บทความเรื่อง : หัวใจหลักของกระบวนการระบบบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001

เรียบเรียงโดย : บรรจง หะรังษี

เรียบเรียงเมื่อ : วันที่ 24 มิถุนายน 2554

บทความนี้มีจุดประสงค์เพื่ออธิบายหัวใจหลักของกระบวนการระบบบริหารจัดการด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 ซึ่งประกอบด้วย 4 ขั้นตอนหลัก กล่าวคือ

- การวางแผน (Plan)
- การดำเนินการตามแผน (Do)
- การเฝ้าระวังและติดตามการดำเนินการตามแผน (Check)
- การดำเนินการเพิ่มเติมตามที่เห็นสมควร (Act)

แม้ในข้อกำหนดหลักของมาตรฐาน ISO/IEC 27001 ซึ่งคือข้อ

4.2.1 Establish the ISMS (เทียบเท่ากับ Plan)

4.2.2 Implement and operate the ISMS (เทียบเท่ากับ Do)

4.2.3 Monitor and review the ISMS (เทียบเท่ากับ Check)

4.2.4 Maintain and Improve the ISMS (เทียบเท่ากับ Act)

ตามลำดับจะมีรายละเอียดปลีกย่อยอยู่มากมายก็ตาม แต่เมื่อพิจารณาแล้วหัวใจหลักของทั้ง 4 ข้อนั้นคือการประเมินความเสี่ยงและการจัดทำแผนการลดความเสี่ยง (หรือก็คือขั้นตอนการวางแผน--Plan) การดำเนินการตามแผนการลดความเสี่ยง (หรือก็คือขั้นตอนการดำเนินการตามแผน -- Do) การเฝ้าระวังและติดตามการดำเนินการตามแผน (หรือก็คือขั้นตอนการเฝ้าระวังและติดตามการดำเนินการตามแผน--Check) และการดำเนินการเพิ่มเติมตามที่เห็นสมควร (หรือก็คือขั้นตอนการดำเนินการเพิ่มเติมตามที่เห็นสมควร--Act) เช่น กรณีที่พบว่ายังมีความเสี่ยงที่ต้องบริหารจัดการอยู่

ก่อนอื่นขออธิบายคำจำกัดความที่สำคัญๆ ที่เกี่ยวข้องกับความเสี่ยงที่ใช้ในบทความนี้ ดังนี้

เหตุการณ์ความเสี่ยง หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศขององค์กร เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกขโมยซึ่งอาจทำให้องค์กรสูญเสียข้อได้เปรียบด้านการแข่งขัน หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสียง

การประเมินความเสี่ยง (Risk assessment) หมายถึง การกำหนดเหตุการณ์ความเสี่ยงที่มีโอกาศเกิดขึ้นได้ กำหนดระดับของผลกระทบหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง และกำหนดค่าความเสี่ยงของเหตุการณ์ความเสี่ยงนั้น การประเมินความเสี่ยงมีจุดประสงค์เพื่อคาดการณ์ว่ามีเหตุการณ์ความเสี่ยงใดบ้างที่เกี่ยวข้องกับทรัพย์สินสารสนเทศหนึ่ง และมีระดับความเสี่ยงมากน้อยเพียงใด ทั้งนี้เพื่อจะได้เตรียมการป้องกันไว้ก่อนก่อนที่เหตุการณ์ความเสี่ยงนั้นจะเกิดขึ้นจริงและทำให้องค์กรเกิดความเสียหาย

ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk) หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่งมีค่าน้อยกว่าค่าที่ยอมรับได้นี้ จะถือว่าทรัพย์สินสารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ (และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม)

แผนการลดความเสี่ยง (Risk treatment plan) หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานเพื่อพิจารณาอนุมัติก่อนดำเนินการ ในบทความนี้ขออธิบายเฉพาะในส่วนที่เป็นหัวใจหลักของทั้ง 4 ข้อดังกล่าว ดังนี้

การวางแผน (Plan)

ขั้นตอนที่หนึ่งคือการวางแผนหรือ Plan ซึ่งเป็นการประเมินความเสี่ยงที่มีต่อทรัพย์สินสารสนเทศ ซึ่งส่วนใหญ่จะหมายถึงทรัพย์สินสารสนเทศใหม่ที่กำลังนำเข้ามาสู่การใช้งาน ที่จะต้องมีการประเมินความเสี่ยงเพื่อเตรียมการป้องกันก่อนเริ่มต้นใช้งานทรัพย์สินใหม่เหล่านั้น เช่น กรณีมีโครงการจัดทำระบบงาน E-mail ที่ต้องดำเนินการให้แล้วเสร็จในปีงบประมาณนี้ ทรัพย์สินสารสนเทศใหม่ของโครงการนี้อาจประกอบด้วย

- ระบบงาน E-mail
- ฮาร์ดแวร์ของระบบงาน E-mail
- ซอฟต์แวร์ต่างๆ ของระบบงาน E-mail เช่น ระบบปฏิบัติการ Windows 2008

เป็นต้น

ณ ที่นี้ขอยกตัวอย่างการประเมินความเสี่ยงโดยใช้ทรัพย์สินสารสนเทศระบบงาน E-mail

ตัวอย่างของเหตุการณ์ความเสี่ยงที่เกี่ยวข้องกับระบบงาน E-Mail ได้แก่

- เหตุการณ์ความเสี่ยงที่ 1: ความเสี่ยงของการไม่ได้มีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบงานโดยพิจารณาจากความเสี่ยงที่มีต่อระบบงานและกำหนดมาตรการรองรับหรือลดความเสี่ยงเหล่านั้น
- เหตุการณ์ความเสี่ยงที่ 2: ความเสี่ยงของการไม่ได้มีการวิเคราะห์และออกแบบระบบโดยคำนึงถึงการตรวจสอบข้อมูลนำเข้า (Input) ระบบงานเพื่อป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุกต่างๆ ดังต่อไปนี้
  - SQL injection
  - Crosssite scripting
  - การรับไฟล์ประเภทที่ไม่ประสงค์ดีเข้ามาในระบบงาน เช่น ไฟล์ที่เป็นไวรัส หรือเป็นไฟล์โปรแกรมที่แอบทำงานอย่างอื่นแอบแฝง เป็นต้น
- เหตุการณ์ความเสี่ยงที่ 3: ความเสี่ยงของการไม่ได้มีการวิเคราะห์และกำหนดประเภทของกิจกรรมสำคัญต่างๆ สำหรับการเข้าถึงหรือการใช้ระบบงานโดยที่กิจกรรมเหล่านั้นอาจมีความจำเป็นต้องตรวจสอบในภายหลัง เช่น

- การล็อกอินเข้าใช้งานระบบ
- การออกจากระบบ เป็นต้น

- เหตุการณ์ความเสี่ยงที่ 4: ความเสี่ยงของการไม่ได้มีการวิเคราะห์และออกแบบระบบโดยกำหนดกลุ่มผู้ใช้งานของระบบงานทั้งหมด บทบาท และ/หรือ สิทธิการเข้าถึงของผู้ใช้งานเหล่านั้นให้ชัดเจน
- เหตุการณ์ความเสี่ยงที่ 5: ความเสี่ยงของการที่ระบบงานไม่สามารถตัดหรือหมดเวลาการใช้งานหลังจากที่เข้าระบบงานมาแล้วและไม่ได้ใช้งานหรือมีกิจกรรมกับระบบเกินกว่าช่วงระยะเวลาหนึ่งที่ได้กำหนดไว้

เมื่อได้ระบุความเสี่ยงที่เกี่ยวข้องกับระบบงาน E-mail แล้วตามตัวอย่างข้างต้น จากนั้นจึงทำการวางแผนเพื่อจัดการกับความเสี่ยงดังกล่าว ขออนุญาตข้ามขั้นตอนการประเมินว่าแต่ละรายการมีความเสี่ยงแค่ไหนไปสู่ขั้นตอนการวางแผนการลดความเสี่ยง แผนการที่เตรียมการไว้โดยสังเขปประกอบด้วย

- จัดทำข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบงานให้ชัดเจนและกำหนดให้ผู้พัฒนาพัฒนาตามข้อกำหนดดังกล่าว
- ออกแบบระบบให้คำนึงถึงการตรวจสอบข้อมูลนำเข้า (Input) ระบบงานเพื่อป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุกต่างๆ ดังต่อไปนี้
  - SQL injection
  - Crosssite scripting
- ออกแบบระบบให้สามารถบันทึกกิจกรรมสำคัญต่างๆ สำหรับการเข้าถึงหรือการใช้ระบบงานโดยที่กิจกรรมเหล่านั้นอาจมีความจำเป็นต้องตรวจสอบในภายหลัง ซึ่งประกอบด้วย
  - การล็อกอินเข้าใช้งานระบบ
  - การออกจากระบบ
- ออกแบบระบบโดยกำหนดกลุ่มผู้ใช้งานของระบบงานทั้งหมด บทบาท และ/หรือ สิทธิการเข้าถึงของผู้ใช้งานเหล่านั้นให้ชัดเจน
- ออกแบบระบบให้สามารถตัดหรือหมดเวลาการใช้งานหลังจากที่เข้าระบบงานมาแล้วและไม่ได้ใช้งานหรือมีกิจกรรมกับระบบเกินกว่า 5 นาที

การดำเนินการตามแผน (Do)

ขั้นตอนถัดไปคือการดำเนินการตามแผน หรือ Do ที่ได้กำหนดไว้ทั้งหมดในข้างต้น กล่าวคือการพัฒนาระบบงาน E-Mail ตามแผนการที่เตรียมไว้ในข้างต้นทั้งหมด

การเฝ้าระวังและติดตามการดำเนินการตามแผน (Check)

ขั้นตอนการติดตามการดำเนินการตามแผน หรือ Check คือการติดตามเพื่อดูว่าการพัฒนาระบบงาน E-Mail ทำตามแผนครบทั้งหมดและได้ผลลัพธ์ที่ถูกต้องหรือไม่ กล่าวคือ

- ระบบงานต้องทำงานได้ครบถ้วนตามข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้
- ระบบงานต้องสามารถป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุกต่างๆ ดังต่อไปนี้

- SQL injection
- Crosssite scripting

- ระบบงานต้องสามารถบันทึกกิจกรรมสำคัญต่างๆ สำหรับการเข้าถึงหรือการใช้ระบบงานซึ่งประกอบด้วย
  - การล็อกอินเข้าใช้งานระบบ
  - การออกจากระบบ
- ระบบงานต้องมีกลุ่มผู้ใช้งาน บทบาท และ/หรือ สิทธิการเข้าถึงของผู้ใช้งานเหล่านั้นอย่างชัดเจน และสามารถควบคุมการเข้าถึงระบบได้ตามสิทธิที่ได้รับ
- ระบบงานต้องสามารถตัดหรือหมดเวลาการใช้งานหลังจากที่เข้าระบบงานมาแล้วและไม่ได้ใช้งานหรือมีกิจกรรมกับระบบเกินกว่า 5 นาที

การดำเนินการเพิ่มเติมตามที่เห็นสมควร (Act)

หากเมื่อ Check ในทุกรายการแล้วและพบปัญหาที่ต้องทำการแก้ไข ให้ดำเนินการเพิ่มเติมตามที่เห็นสมควร (Act) เช่น กรณีพบว่าระบบงานยังไม่รองรับปัญหาการบุกรุกระบบ SQL Injection ให้ดำเนินการแก้ไข (Take action) เพื่อให้ระบบสามารถจัดการกับปัญหานี้ได้

การเฝ้าระวังและติดตามการดำเนินการตามแผนและการดำเนินการเพิ่มเติมตามที่เห็นสมควร

ความเสี่ยงทั้ง 5 รายการแม้จะได้มีการการเฝ้าระวังและติดตามเพื่อลดความเสี่ยงในระหว่างที่ระบบบงาน E-Mail ยังอยู่ในระหว่างการพัฒนาแล้วก็ตาม ภายหลังจากระบบงานพัฒนาแล้วเสร็จและติดตั้งให้บริการไปแล้ว ก็ควรที่จะเฝ้าระวังและติดตามต่อไป ตัวอย่างของการเฝ้าระวังและติดตาม เช่น

สำหรับเหตุการณ์ความเสี่ยงที่ 1: ดูว่ากรณีที่มีการปรับปรุงระบบงาน E-Mail เพิ่มเติม ได้มีการระบุข้อกำหนดความต้องการด้านความมั่นคงปลอดภัยใหม่ที่ควรเพิ่มเติมเข้าไปแล้ว หรือไม่

สำหรับเหตุการณ์ความเสี่ยงที่ 2: ดูว่ากรณีที่มีการปรับปรุงระบบงาน E-Mail เพิ่มเติม ได้มีการ วิเคราะห์และออกแบบระบบเพื่อป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุกต่างๆ ดังกล่าวแล้วหรือไม่

สำหรับเหตุการณ์ความเสี่ยงที่ 3: ดูว่ากรณีที่มีการปรับปรุงระบบงาน E-Mail เพิ่มเติม ได้มีการวิเคราะห์และกำหนดประเภทของกิจกรรมเพิ่มเติมที่จำเป็นแล้วหรือไม่ โดยที่กิจกรรมเหล่านั้นอาจมีความจำเป็นต้องตรวจสอบในภายหลัง

สำหรับเหตุการณ์ความเสี่ยงที่ 4: ดูว่ากรณีที่มีการปรับปรุงระบบงาน E-Mail เพิ่มเติม ได้มีการ การวิเคราะห์และออกแบบระบบในส่วนของกลุ่มผู้ใช้งานใหม่ บทบาท และ/หรือ สิทธิการเข้าถึงของผู้ใช้งานเหล่านั้นแล้วหรือไม่

หากมีความเสี่ยงใหม่หรือเพิ่มเติมอันเกิดจากการเฝ้าระวังและติดตาม เช่น

- ยังไม่ได้วางแผนรองรับข้อกำหนดความต้องการด้านความมั่นคงปลอดภัยใหม่
- ยังไม่ได้วางแผนรองรับปัญหาที่เกี่ยวข้องกับการบุกรุกระบบต่างๆ สำหรับระบบงานที่ปรับปรุงเพิ่มเติม
- ยังไม่ได้วางแผนรองรับกิจกรรมเพิ่มเติมที่ต้องมีการบันทึกเก็บไว้

ก็ยังถือว่ายังมีความเสี่ยงใหม่หรือเพิ่มเติมอยู่ ดังนั้นจึงต้องวางแผนการลดความเสี่ยงเพิ่มเติม หรือ Take action (ซึ่งก็คือการดำเนินการเพิ่มเติมตามที่เห็นสมควรนั่นเอง)

โดยสรุปวงจรชีวิต Plan Do Check Act นี้จึงก่อเกิดนับตั้งแต่เริ่มมีทรัพย์สินสารสนเทศใหม่ที่กำลังถูกนำเข้ามาใช้งานกับองค์กร จากนั้นแม้ว่าจะมีการติดตั้งและใช้งานทรัพย์สินเหล่านั้นไปแล้วก็ตาม ก็ยังคงต้อง Check และ Act อย่างต่อเนื่อง (กล่าวคือ ประเมินความเสี่ยงเพิ่มเติมตามความจำเป็น) จวบจนกระทั่งทรัพย์สินเหล่านั้นจะสิ้นสุดอายุขัยหรือหมดอายุการใช้งานนั่นเอง จึงยุติการประเมินความเสี่ยงสำหรับทรัพย์สินเหล่านั้น

อย่างไรก็ตามหลายครั้งเมื่อทรัพย์สินสารสนเทศหนึ่งหมดอายุขัยการใช้งาน เช่น กรณีเทคโนโลยีสารสนเทศระบบงาน E-Mail หนึ่งจะมีอายุขัยการใช้งานระหว่าง 3-7 ปี ทรัพย์สินสารสนเทศเดียวกันแต่เป็นของใหม่ เช่น ระบบงาน E-Mail ซึ่งเป็นเทคโนโลยีสารสนเทศใหม่ก็จะถูกนำมาเปลี่ยนทดแทนแทนเทคโนโลยีของระบบเดิม แต่ถึงกระนั้นก็ตามทรัพย์สินใหม่นั้นก็ต้องเข้าสู่วงจรชีวิต Plan Do Check Act อีกครั้งเช่นเดียวกับการประเมินความเสี่ยงในข้างต้น ดังนั้นจึงเห็นได้ว่าวงจรชีวิตดังกล่าวจึงมีการไหลอย่างต่อเนื่องและไม่มีที่สิ้นสุด