มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (อ้างอิงตาม ISO/IEC 27001:2005)

เรียบเรียงโดย...ปรีชา คำแหง

ความก้าวหน้าทางเทคโนโลยีที่เพิ่มมากขึ้นแบบทวีคูณ ส่งผลให้มีความต้องการการดูแลความมั่นคงปลอดภัยทางสารสนเทศเพิ่มขึ้นเป็นเงาตามตัว เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการบุกรุก ภัยคุกคามในรูปแบบต่างๆ องค์กรจึงต้องมีมาตรการในการป้องกันระบบสารสนเทศของตน โดยนำมาตรฐาน ISO/IEC 27001 มาใช้เพื่อมุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และเป็นมาตรฐานอ้างอิงในการเสริมสร้างความมั่นใจในประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร มาตรฐาน ISO/IEC 27001 ใช้หลักการ P-D-C-A เป็นพื้นฐานในการปฏิบัติงานเช่นเดียวกับมาตรฐาน ISO 9001 ดังนั้นองค์กรที่มีระบบบริหารงานคุณภาพตามมาตรฐาน ISO 9001 อยู่แล้วจึงประยุกต์ใช้ ISO/IEC 27001 ได้อย่างไม่ยุ่งยาก

ที่มาของ ISO/IEC 27001 มาจาก BS 7799 (BS : British Standard) part 2 เนื้อหาประกอบด้วย ข้อกำหนดและแนวทางในการจัดตั้งและการนำไปใช้งาน “ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ” (Information Security Management Systems : ISMS) ภายในองค์กรและการตรวจรับรองระบบ (Certification) โดยได้รับการเปลี่ยนสถานะเป็น ISO Standard เมื่อปี ค.ศ. 2005

BS 7799 part 1 เป็นส่วน best practice สำหรับการบริหารความมั่นคงของข้อมูล ISO/IEC 17799 ได้ถูกประกาศใช้เป็นอย่างทางการในปี ค.ศ. 2000 ซึ่งประกอบด้วยหัวข้อของการควบคุมด้านความมั่นคงของข้อมูลทั้งหมด 127 หัวข้อ แบ่งออกเป็น 10 หมวดหลัก ต่อมาในเมื่อปี ค.ศ. 2005 ได้รับการปรับปรุงโดยเพิ่มข้อกำหนดเป็น 133 หัวข้อ และ 11 หมวดหลัก และถูกเปลี่ยนชื่อเป็น ISO/IEC 27002 ซึ่งยังคงถูกใช้งานมาจนถึงปัจจุบัน

แนวทางการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศตามมาตรฐาน ISO/IEC 27001 : 2005 (ทั้งนี้ไม่กล่าวข้อ 1-3 ; Scope, Normative reference, Terms and definitions)

ข้อ 4 ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security management system)

4.1 ข้อกำหนดทั่วไป

องค์กรต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการต่างๆทางธุรกิจขององค์กร รวมทั้งความเสี่ยงที่อาจจะเกิดขึ้น โดยใช้ PDCA model มาประยุกต์ใช้ ในรูปภาพที่ 1

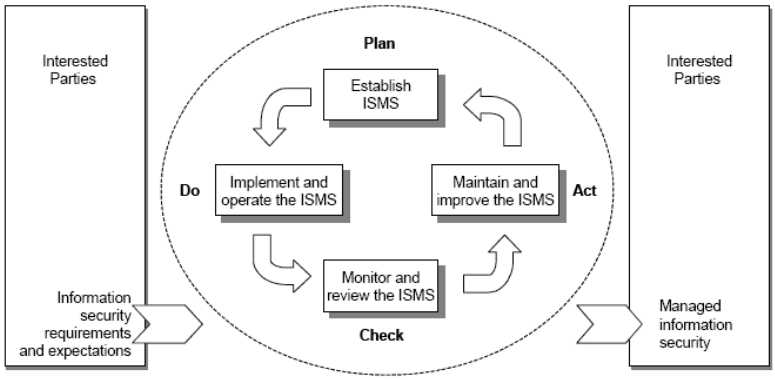

Figure 1 — PDCA model applied to ISMS processes

4.2 การกำหนดและบริหารจัดการระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Establishing and managing the ISMS)

4.2.1 กำหนดหรือวางแผนระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Establish the ISMS) - PLAN

องค์กรต้องปฏิบัติดังนี้

ก) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศโดยพิจารณาถึงคุณลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี รวมถึงรายละเอียดของสิ่งอื่นๆ ที่ไม่รวมอยู่ในขอบเขต

ข) กำหนดนโยบายโดยพิจารณาถึงคุณลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สินและเทคโนโลยี นโยบายความมั่นคงปลอดภัยจะต้องมีองค์ประกอบดังนี้ กรอบในการดำเนินการ ทิศทางและหลักการที่เกี่ยวข้อง, ข้อกำหนดทางธุรกิจและกฎหมายหรือข้อกำหนดของหน่วยกำกับดูแล, กลยุทธ์ขององค์กร, เกณฑ์ในการประเมินความเสี่ยงและต้องได้รับการอนุมัติจากผู้บริหาร

ค) กำหนดวิธีการประเมินความเสี่ยงที่อาจเกิดขึ้นกับองค์กรโดยระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับเกณฑ์ในการยอมรับระดับความเสี่ยงตามข้อกำหนดของกฎหมายหรือหน่วยกำกับดูแลรวมทั้งวิธีประเมินความเสี่ยงที่เลือกใช้ต้องมั่นใจได้ว่าจะให้ผลลัพธ์ที่มีความทวนซ้ำได้

ง) บ่งชี้ความเสี่ยงโดยระบุทรัพย์สินที่อยู่ในขอบเขตของระบบบริหารจัดการความปลอดภัยรวมทั้งเจ้าของทรัพย์สินเหล่านั้น , ระบุภัยคุกคามที่มีต่อทรัพย์สิน, ระบุจุดอ่อนที่ก่อให้เกิดภัยคุกคามได้, ระบุผลกระทบที่ก่อให้เกิดความสูญเสียทางด้านความลับ ความถูกต้องครบถ้วนและความพร้อมใช้ของทรัพย์สินเหล่านั้น

จ) วิเคราะห์และประเมินความเสี่ยง โดยจัดให้มีการประเมินผลกระทบในการรักษาความมั่นคงปลอดภัยต่อองค์กรจากความล้มเหลวโดยพิจารณาผลของการสูญเสียความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น, ความน่าจะเป็นที่ก่อให้เกิดความเสี่ยงจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย, กำหนดระดับความเสี่ยงที่ยอมรับได้

ฉ) ระบุและประเมินทางเลือกการจัดการกับความเสี่ยงซึ่งอาจรวมถึงการใช้มาตรการควบคุม หรือยอมรับความเสี่ยงที่เกิดขึ้นแต่อยู่ภายใต้เกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้ หรือหลีกเลี่ยงความเสี่ยงเหล่านั้น หรือโอนย้ายความเสี่ยงไปสู่ผู้อื่นรับแทน เช่น บริษัทประกันภัย, ผู้ผลิต

ช) เลือกวัตถุประสงค์ของการควบคุมและควบคุมมาตรการทางด้านความมั่นคงปลอดภัยเพื่อจัดการกับความเสี่ยง

ซ)การเห็นชอบและยอมรับสำหรับความเสี่ยงที่ยังหลงเหลืออยู่

ฌ) การอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ

ญ) จัดทำ Statement of Applicability (SoA) ซึ่งจะประกอบไปด้วยวัตถุประสงค์และมาตรการตามที่เลือกไว้ในข้อ 4.2.1g รวมทั้งเหตุผลของการเลือกใช้งาน, วัตถุประสงค์และมาตรการที่ได้ใช้งานอยู่ในปัจจุบันและวัตถุประสงค์และมาตรการอื่นๆ ที่ไม่มีการใช้งานรวมทั้งเหตุผลที่ไม่มีการใช้งาน

4.2.2 การลงมือปฏิบัติและดำเนินงานตามระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Implement and operate the ISMS) - DO

ก) สร้างแผนการจัดการความเสี่ยงโดยระบุถึงการบริหารจัดการ ทรัพยากรที่ใช้ หน้าที่ความรับผิดชอบ และลำดับความสำคัญในการดำเนินการจัดการความเสี่ยง

ข) ปฏิบัติตามแผนเพื่อให้เป็นไปตามวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

ค) ปฏิบัติตามมาตรการที่เลือกไว้ในข้อ 4.2.1 เพื่อให้เป็นไปตามวัตถุประสงค์ดังกล่าว

ง) กำหนดวิธีในการวัดความประสิทธิผลของมาตรการที่เลือกมาใช้งาน เพื่อใช้ในการเปรียบเทียบผลเมื่อใช้มาตรการที่เหมือนเดิม

จ) อบรมและสร้างความตระหนักตามแผนที่กำหนดไว้

ฉ) บริหารการดำเนินงานตามระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับข้อมูล

ช) บริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

ซ) ปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ สามารถตรวจจับเหตุการณ์และตอบสนองได้ทันท่วงที

4.2.3 เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Monitor and review the ISMS) - CHECK

ก) เฝ้าระวังและทบทวนกระบวนงานและการควบคุมอื่นๆ เช่น ตรวจจับข้อผิดพลาดจากการประมวลผล, ช่วยให้ผู้บริหารสามารถระบุได้ว่ากิจกรรมทางด้านความมั่นคงปลอดภัยที่มอบหมายให้กับบุคลากรขององค์กรเป็นไปตามที่คาดหมายไว้หรือไม่

ข) ทบทวนความประสิทธิผลของระบบอย่างสม่ำเสมอ

ค) วัดประสิทธิผลของมาตรการว่าเป็นไปตามข้อกำหนดที่ตั้งไว้หรือไม่

ง) ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนด ทบทวนความเสี่ยงที่ยังเหลืออยู่และระดับความเสี่ยงที่ยอมรับได้ โดยพิจารณาการเปลี่ยนแปลงตามองค์ประกอบด้วยคือ องค์กร, เทคโนโลยี, วัตถุประสงค์และกระบวนการทางธุรกิจ, ภัยคุกคามที่ระบุไว้, ประสิทธิผลของมาตรการที่ปฏิบัติ และเหตุการณ์ภายนอก เช่นการเปลี่ยนแปลงทางด้านกฎหมาย เกณฑ์กำหนดด้านสิ่งแวดล้อม

จ) ดำเนินการตรวจสอบระบบภายในองค์กรตามรอบระยะเวลา

ฉ) ทบทวนระบบเพื่อให้มั่นใจว่าขอบเขตที่กำหนดเพียงพอต่อกระบวนการที่ได้ระบุไว้

ช) ปรับปรุงแผนโดยพิจารณาผลของการเฝ้าระวังและทบทวนกิจกรรม

ซ) บันทึกการดำเนินการหรือเหตุการณ์ที่อาจมีผลกระทบต่อความประสิทธิผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย

4.2.4 บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Maintain and improve the ISMS) - ACT

ก) ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ตามที่ระบุไว้

ข) ใช้มาตรการเชิงแก้ไขและป้องกันโดยประยุกต์จากประสบการณ์ที่ได้เรียนรู้ทางด้านความมั่นคงปลอดภัยขององค์กรเอง

ค) แจ้งการดำเนินการและการปรับปรุงให้แก่ทุกหน่วยที่เกี่ยวข้องโดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้นอาจเป็นข้อตกลงว่าควรปฏิบัติอย่างไร

ง) ตรวจสอบการปรับปรุงที่ได้ดำเนินการแล้วว่าบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

4.3 ข้อกำหนดทางด้านการจัดทำเอกสาร (Documentation requirments)

4.3.1 เอกสารที่จำเป็นต้องมีบันทึกแสดงการตัดสินใจของผู้บริหารเพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามที่คาดหวังและตรงตามข้อกำหนดเพื่อให้มั่นใจว่าผลที่ได้สามารถนำมาเทียบเคียงกันได้ โดยเอกสารจะต้องประกอบด้วย นโยบายความมั่นคงปลอดภัยและวัตถุประสงค์สนับสนุนระบบ, วิธีการประเมินความเสี่ยง, รายงานผลการประเมินความเสี่ยง, แผนการจัดการความเสี่ยง, ขั้นตอนการปฏิบัติที่เกี่ยวข้องเพื่อให้เป็นไปตามแผนที่วางไว้ รวมทั้งวิธีการวัดความประสิทธิผลของมาตรการ, สิ่งที่ต้องบันทึกไว้ที่กำหนดในมาตรฐานนี้ และ เอกสารแสดงการใช้งานมาตรการ

4.3.2 เอกสารตามข้อกำหนดจะต้องได้รับการป้องกันและควบคุม มีขั้นตอน ดังนี้

ก) อนุมัติก่อนการใช้งานเอกสาร

ข) ทบทวน ปรับปรุง และอนุมัติเอกสารตามความจำเป็น

ค) ระบุการเปลี่ยนแปลงและสถานภาพของเอกสารที่เป็นปัจจุบัน

ง) กำหนดฉบับที่ของเอกสารและมั่นใจว่ามีอยู่ในจุดใช้งาน

จ) มั่นใจว่าเอกสารที่จัดทำขึ้นสามารถทำความเข้าใจ และบ่งชี้ได้ง่าย

ฉ) มั่นใจว่าเอกสารมีพร้อมใช้งาน รวมทั้งการโอนย้าย การจัดเก็บ และการทำลายจะต้องเป็นไปตามขั้นตอนปฏิบัติที่จัดทำไว้สำหรับเอกสารชนิดนั้นๆ

ช) ระบุว่าเอกสารใดเป็นเอกสารจากภายนอก

ซ) การแจกจ่ายเอกสารมีการควบคุม

ฌ) ป้องกันการใช้เอกสารที่เลิกใช้งานแล้ว

ญ) มีการระบุเอกสารที่เหมาะสมหรือมีความจำเป็นต่อไปถึงแม้ว่าเป็นเอกสารล้าสมัยแล้วแต่ยังคงเก็บไว้เพื่อจุดประสงค์ใดๆ

4.3.3 การควบคุมการบันทึก

องค์กรจะต้องมีการกำหนดและดูแลรักษาบันทึก เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย โดยบันทึกจะจำเป็นต้องมีมาตรการระบุตัวตน การจัดเก็บ การป้องกัน การนำกลับมาใช้ การรักษา และการทำลาย

โปรดติดตามข้อ 5- 8 ในฉบับต่อไป

เอกสารอ้างอิง

1. International Standard ISO/IEC 27001: 2005 (First edition)
2. http://en.wikipedia.org/wiki/ISO/IEC_27001 (เข้าถึง วันที่ 12 มีนาคม 2555)
3. หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550