคงปลอดภัยด้านไอซีที โดยได้มีการกำหนดขั้นตอน 5 ขั้นตอนหลักๆ ดังนี้

1. กำหนดสภาวะแวดล้อม (Stage 1: Establishing the Context)

ตาราง 9 แสดงการกำหนดสภาวะแวดล้อม

ลำดับ	สภาวะแวดล้อม	ประเด็นสำคัญ
1	การบริหารจัดการความเสี่ยง	ใครเป็นผู้ดำเนินงาน, เป้าหมายของกระบวนการเหล่านี้คืออะไรและ กรอบของกระบวนการบริหารจัดการคืออะไร
2	กลยุทธ์	อะไรคือจุดแข็งและจุดอ่อน, อะไรมีลำดับความสำคัญ, ใครคือผู้มีส่วนได้-เสีย, อะไรคือภัยคุกคามและโอกาส, และอะไรคือแรงผลักดันจากภายนอก
3	การจัดองค์การ	อะไรคือวัตถุประสงค์ที่ระบบไอซีทีถูกนำมาใช้งาน , อะไรเป็นแรงขับจากภายใน, อะไรเป็นปัจจัยแห่งความสำเร็จของระบบ ICT, มีทรัพยากรอะไรบ้างที่ สามารถนำมาใช้ได้ และ ระบบ ICT ที่สามารถช่วยให้เป้าหมายหลักและความสำคัญขององค์กรบรรลุผลได้อย่างไร

ตาราง 9 (ต่อ)

ลำดับ	สภาวะแวดล้อม	ประเด็นสำคัญ
4	วิธีประเมินผล	เงื่อนไขตามกฎหมาย, มี อุปสรรคอะไรบ้างในด้าน งบประมาณทรัพยากรบุคคล และ/หรือการปฏิบัติงาน ระดับความเสี่ยงที่ยอมรับได้อยู่ที่ไหน
5	โครงสร้าง	มีทรัพย์สินที่เกี่ยวข้องอะไรบ้าง, ทรัพย์สินเหล่านี้ถูกใช้ไปอย่างไร, และ อะไรคือห้วงเวลา/เฟส หรือองค์ประกอบทางโครงสร้างของกิจกรรมใดๆ

2. บ่งชี้ปัจจัยความเสี่ยง (Stage 2: Identifying the Risks)

หลังจากดำเนินการในขั้นที่ 1 เรียบร้อยแล้วจะต้องบ่งชี้ปัจจัยความเสี่ยงซึ่งครอบคลุมความเสี่ยงให้มากที่สุดเท่าที่จะทำได้ มีประเด็นที่ต้องทำในแต่ละกรณี ได้แก่ เป็นความเสี่ยงของอะไรเกิดขึ้นได้อย่างไร และผลต่อเนื่องของความเสี่ยงที่จะเกิดขึ้น ขั้นตอนต่อไปจึงเป็น วิเคราะห์ความเสี่ยงเหล่านี้

3. วิเคราะห์ความเสี่ยง (Stage 3: Analyzing the Risks)

จุดประสงค์ของการวิเคราะห์ฯ คือเพื่อแยกความเสี่ยงที่ยอมรับได้ออกมาจากความเสี่ยงที่ยอมรับไม่ได้ และจัดให้มีข้อมูลที่เพียงพอสำหรับการประเมินและจัดการกับความเสี่ยงเหล่านั้นจากนั้นจึงทำรายการความเสี่ยงที่ระบุไว้แยกเป็นแต่ละกรณี โดยมีรายละเอียดตามขั้นตอนดังต่อไปนี้

3.1 ระบุผลต่อเนื่องของความเสี่ยงนี้

3.2 ระบุสาเหตุของความเสี่ยงและบันทึกแหล่งข้อมูลหรือโลจิกของการค้นหาแหล่งที่มานั้นๆ

3.3 ระบุระดับความเสี่ยงในภาพรวม โดยใช้ตารางสัมพันธ์ (Matrix) การหาสาเหตุที่มาของความเสี่ยงอาจสร้างเป็นประเด็นในตาราง 10

ตาราง 10 แสดงตัวอย่างการหาสาเหตุที่มาของความเสี่ยง

ความเสี่ยงถ้าเกิด	อัตราของความน่าจะเป็น
คาดว่าจะเกิดได้ในทุกกรณี	ค่อนข้างแน่นอน

ตาราง 10 (ต่อ)

น่าจะเกิดได้ในทุกกรณี	น่าจะเป็น
อาจจะเกิดได้บางครั้ง และอาจยากที่จะควบคุม เนื่องจากมีอิทธิพลจากปัจจัยภายนอก	เป็นไปได้
เกิดได้บางครั้ง	ไม่น่าจะเป็น
อาจเกิดได้ในบางกรณีเฉพาะ	ยาก

การกำหนดกลุ่มและคำอธิบายความเสี่ยงเพื่อสร้างตารางใช้วิเคราะห์ดังตาราง 11

ตาราง 11 แสดงตัวอย่างการกำหนดกลุ่มและคำอธิบายความเสี่ยงเพื่อสร้างตารางใช้วิเคราะห์

ระดับ	ความหมาย	คำอธิบาย
E	Extreme	ต้องการค้นคว้าอย่างละเอียดเพิ่มเติมและการวางแผนการบริหารจัดการจากผู้บริหารระดับสูง
H	High	ต้องการให้ผู้บริหารระดับสูงรับทราบ
M	Moderate	สามารถจัดการได้โดยการเฝ้าระวังหรือกระบวนการตอบโต้เฉพาะ แต่ละกรณีได้
L	Low	สามารถจัดการได้โดยกระบวนการที่ปฏิบัติประจำ

ตาราง 12 แสดงตัวอย่างการสร้างตาราง (Matrix)

ความน่าจะเป็น	ระดับความร้ายแรง	ผลต่อเนื่อง			
		สำคัญ	ปานกลาง	เล็กน้อย	ไม่มีผลกระทบ
ค่อนข้างแน่นอน	E	E	E	H	H
น่าจะเป็น	E	E	H	H	M
เป็นไปได้	E	E	H	M	L
ไม่น่าจะเป็น	E	H	M	L	L
ยาก	H	H	M	L	L

4. ระบุและจัดลำดับความเสี่ยง (Stage 4: Assessing and Prioritizing Risks)

จุดประสงค์ของการระบุ และจัดลำดับความเสี่ยงเพื่อที่จะหาความเร่งด่วนของการบริหารจัดการความเสี่ยง โดยเปรียบเทียบระดับของความเสี่ยงกับมาตรฐานที่เลือกไว้ เป้าหมายของระดับความเสี่ยงที่ตั้งไว้ และมาตรการทางเลือกอื่น ถ้ามีตัวอย่างขั้นตอนในการระบุและจัดลำดับความเสี่ยงที่เลือกไว้ และสร้างทะเบียน แสดงในตาราง 13

ตาราง 13 แสดงตัวอย่างขั้นตอนในการระบุและจัดลำดับความเสี่ยงที่เลือกไว้ และสร้างทะเบียน

ลำดับ	กิจกรรม
1	จัดทำเอกสารแสดงทะเบียนความเสี่ยงแต่ละกรณี ควบคู่กับมาตรฐานที่เลือกไว้ เป้าหมายของระดับความเสี่ยงที่ตั้งไว้ และมาตรการทางเลือกอื่น (ถ้ามี) เพื่อหาว่าอะไรเป็นความเสี่ยงที่ยอมรับได้
2	ระบุในแต่ละตารางเมื่อเทียบกับมาตรการที่บันทึกไว้ในลำดับที่ 1 เพื่อที่จะหาว่าความเสี่ยงนั้นยอมรับได้หรือไม่ ถ้ารับได้ให้ลงทะเบียนไว้
3	ใช้มาตรการในลำดับที่ 1 เพื่อที่จะกำหนดความเร่งด่วน ความเสี่ยงที่ยอมรับไม่ได้และบันทึกค่าไว้

5. พัฒนาแผนรับมือ (Stage 5: Developing a Risk Treatment Plan)

แผนการรับมือกับความเสี่ยง (Risk Treatment Plan) จะแสดงวิธีการที่จะประยุกต์ใช้การควบคุมการรับมือกับความเสี่ยงอย่างเป็นระบบ ทั้งนี้เพื่อลดผลกระทบ ลดความน่าจะเป็นและ/หรือลดผลต่อเนื่องที่อาจจะเกิดขึ้นมาภายหลังโดยมีขั้นตอนควรดำเนินการดังตาราง 14

ตาราง 14 แสดงขั้นตอนการควบคุมการรับมือกับความเสี่ยง

ลำดับ	กิจกรรม
1	เขียนความเสี่ยงที่ระบุไว้ว่าเป็นกรณีที่ยอมรับไม่ได้ จากทะเบียนความเสี่ยงตามลำดับความสำคัญ
2	บันทึกการควบคุมที่เหมาะสมสำหรับความเสี่ยงแต่ละกรณีบนตารางความเสี่ยง อาจมีได้ มากกว่าหนึ่งวิธี

ตาราง 14 (ต่อ)

ลำดับ	กิจกรรม
3	วิเคราะห์ Cost/benefit แล้วบันทึกผลว่า ยอมรับได้หรือไม่ได้สำหรับวิธีควบคุมแต่ละวิธี
4	คำนวณผลกระทบข้างเคียง ถ้ามี จากการควบคุมที่ยอมรับได้
5	บันทึกผลจากข้อ 4 ในทะเบียนความเสี่ยง
6	บันทึกการควบคุมที่ยอมรับได้ในทะเบียนการควบคุม จากนั้นจึงพัฒนาแผนฯ โดยการกำหนดความรับผิดชอบ ตารางการทำงานและวิธีการเฝ้าระวังสำหรับการนำไปใช้ต่อไป

ซึ่งขอบเขตของการพัฒนาระบบบริหารข้อมูลเพื่อการประเมินความเสี่ยงด้านสารสนเทศ โดยการพัฒนาระบบในครั้งนี้จะเน้นการพัฒนาเฉพาะการประเมินความเสี่ยง และการเลือกการควบคุม รวมทั้งการบันทึกความเสี่ยงที่ยอมรับได้ (Risk Acceptance) เท่านั้น