คำถามจากสัมมนาเรื่องข้อกำหนด ISO/IEC 27002 ฉบับใหม่ กับการเตรียมการรับการปรับเปลี่ยน ISO/IEC 27001 ครั้งที่ 1

1. ฝากคำถามครับ องค์กรผมกำลังเริ่ม ISO27001:2013 ต้นเดือน กพ นี้ (สรุปผลคัดเลือก Consulting Services แล้ว เรียบร้อย) ที่อยากทราบคือ จะมีผลในการจัดเตรียม เพื่อขอใบรับรองภายใน 270 วัน อย่างไรบ้างครับ เนื่องจากเรายังคง Annex 114 Control แบบเดิมอยู่

BSI: เนื่องจาก ISO/IEC 27002 จะประกาศ ปลายเดือน ม.ค. หรือต้น เดือน ก.พ. และหลังจากนั้น ISO/IEC 27001 ถึงจะประกาศ ตัว control annex A ออกมา เมื่อประกาศเสร็จแล้ว ทาง ผู้ตรวจ จะต้องรอทาง AB (Accreditation Body) ประกาศเรื่อง transition ออกมา ผมว่าอีกสักพักใหญ่ๆ จึงคิดว่า หากกำลังทำ ISO/IEC 27001 น่าจะทำ annex A ตามตัวเดิม แต่อาจจะใส่ ตัวใหม่ของ ISO/IEC 27002 ไว้ เพื่อเตรียมตัวปรับเปลี่ยนต่อไปครับ

2. threat intelligence คืออะไรคะ ช่วยยกตัวอย่างหน่อยค่ะ

BSI: เป็น การควบคุมโดยการ รวบรวม วิเคราะห์ Information ที่เกี่ยวข้องกับ Information Security Threat เพื่อมาเตรียมการ จัดการ ภายในองค์กรครับ

3. Threat intelligence รวมถึงภัยคุกคามทางกายภาพ ด้วยหรือป่าวครับ

BSI: หมายถึง การควบคุมโดยการ รวบรวม วิเคราะห์ Information ที่เกี่ยวข้องกับ Information Security Threat เพื่อมาเตรียมการ จัดการ ภายในองค์กรครับ ครอบคลุม ทุกอย่างทั้ง physical และ logical

4. เพิ่ม cloud service มาด้วยจะกระทบ หรือมีการเปลี่ยนแปลงไปถึง ISO 27017 หรือไม่คะ

BSI: เนื่องจาก ISO/IEC 27017 นั้นเขียนล้อตาม ISO/IEC 27002 ดังนั้น ISO/IEC 27017 นั้นต้องปรับเปลี่ยนให้สอดคล้องกับ ISO/IEC 27002 ครับ เพราะ ตัวข้อกำหนด ISO/IEC 27002 นั้นเปลี่ยน รวมถึง standard ที่เกี่ยวข้องอื่นๆด้วย เช่น ISO/IEC 27018, ISO/IEC 27799 เป็นต้น

5. ระบบตรวจจับ เช่น cctv ไหมคะ

BSI: การตรวจสอบด้วย CCTV ถือเป็น Physical security monitoring ครับ

6. เหมือน ISO 20000 หรือเปล่าคะ

BSI: ข้อ 8.9 configuration management ใกล้เคียงกับ Configuration management ของ ISO/IEC 20000-1 แต่ใน ISO/IEC 27002 จะเขียนอิบายอีกแบบ แต่โดยสรุปใกล้เคียงกันครับ

7. ถ้าทำ ISO20000 อยู่แล้ว มี config mgt อยู่แล้ว ไม่ทราบว่า เพิ่ม 8.9 ขึ้นมานี้ ทางองค์กรต้องปรับเพิ่มอีกมั้ยคะ

BSI: หากมี ISO/IEC 20000-1 อยู่แล้ว ก็applied กับข้อ 8.9 ได้ครับ แต่ข้อนี้จะเน้น ค่า configuration ของระบบครับ

8. ข้อที่ 8.9 ต้องเก็บ configuration baseline ไหมคะ

BSI: ตัว control ไม่ได้พูดถึงรายละเอียด baseline ครับ แต่ข้อนี้จะเน้น การควบคุมค่า configuration ของระบบครับ

9. ข้อที่ 8.10 ต่างจาก CL. 7.5 เรื่อง retention of record อย่างไรคะ

BSI: ข้อ 8.10 ของ ISO/IEC 27002 พูดถึงเรื่องการ deleted ข้อมูล แต่ ใน CL 7.5 (ISO/IEC 27001) จะพูดถึงเรื่องการควบคุมเอกสาร (Documented information control)

10. ในกรณีที่ลบข้อมูล แล้วมีผลในเชิงกฎหมายตามมาจะทำยังไงครับ

BSI: ข้อกำหนด เขียนไว้ชัดครับว่า ข้อนี้ (8.10) ทำเพื่อ ป้องกันการเปิดเผยข้อมูลที่ sensitive และเพื่อให้สอดคล้องกับข้อกำหนดกฎหมาย ระเบียบข้อบังครับ และพันธสัญญา ต่างๆครับ

11. หลายตัวเกี่ยวข้องกับ ISO 27701 ที่ขอ cert ไว้ต้องปรับด้วยใช่ไหมคะ

BSI: ครับ ต้องเตรียมตัวปรับ SOA ให้สอดคล้องกับ ISO/IEC 27001 ที่จะมีการ revised Annex A ครับ

12. ISO 27001 เราสามารถนำมาใช้ Compliance PDPA ที่จะมีผล วันที่ 1 มิย 65 นี้ ได้ทั้งหมดมั้ยครับ ถ้าไม่ได้ มีส่วนไหนต้องเติมบ้างครับ

BSI: PDPA เป็นกฎหมาย ด้านความปลอดภัยข้อมูล โดยมีหลาย องค์ประกอบ การนำ ISO/IEC 27001 ประยุกต์ใช้อาตเพื่อตอบโจทย์ เรื่อง การรักษาความปลอดภัย ของPII ที่อาจจะเกิด incident ได้ แต่ประเด็นด้านอื่นๆก็มีครับ อาจจะต้อง ศึกษาเพิ่มเติม

13. Sensitive ในที่นี้แตกต่างกับ PDPA ใช่มั้ยครับ แปลว่าต้องตีความหมาย Sensitive ในด้านขององค์กรใช่มั้ยครับ

BSI: Sensitive ใน ISO/IEC 27002 นี้จะเป็นข้อมูลที่มีความสำคัญในระดับ confidential มากๆ ในองค์กร อาจไม่ได้มองแค่ PII อย่างเดียวครับ

14. data masking จะกว้างกว่า data labelling ใช่มั้ยคะ

BSI: Data masking คือการ ทำให้ข้อมูล บางส่วนมองไม่เห็น แต่ data labelling คือการแสดงว่า ระดับconfidential classification ของข้อมูลนั้นๆ เป็น level อะไร

15. ข้อที่ 8.16 เกี่ยวข้องกับระบบ SIEM โดยตรง ? ครับ

BSI: 8.16 Monitoring activities เป็นกิจกรรมที่เฝ้าติดตาม ไม่ว่าจะใช้ tools อะไรก็ได้ครับ ข้อกำหนดไม่ได้ พูดถึง Tools

16. ข้อที่ 8.16 ในกรณีองค์กรที่มีการทำ SOC ถือว่าครอบคลุมในเชิงกระบวนการจัดการตามข้อกำหนดที่อัพเดทมาใหม่ใช่หรือไม่คะ ?

BSI: 8.16 Monitoring activities เป็นกิจกรรทที่เฝ้าติดตาม ไม่ว่าจะใช้ tools อะไรก็ได้ครับ ข้อกำหนดไม่ได้ พูดถึง Tools ความพอเพียงต้องขึ้นกับ ความเสี่ยงครับ

17. ข้อที่ 8.23 content filter บน fw พอไหมหรือว่าต้องใช้ proxy

BSI: 8.23 Web filtering ข้อกำหนดไม่ได้ พูดถึง Tools ความพอเพียงต้องขึ้นกับ ความเสี่ยงครับ

18. ข้อที่ 8.28 เหมือนจะเป็น subset ของ 8.25 หรือเปล่าครับ

BSI: 8.28 Secure coding และ 8.25 secure development life cycle โดย ในข้อ 8.25 จะเน้นภาพรวมครับ แต่ 8.28 จะ เน้น coding ครับ

19. บางข้อกำหนดไม่สามารถใช้ policy ได้เช่น DLP ถ้าไม่มีเงินลงทุนทำแนะนำยังไงครับ

BSI: ISO/IEC 27001 ไม่ได้ให้ต้อง implement ทุกข้อ การ implement จะเป็นไปตาม ความเสียง ขององค์กร ตามบริทบองค์กร ตามintended outcome ขององค์กรครับ

20. web filtering เข้าใจว่าใช้ WAF (web app. firewall) ไหมครับ

BSI: 8.2.3 Web filtering เป็นการบริหารจัดการการเข้าถึง เว็ปไซต์ภายนอกให้ลดความเสี่ยงจาก Malicious content

21. 27002 เวอร์ชั่นใหม่เริ่มใช้งานเมื่อไรนะคะ

BSI: จะออกเป็นทางการ ปลาย มกราคม หรือ ต้น กุมภาพันธ์ นี้

22. นโยบายใหม่จะมีการแปลเป็นไทยไหมครับ เพื่อให้เหมือนกันทุกองค์กร ถ้าแต่ละองค์กรแปลกันเอง อาจจะทำให้ข้อนโยบายเป็นภาษาไทยที่ไม่เหมือนกัน

BSI: ทาง BSI จะพยายาม แปลให้ครับใน แต่หากแปลกันเองก็ไม่น่ามีปัญหาครับ เพราะภาษาอังกฤษ มีน fix อยู่แล้ว

23. จะตรวจเพื่อ certify ปลาย ก.พ. ต้องใช้versionไหนคะ

BSI: น่าจะเป็น version เดิมครับเพราะ ISO/IEC 27001 จะออก ประมาณ Q1 หรือ ต้น Q2

24. ISO 27701 ต้องเปลี่ยนตามด้วย จะใช้เวลาปรับนานหรือเปล่าคะ

BSI: ISO/IEC 27001 จะออก ประมาณ Q1 หรือ ต้น Q2

25. แปลว่าเปลี่ยนข้อมูลใน SoA ทันที ซึ่งมีผลกระทบต่อบริษัทที่กำลัง Implement ใหม่ ทันที เพราะรอบตรวจ อยู่ที่ Quarter 3-4 หรือสามารถใช้ ตัวเดิม ได้มั้ยครับ?

BSI: ISO/IEC 27001 จะออก ประมาณ Q1 หรือ ต้น Q2 หลังจากนั้น อาจจะต้องมีเวลาอีกเล็กน้อยในการประกาศของ Accreditation Body ผมแนะนำให้ เป็นตัวเก่าก่อน แต่เตรียมตัวใหม่เพิ่ม ไว้ น่าจะดีกว่าครับ

26. แต่องค์กรที่ทำ ISO ใหม่ละครับ ใช้ Version เดิมหรือใหม่ครับ

BSI: ISO/IEC 27001 จะออก ประมาณ Q1 หรือ ต้น Q2 หลังจากนั้น อาจจะต้องมีเวลาอีกเล็กน้อยในการประกาศของ Accreditation Body ผมแนะนำให้ เป็นตัวเก่าก่อน แต่เตรียมตัวใหม่เพิ่ม ไว้ น่าจะดีกว่าครับ

27. ขอหน้า req technology ได้ไหมคะ ขอบคุณค่ะ

BSI: เดี๋ยวไว้คุยตอน EP 2 ได้ครับ (*คลิกที่นี่ เพื่อสมัครเข้าร่วมสัมมนา ครั้งที่ 2)*

28. ต้อง re cert ใหม่หรือไม่

BSI: ไม่ต้องครับ แต่อาจจะมีกระบวนการ transition ครับ ต้องรอทาง Accreditation Body ประกาศครับ

29. แปลว่าอาจจะเริ่มตรวจได้เร็วสุดปีหน้าไหมคะ version ใหม่

BSI: ต้องรอทาง Accreditation Body ประกาศครับ

30. แสดงว่า ถ้าขอใบรับรอง จาก CB ภายใน ปีนี้ ก็ยังยึด 27001:2013 ได้ใช่มั้ยครับ

BSI: ISO/IEC 27001 จะออก ประมาณ Q1 หรือ ต้น Q2 หลังจากนั้น อาจจะต้องมีเวลาอีกเล็กน้อยในการประกาศของ Accreditation Body ผมแนะนำให้ เป็นตัวเก่าก่อน แต่เตรียมตัวใหม่เพิ่ม ไว้ น่าจะดีกว่าครับ

31. สรุปคือตอนนี้การเลือก Control สำหรับองค์กรที่ต้องทบทวนใหม่ ต้องใช้ Control ใหม่เลยใช่หรือไม่ แต่การตรวจยังคงตรวจตาม Annex A 114 Controls

BSI: ISO/IEC 27001 จะออก ประมาณ Q1 หรือ ต้น Q2 หลังจากนั้น อาจจะต้องมีเวลาอีกเล็กน้อยในการประกาศของ Accreditation Body หลังจากนั้น จะมี process transition ของลูกค้าเก่าครับ

32. ถ้า BSI ยังไม่ประกาศว่าจะตรวจด้วย version 2022 แต่เรา implement ตาม version 2022 ไปก่อนได้ไหมครับ หรือแนะนำให้รอก่อน

BSI: Implement ได้ครับ แต่ SOA อาจจะต้องล้อ version เก่าก่อน เดี๋ยว EP. 2 เรามาพูดเรื่อง Version เก่า กับ ใหม่ครับ มันมีการเทียบได้อยู่ (*คลิกที่นี่ เพื่อสมัครเข้าร่วมสัมมนา ครั้งที่ 2)*

33. ISO อะไรที่เกี่ยวกับ PDPA ครับ

BSI: ISO/IEC 27701 ครับ

34. แล้วถ้าผ่านการรับรอง 27001 และ 27701 แล้วจะสอดคล้องตาม PDPA หรือยังครับ

BSI: PDPA เป็นกฎหมาย ด้านความปลอดภัยข้อมูล โดยมีหลาย องค์ประกอบ การนำ ISO/IEC 27001 ประยุกต์ใช้อาตเพื่อตอบโจทย์ เรื่อง การรักษาความปลอดภัย ของPII ที่อาจจะเกิด incident ได้ แต่ประเด็นด้านอื่นๆก็มีครับ อาจจะต้องศึกษาเพิ่มเติม

35. BSI จะมี course อบรม 27002:2022 เมื่อไหร่

BSI: เร็วๆนี้ครับ เดี๋ยวจะประกาศให้ทราบครับ

36. จะมีทำ mapping ไหมครับ ว่า เช่น 5.1.1 ตรงกับ ข้อ… ใน ISO 27002:2013

BSI: ในตัว ISO/IEC27002 version ใหม่ มีครับ เดี๋ยวคุยกัน EP. 2 ครับ (*คลิกที่นี่ เพื่อสมัครเข้าร่วมสัมมนา ครั้งที่ 2)*

37. ต้องรอให้กฎหมายเกี่ยวกับ PDPA ออกเป็นทางการก่อนใช่ไหมคะ เนื่องจากพยายามแบ่งรายละเอียดเกี่ยวกับ PDPA ให้ชัดเจนค่ะ

BSI: PDPA กฎหมายหลักออกแล้ว 2562 แต่กฎหมายลูกกำลังตามออกมาครับ