บทความเรื่อง : Plan-Do-Check-Act ตามมาตรฐาน ISO/IEC 27001 กับข้อคำถามสำคัญที่ต้องการคำตอบ : ตอน ตอบข้อคำถามที่ 1

เรียบเรียงโดย : บรรจง หะรังษี

เรียบเรียงเมื่อ : วันที่ 29 กรกฎาคม 2554

บทความนี้มีจุดประสงค์ต้องการไขความกระจ่างสำหรับคำถามที่เกิดขึ้นในบทความ “Plan-Do-Check-Act ตามมาตรฐาน ISO/IEC 27001 กับข้อคำถามสำคัญที่ต้องการคำตอบ” โดยบทความนี้จะตอบข้อคำถามที่ 1 ที่ว่า หากจุดอ่อนหนึ่งไม่ได้เป็นจุดอ่อน กล่าวคือตอนที่ประเมินความเสี่ยง พบว่า “มีการปฏิบัติที่ดีซึ่งหักล้างกับจุดอ่อนนั้น” ต้องประเมินความเสี่ยงกรณีนี้หรือไม่ และจะประเมินอย่างไร

จุดอ่อนของเหตุการณ์ความเสี่ยงและ Best practice

การกำหนดเหตุการณ์ความเสี่ยงคือการระบุภัยคุกคามและจุดอ่อนที่ภัยคุกคามสามารถใช้ให้เป็นประโยชน์ และส่งผลให้เหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง ประเด็นสำคัญในการกำหนดเหตุการณ์ความเสี่ยงคือการตรวจสอบว่าองค์กรยังมีจุดอ่อนใดๆ อยู่หรือไม่ (ซึ่งจะส่งผลให้ความเสี่ยงหนึ่งเกิดขึ้นได้จริง) โดยทั่วไปจากประสบการณ์ด้านไอซีทีโดยเฉพาะอย่างยิ่งกับการรักษาความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27002 พอจะกล่าวได้ว่าจุดอ่อนมักจะหมายถึงสิ่งที่ควรทำหรือปฏิบัติ (Best practice ซึ่งแปลเป็นไทยว่าสิ่งที่ควรปฏิบัติอยู่เสมอ) แต่ยังไม่ได้ปฏิบัติเลยหรือยังปฏิบัติไม่ดีพอ หรือพอจะกล่าวได้ว่าจุดอ่อนเป็นสิ่งที่ตรงกันข้ามกับ Best practice ก็ได้ หากสามารถระบุจุดอ่อนต่างๆ ได้อย่างมากมายและครอบคลุม จะหมายถึงว่าผู้ประเมินความเสี่ยงก็อาจจะสามารถจัดการกับความเสี่ยงต่างๆ เหล่านั้นได้อย่างมากมายและครอบคลุมเช่นกัน

ประเด็นถัดมาคือแล้วจะรู้ได้อย่างไรว่าองค์กรมีจุดอ่อนอะไรบ้าง คำตอบโดยหลักการคือทางหนึ่งที่เป็นไปได้คือการนำ Best practice ด้านไอซีที เช่น ของ ITIL หรือด้านการรักษาความมั่นปลอดภัยของ ISO/IEC 27002 มาพิจารณาเพื่อดูว่ามีประเด็นใดบ้างที่ยังไม่ได้ปฏิบัติเลยหรือยังปฏิบัติไม่ดีพอ ประเด็นเหล่านี้จะนำสู่ความเสี่ยงที่ต้องมีการบริหารและจัดการเพิ่มเติมต่อไป

ประเด็นดังต่อไปนี้เป็น Best practice ที่นำมาจาก ISO/IEC 27002

- การจัดทำสัญญาห้ามเปิดเผยข้อมูลสำคัญขององค์กร
- การกำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน
- การกำหนดอย่างชัดเจนว่าใครเป็นเจ้าของทรัพย์สินสารสนเทศ เช่น ใครเป็นเจ้าของ ระบบงาน ใครเป็นเจ้าของข้อมูลในระบบงาน ใครเป็นเจ้าของซอฟต์แวร์ต่างๆ ของระบบงาน เป็นต้น
- การระบุความต้องการด้านความมั่นคงปลอดภัยของระบบงานที่จะทำการพัฒนาขึ้นมา
- การวิเคราะห์และออกแบบระบบโดยคำนึงถึงการตรวจสอบข้อมูลนำเข้า (Input) ให้มีความถูกต้องและเชื่อถือได้

- การรายงานปัญหาการใช้งานและการจัดการภายในระยะเวลาอันสมควร

ประเด็นเหล่านี้หากยังไม่ได้ปฏิบัติเลยหรือยังปฏิบัติไม่ดีพอก็อาจเป็นจุดอ่อนสำคัญขององค์กร ซึ่งอาจส่งผลให้ความเสี่ยงเกิดขึ้นจริงและสร้างความเสียหายให้แก่องค์กรได้ เช่น

- ความเสี่ยงข้อมูลลับหรือข้อมูลสำคัญขององค์กรถูกเปิดเผยโดยไม่ได้รับอนุญาต/การไม่ได้กำหนดให้มีการจัดทำสัญญาห้ามเปิดเผยข้อมูลสำคัญขององค์กร
- ความเสี่ยงการเกิดข้อพิพาท ข้อขัดแย้ง หรือข้อถกเถียงในการตรวจรับระบบงาน/การไม่ได้กำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน

เป็นต้น

ISO/IEC 27002 ได้รวบรวม Best practice ด้านการรักษาความมั่นคงปลอดภัยไว้โดยแยกเป็นมาตรการความมั่นคงปลอดภัย (Control) จำนวน 133 ข้อ ดังนั้นการจะค้นหาจุดอ่อนต่างๆ ขององค์กรสามารถพิจารณาจากมาตรการดังกล่าวได้

อย่างไรก็ตาม Best practice ในมาตรฐาน ISO/IEC 27002 ก็ไม่ได้ครอบคลุมในอีกหลายๆ เรื่อง อาทิ

- การวิเคราะห์และกำหนดทางเลือกในการพัฒนาระบบงานให้เหมาะสมต่อการใช้งานในระยะยาว เช่น
  - การจัดหาซอฟต์แวร์สำเร็จรูปมาใช้งานสำหรับกรณีที่มีซอฟต์แวร์ขายอยู่แล้วในตลาดและสอดคล้องกับความต้องการใช้งาน
  - การจ้างพัฒนาระบบงานสำหรับกรณีที่ไม่มีซอฟต์แวร์ขายในตลาดหรือไม่สอดคล้องกับความต้องการใช้งาน
- การกำหนดรายละเอียดทางเทคนิคของระบบงานให้ชัดเจนและครอบคลุม
- การมีขั้นตอนปฏิบัติที่ชัดเจนสำหรับการบริหารจัดการโครงการพัฒนาระบบ ยังคงต้องอาศัยจากประสบการณ์การทำงานของผู้ประเมินความเสี่ยงหรือใช้ Best practice จากมาตรฐานหรือเอกสารอ้างอิงอื่นๆ เช่น ITIL COBIT เป็นต้น ในการที่จะระบุว่าองค์กรยังมีจุดอ่อนเพิ่มเติมที่สำคัญๆ อยู่หรือไม่

โดยทั่วไปเมื่อมีประสบการณ์การทำงานที่มากขึ้น หรือได้ศึกษาข้อมูลจากมาตรฐานหรือแหล่งความรู้ต่างๆ มากขึ้น ผู้ประเมินความเสี่ยงก็จะได้ มี หรือสั่งสม Best practice ในการปฏิบัติงานเพิ่มมากขึ้นตามลำดับ ซึ่งหมายความว่าสามารถจัดการกับจุดอ่อนได้มากขึ้นตามลำดับ หรือก็คือบริหารจัดการความเสี่ยงได้มากขึ้นตามฐานของประสบการณ์ที่เพิ่มขึ้นเมื่อเวลาผ่านไป

แผนการควบคุมความเสี่ยง

แผนการควบคุมความเสี่ยงหมายถึง Best practice วิธีการ หรือแนวทางปฏิบัติ ซึ่งองค์กรใช้ในการจัดการกับเหตุการณ์ความเสี่ยงหนึ่ง เช่น

- ความเสี่ยงการเกิดข้อพิพาธ ข้อขัดแย้ง หรือข้อถกเถียงในการตรวจรับระบบงาน/การไม่ได้มีการกำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน
- แผนการควบคุมความเสี่ยงคือ
    - กำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน

จากฐานของประสบการณ์และจากการศึกษาข้อมูลจากมาตรฐานหรือแหล่งความรู้ต่างๆ ณ ที่เวลาหนึ่ง องค์กรอาจมี Best practice ที่ปฏิบัติอยู่เป็นประจำส่วนหนึ่ง เช่น มีการกำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจนในทุกครั้งที่มีการจ้างพัฒนาระบบงาน แต่ในขณะที่ก็ยังมีอีกส่วนหนึ่งที่ยังเป็นจุดอ่อนหรือยังไม่ได้มีการปฏิบัติอย่างสม่ำเสมอไม่ว่าจะด้วยสาเหตุใดก็ตาม เช่น ขาดบุคลากร ขาดงบประมาณ ไม่มีเวลา ขาดความรู้หรือความเข้าใจที่จะปฏิบัติได้อย่างถูกต้อง

เมื่อจุดอ่อนเหล่านั้นได้มีการแก้ไขหรือได้มีการปฏิบัติอย่างสม่ำเสมอมากขึ้น และสั่งสมเป็น Best practice เพิ่มขึ้นขององค์กร นั่นหมายถึงว่าองค์กรเริ่มบริหารจัดการกับความเสี่ยงที่เกิดจากจุดอ่อนเหล่านั้นอย่างเป็นรูปธรรมแล้ว เช่น ในตอนแรกองค์กรอาจมีจุดอ่อนเรื่องการไม่ได้กำหนดให้มีการจัดทำสัญญาห้ามเปิดเผยข้อมูลสำคัญขององค์กรในสัญญาจ้างพัฒนาระบบ (ซึ่งทำให้มีความเสี่ยงเรื่องข้อมูลลับหรือข้อมูลสำคัญขององค์กรถูกเปิดเผยโดยไม่ได้รับอนุญาต) เพราะไม่เคยปฏิบัติเลยหรือปฏิบัติบ้างในบางครั้ง ในภายหลังเมื่อองค์กรได้เรียนรู้มากขึ้นจากประสบการณ์หรืออื่นๆ และเห็นว่ามีความจำเป็น จึงอาจกำหนดเป็น Best practice เพิ่มและกำหนดให้ผู้ประเมินความเสี่ยงปฏิบัติตามโดยเคร่งครัด กล่าวคือต้องจัดทำสัญญาห้ามเปิดเผยข้อมูลสำคัญขององค์กรในทุกสัญญาจ้างพัฒนาระบบ ถึงจุดนี้แสดงว่าองค์กรมีแผนควบคุมความเสี่ยงเรื่องข้อมูลลับหรือข้อมูลสำคัญขององค์กรถูกเปิดเผยโดยไม่ได้รับอนุญาตแล้ว

จากประสบการณ์การทำงานของผู้เขียน พบว่าในบางครั้งองค์กรมีการควบคุมความเสี่ยงในเรื่องหนึ่งอยู่เสมอแล้ว เช่น ในกรณีของหน่วยงานราชการต่างๆ ความเสี่ยงเรื่องการเกิดข้อพิพาธ ข้อขัดแย้ง หรือข้อถกเถียงในการตรวจรับระบบงาน/การไม่ได้มีการกำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน องค์กรจะกำหนดให้มีการจัดทำเกณฑ์การตรวจรับระบบงานทุกครั้ง เพียงแต่ว่าการควบคุมความเสี่ยงดังกล่าวอาจไม่ได้เขียนไว้อย่างเป็นลายลักษณ์อักษร ตัวอย่างของแผนควบคุมความเสี่ยงในกรณีนี้คือ

- ความเสี่ยงการเกิดข้อพิพาธ ข้อขัดแย้ง หรือข้อถกเถียงในการตรวจรับระบบงาน/การไม่ได้มีการกำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน
- แผนการควบคุมความเสี่ยงคือ
    - กำหนดเกณฑ์การตรวจรับระบบงานอย่างชัดเจน

เพื่อให้การบริหารจัดการความเสี่ยงต่างๆ อันหลากหลายมีความเป็นรูปธรรมมากขึ้นและลดความเสี่ยงได้มากกว่า (ที่ไม่ได้เขียนไว้) ควรกำหนดให้มีการจัดทำแผนควบคุมความเสี่ยงอย่างเป็นลายลักษณ์อักษร และกำหนดให้ผู้ประเมินความเสี่ยงมีการปฏิบัติตามแผนเหล่านั้นโดยเคร่งครัด ความเสี่ยงที่มีแผนฯ ที่ชัดเจนเหล่านี้ควรถือว่ามีระดับความเสี่ยงที่ยอมรับได้ (แต่ถึงกระนั้นก็ยังคงต้องกำหนดให้ปฏิบัติตามแผนฯ อย่างเคร่งครัดด้วย)

เมื่อมีหรือพบจุดอ่อนใหม่หนึ่งซึ่งอาจเป็นจุดอ่อนที่ไม่ทราบหรือไม่รู้มาก่อนก็ตาม หรือเป็นจุดอ่อนที่ทราบแต่ยังไม่ได้รับการควบคุมอย่างชัดเจนหรืออย่างเป็นรูปธรรม ซึ่งทำให้องค์กรมีความเสี่ยงจากจุดอ่อนดังกล่าว และ ณ ขณะนี้องค์กรต้องการควบคุมจุดอ่อนนี้ ก็ให้ผู้ประเมินความเสี่ยงเพิ่มความเสี่ยงใหม่และแผนการควบคุมความเสี่ยงนั้นเข้าไปในรายการแผนการควบคุมฯ ปัจจุบันซึ่งก็จะทำให้องค์กรและผู้ประเมินความเสี่ยงมีฐานการควบคุมความเสี่ยงที่มากยิ่งขึ้นเรื่อยๆ (เสมือนมีประสบการณ์เกี่ยวกับความเสี่ยงต่างๆ มากขึ้นเรื่อยๆ ตามลำดับเมื่อเวลาผ่านไป)

จากข้อคำถามที่ 1 ที่ว่าหากจุดอ่อนหนึ่งไม่ได้เป็นจุดอ่อน กล่าวคือตอนที่ประเมินความเสี่ยง พบว่า “มีการปฏิบัติที่ดีซึ่งหักล้างกับจุดอ่อนนั้น” ต้องประเมินความเสี่ยงกรณีนี้หรือไม่ และจะประเมินอย่างไร ความเสี่ยงในลักษณะนี้ถือว่ามีระดับความเสี่ยงที่ยอมรับได้หรือไม่ คำตอบคือหากมีการปฏิบัติที่ดีซึ่งหักล้างกับจุดอ่อนนั้นอยู่เสมอ หรือเป็น Best practice ขององค์กรอยู่แล้ว หรือองค์กรต้องการบริหารจัดการกับความเสี่ยงที่เกิดจากจุดอ่อนเหล่านั้นอย่างเป็นรูปธรรม ก็ให้จัดทำเป็นแผนการควบคุมความเสี่ยงและกำหนดให้ผู้ประเมินความเสี่ยงมีการปฏิบัติตามแผนเหล่านั้นโดยเคร่งครัด ความเสี่ยงในลักษณะนี้ถือว่ามีระดับความเสี่ยงที่ยอมรับได้