บทความเรื่อง : Plan-Do-Check-Act ตามมาตรฐาน ISO/IEC 27001 กับข้อคำถามสำคัญที่ต้องการคำตอบ

เรียบเรียงโดย : บรรจง หะรังษี

เรียบเรียงเมื่อ : วันที่ 24 มิถุนายน 2554

บทความนี้มีจุดประสงค์ต้องการแสดงให้เห็นวงจรการบริหารและจัดการความเสี่ยงตามมาตรฐาน ISO/IEC 27001 และข้อคำถามสำคัญต่อวงจรดังกล่าวที่ต้องการคำตอบที่ชัดเจน บทความจะเริ่มต้นจากการอธิบายวงจรการบริหารและจัดการความเสี่ยงและตามด้วยข้อคำถามสำคัญดังกล่าว

วงจรการบริหารและจัดการความเสี่ยงประกอบด้วย 4 ขั้นตอนดังนี้

- การวางแผน (Plan)
- การดำเนินการตามแผน (Do)
- การเฝ้าระวัง ตรวจสอบ และติดตามการดำเนินการ (Check)
- การดำเนินการเพิ่มเติมตามที่เห็นสมควร (Act)

ข้อกำหนดหลักในมาตรฐาน ISO/IEC 27001 ที่สอดคล้องกับวงจรดังกล่าวคือ

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)

แต่ละข้อมีความสอดคล้องกับ Plan-Do-Check-Act ตามลำดับ โดยสรุปแล้วข้อกำหนดหลักดังกล่าวกล่าวถึงวงจรการบริหารและจัดการความเสี่ยงดังนี้

- ขั้นตอนการ **Plan** ได้กล่าวถึงการระบุและประเมินความเสี่ยงและการกำหนดทางเลือกในการจัดการกับความเสี่ยง
- ขั้นตอนการ **Do** ได้กล่าวถึงการจัดทำแผนการลดความเสี่ยง (Risk treatment plan) และการดำเนินการตามแผนดังกล่าว
- ขั้นตอนการ **Check** ได้กล่าวถึง 2 ประเด็นหลักที่เกี่ยวข้องกับความเสี่ยงดังนี้

- ประเด็นที่ 1 คือการเฝ้าระวังและทบทวนเพื่อดูว่าความเสี่ยงที่ประเมินไว้ได้กลายเป็นจริงหรือไม่ ได้แก่
  - การเฝ้าระวังเพื่อดูว่ามีความผิดพลาดหรือข้อผิดพลาดจากการประมวลผลหรือไม่
  - การเฝ้าระวังเพื่อดูว่ามีการละเมิดข้อกำหนดที่จัดทำไว้หรือไม่ ทั้งในส่วนของการใช้หรือมีความพยายามที่จะละเมิด หรือได้มีการละเมิดเกิดขึ้นแล้วก็ตาม
  - การเฝ้าระวังเพื่อดูว่ามีเหตุการณ์ด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่ ทั้งในส่วนของการใช้ความพยายามที่จะก่อให้เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย หรือได้มีเหตุการณ์ด้านความมั่นคงปลอดภัยเกิดขึ้นแล้วก็ตาม
  - การเฝ้าระวังเพื่อดูว่ากิจกรรมที่มอบหมายให้ดำเนินการหรือที่มีการใช้ไอซีทีเป็นไปตามที่คาดหมายหรือที่ต้องการหรือไม่
  - การเฝ้าระวังเพื่อตรวจหาว่ามีเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยเกิดขึ้นหรือไม่ โดยการใช้ตัวชี้วัดต่างๆ มาเป็นเครื่องมือช่วยในการตรวจหา ทั้งนี้เพื่อจะได้ดำเนินการป้องกันไว้ก่อน
- ประเด็นที่ 2 คือการพิจารณาทบทวนผลการประเมินความความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้ (โดยนำข้อมูลจากหลายๆ แหล่งมาพิจารณา) และการทบทวนความเสี่ยงที่เหลืออยู่และระดับความเสี่ยงที่ยอมรับได้

- ขั้นตอนการ **Act** ได้กล่าวถึงการดำเนินการปรับปรุงแก้ไขตามที่ได้ระบุไว้ (ในขั้นตอน Check) รวมถึงการดำเนินการเชิงแก้ไข (เช่น เกิดจากความไม่สอดคล้องกับข้อกำหนดตามมาตรฐาน ISO/IEC 27001) และการดำเนินการเชิงป้องกัน (เช่น พบเหตุการณ์ความเสี่ยงใหม่ที่ต้องทำการป้องกัน)

ข้อคำถามที่เกี่ยวข้องกับขั้นตอนดังกล่าวและต้องการคำอธิบายที่ชัดเจนมากขึ้นเพื่อให้สามารถประเมินความเสี่ยงได้อย่างถูกต้องมากขึ้น มีดังนี้

- <u>ข้อคำถามที่ 1</u> ขั้นตอนการ Plan: ในการระบุความเสี่ยงต่อทรัพย์สินหนึ่ง มาตรฐาน ISO/IEC 27001 ได้กำหนดให้มีการระบุภัยคุกคามและจุดอ่อนที่มีต่อทรัพย์สินนั้น บางภัยคุกคามต่อทรัพย์สินหนึ่ง เช่น ไวรัสที่เกิดจากจุดอ่อน “การไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส” หากจุดอ่อนดังกล่าวไม่ได้เป็นจุดอ่อน กล่าวคือตอนที่ประเมินความเสี่ยง พบว่า “ได้มีการติดตั้งโปรแกรมป้องกันไวรัสแล้ว” ต้องประเมินความเสี่ยงกรณีนี้หรือไม่ และจะประเมินอย่างไร ความเสี่ยงในลักษณะนี้ถือว่ามีระดับความเสี่ยงที่ยอมรับได้หรือไม่
- <u>ข้อคำถามที่ 2</u> ขั้นตอนการ Plan: การประเมินความเสี่ยงต้องประเมินพร้อมกันทีเดียว ประเมินแยกกันเป็นแต่ละครั้ง หรือเป็นกรณีอื่นๆ เช่น สมมติว่าองค์กรต้องการวางแผนจัดทำระบบงานใหม่ ซึ่งอาจมีความเสี่ยงหลายๆ รายการดังนี้

- ความเสี่ยงค่าใช้จ่ายในการบำรุงรักษาระบบงานในระยะยาวค่อนข้างสูง/การไม่ได้มีการวิเคราะห์และกำหนดทางเลือกในการพัฒนาระบบงานให้เหมาะสมต่อการใช้งาน
- ความเสี่ยงการเกิดข้อพิพาธ ข้อขัดแย้ง หรือข้อถกเถียงในการตรวจรับระบบงาน/การไม่ได้กำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน
- ความเสี่ยงระบบงานที่ได้รับไม่ตรงตามความต้องการขององค์กร/การไม่ได้กำหนดรายละเอียดทางเทคนิคของระบบงาน
- ความเสี่ยงระบบงานไม่มีผู้รับผิดชอบชัดเจนเมื่อเกิดปัญหา/การไม่ได้กำหนดว่าใครเป็นเจ้าของระบบงาน ใครเป็นเจ้าของข้อมูลในระบบงาน ใครเป็นผู้ดูแลระบบ ใครเป็นเจ้าของซอฟต์แวร์ต่างๆ ของระบบงาน
- ความเสี่ยงระบบงานไม่ปลอดภัยเพียงพอ/การไม่ได้กำหนดให้มีระบุความต้องการด้านความมั่นคงปลอดภัยของระบบงานโดยพิจารณาจากความเสี่ยงที่มีต่อระบบงาน
- ความเสี่ยงระบบงานถูกบุกรุก/การไม่ได้มีการวิเคราะห์และออกแบบระบบโดยคำนึงถึงการตรวจสอบข้อมูลนำเข้า (Input) ระบบงานเพื่อป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุก
- ความเสี่ยงปัญหาการใช้งานมีการแก้ไขโดยใช้เวลานานเกินไป/การไม่ได้มีการกำหนดขั้นตอนปฏิบัติที่ชัดเจนในการแก้ไขปัญหาการใช้งาน โดยที่ขั้นตอนฯ ต้องคำนึงถึงระยะเวลาในการแก้ไขปัญหาที่เหมาะสมด้วย

จากความเสี่ยงทั้งหมด ผู้ประเมินความเสี่ยงควรประเมินพร้อมกันทีเดียวทั้งหมดเลย หรือประเมินแยกกันเป็นแต่ละครั้ง เช่น ในช่วงวางแผนจัดทำระบบงานใหม่ ความเสี่ยงที่เกี่ยวข้องที่ต้องประเมินและจัดการอาจเป็น

- ความเสี่ยงค่าใช้จ่ายในการบำรุงรักษาระบบงานในระยะยาวค่อนข้างสูง/การไม่ได้มีการวิเคราะห์และกำหนดทางเลือกในการพัฒนาระบบงานให้เหมาะสมต่อการใช้งาน
- ความเสี่ยงการเกิดข้อพิพาธ ข้อขัดแย้ง หรือข้อถกเถียงในการตรวจรับระบบงาน/การไม่ได้กำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน
- ความเสี่ยงระบบงานที่ได้รับไม่ตรงตามความต้องการขององค์กร/การไม่ได้กำหนดรายละเอียดทางเทคนิคของระบบงาน
- ความเสี่ยงระบบงานไม่มีผู้รับผิดชอบชัดเจนเมื่อเกิดปัญหา/การไม่ได้กำหนดว่าใครเป็นเจ้าของระบบงาน ใครเป็นเจ้าของข้อมูลในระบบงาน ใครเป็นผู้ดูแลระบบ ใครเป็นเจ้าของซอฟต์แวร์ต่างๆ ของระบบงาน

และในช่วงของการจัดหาระบบใหม่ ความเสี่ยงที่เกี่ยวข้องที่ต้องประเมินและจัดการอาจเป็น

- ความเสี่ยงระบบงานไม่ปลอดภัยเพียงพอ/การไม่ได้กำหนดให้มีระบุความต้องการด้านความมั่นคงปลอดภัยของระบบงานโดยพิจารณาจากความเสี่ยงที่มีต่อระบบงาน
- ความเสี่ยงระบบงานถูกบุกรุก/การไม่ได้มีการวิเคราะห์และออกแบบระบบโดยคำนึงถึงการตรวจสอบข้อมูลนำเข้า (Input) ระบบงานเพื่อป้องกันปัญหาที่เกี่ยวข้องกับการบุกรุก

- ข้อคำถามที่ 3 ขั้นตอนการ Plan: การประเมินความเสี่ยงต้องดำเนินการประเมินเมื่อไร เช่น เมื่อมีทรัพย์สินใหม่เกิดขึ้น เมื่อทรัพย์สินมีการเปลี่ยนแปลง หรือเป็นกรณีอื่นๆ ผู้ประเมินความเสี่ยงบางท่านมีความเข้าใจว่าควรทำปีละ 1- 2 ครั้ง
- ข้อคำถามที่ 4 ขั้นตอนการ Check: ในส่วนของ “การเฝ้าระวังเพื่อดูว่ากิจกรรมที่มอบหมายให้ดำเนินการหรือที่มีการใช้ไอซีทีเป็นไปตามที่คาดหมายหรือที่ต้องการหรือไม่” คำว่า “กิจกรรมที่มอบหมายให้ดำเนินการ” หมายถึงกิจกรรมอะไร ใช่เป็นกิจกรรมตามนโยบายหรือขั้นตอนปฏิบัติหรือไม่ หรือเป็นกิจกรรมตามแผนการลดความเสี่ยงหรือกิจกรรมอื่นๆ

ผู้เขียนมีความเห็นว่าควรมีการให้ความกระจ่างในข้อคำถามทั้งหมดในข้างต้น และให้แนวทางหรือวิธีการประเมินความเสี่ยงที่ชัดเจนมากกว่าตามที่ปรากฏในมาตรฐาน ISO/IEC 27001 ทั้งนี้เพื่อให้ผู้ประเมินความเสี่ยงสามารถปฏิบัติตามวงจรการบริหารและจัดการความเสี่ยงได้อย่างถูกต้องมากขึ้นและตามแนวทางที่จะนำเสนอต่อไป จะมีความเป็นระบบระเบียบมากยิ่งขึ้นในการประเมินความเสี่ยง

บทความตอนต่อๆ ไปจะเริ่มไขข้อคำถามเหล่านั้นทีข้อคำถามเรียงตามลำดับไป จนกระทั่งสุดท้ายจะนำเสนอวงจร Plan-Do-Check-Act ที่เสนอปรับปรุงใหม่แต่ยังครอบคลุมของเดิมทุกประการ