<u>คำถามจากสัมมนา เรื่อง ส่องข้อกำหนดมีอะไรใหม่ใน ISO/IEC 27002:2022</u>

1. องค์กรผม กำลังทำ ISO27001:2013 กำหนดระยะเวลาไว้ 9 เดือน (เมย-ธค 65) โดยจ้างที่ปรึกษามาช่วย คาดว่าจะตรวจกับ CB เดือน ธันวาคม 2565 นี้ครับ คำถามคือ ทาง consult ยังใช้ Control 27002:2013 อยู่ (114 controls) จะมี concerns อะไรในการตรวจกับ CB ตอนเดือนธันวาคมมั้ยครับ และในระยะยาว 2-3 ปี จะมีผลกระทบหรือไม่อย่างไรครับ

BSI: จากทาง ที่ BSI แจ้งใน webinar แล้วครับว่า เมื่อ ทาง ISO ออกข้อกำหนด ISO/IEC 27001 มาแล้ว ทาง CB จะต้องรอให้ทาง AB ประกาศ กระบวนการตรวจก่อน หลังจากนั้นทาง CB ถึงจะตรวจ Version ที่จะออกนี้ได้ และหลังจาก ทาง AB ประกาศมาแล้ว คาดว่าจะมี transition period ครับ โดยคาดว่าไม่น่าจะมีประเด็นอะไรครับ แต่ทั้งนี้ทั้งนั้น คงต้องรอทาง AB ออกข้อกำหนดมาให้ CB ก่อน ถึงจะทราบแน่นอนครับ

2. ISO 27002:2022 มีผลกระทบในส่วนขององค์กรที่ Imp. ISO/IEC 27701 ด้วยไหมครับ เนื่องจากมีการอ้างอิงถึง ISO/IEC 27001 ในส่วนของ Control (เพิ่มเติม / ปรับปรุง / เปลี่ยนแปลง) รบกวนสอบถามว่าจะมีผลกระทบอย่างไรครับ

BSI: ISO/IEC 27701 มีข้อกำหนด ของตัวเอง แต่requirementข้อ6 เป็น guideline มีการอ้างอิงข้อกำหนด ISO/IEC 27002:2013 ในอนาคตผมคิดว่าอาจจะมีการปรับครับ แต่ต้องรอทาง ISO ครับ คำถามว่ามีผลอะไรไหม ผมว่ามีบ้างแต่ไม่น่าจะมากครับ เพราะข้อ 6 เป็น guideline ครับ

3. องค์กรผม ต้องทำระบบ ไหนก่อน ISO27001 --> ISO27701 --> ISO27002 ตามลำดับนี้หรือเปล่าครับ

BSI: ISO/IEC 27002 เป็น control ครับ จะใช้คู่กับ ISO/IEC 27001 ในการเลือก security control หากองค์กรท่าน จะImplement ผมแนะนำเป็น ISO/IEC 27001 ครับ และ เลือกcontrol จาก Annex A ของ ISO/IEC 27001 และ รายละเอียดการ control ไปดูใน ISO/IEC 27002 ครับ

สำหรับ ISO/IEC 27701 เป็น เรื่อง Privacy Information Management System ซึ่งการตรวจรับรองตัวนี้ขอบเขตการตรวจต้องอยู่ภายใต้ ISO/IEC 27001ครับ โดยจะ certify พร้อมกับ ISO/IEC 27001 หรือ Certify หลัง ISO/IEC 27001 ก็ได้ครับ อยู่ที่องค์กรครับ

4. ไม่ทราบว่ามีสรุป ตัวคุมที่ slide ไม่มีการเปลี่ยนแปลงหรือไม่ครับ พอดีจะเห็นแค่ตัวใหม่ ปรับปรุง และรวมน่ะครับ

BSI: ครั้งนี้เราคุย เฉพาะตัวที่ปรับเปลี่ยนครับ

5. SOA ต้อง Running No. Control ใหม่ทั้งหมดตามที่เปลี่ยนไป หรือไม่

BSI: SOA ตามข้อกำหนด ISO/IEC 27001 (6.1.3 d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c))and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A) โดยสรุปต้องมีข้อกำหนด ให้ครบ Annex A ใหม่ครับ

6. เราสามารถปรับ control ที่มีอยู่ในปัจจุบันให้ล้อตาม version ใหม่ได้เลยไหมครับ แม้ว่าบริษัทจะยังไม่ได้ขอ upgrade version

BSI: อาจทำได้ครับ แต่มีประเด็นคือทาง CB ต้องอ้างอิงการตรวจตามversion เดิมครับ ผมแนะนำ ให้มี version เดิมคู่ไปก่อนน่าจะดีกว่าครับ

7. What is the impact to Financial Institutions on the new ISO?
BSI: กระทบกับ ผู้ที่ Implement ISO/IEC 27001 ทุกsector ครับ เพราะ Information control ใน Annex A มีการปรับเปลี่ยนครับ

8. What is the additional topic that may be required for annual audit from this new ISO?
BSI: ISO/IEC 27002 ไม่ได้มีการกำหนดเรื่องนี้ครับ

9. Will this new ISO impact to the existing certificate we have for 3 years?

BSI: ต้องรอทาง AB ประกาศครับ โดยรายละเอียดรบกวนดูคำถามข้อ 1 ครับ

10. การปรับเปลี่ยน Annex A ของ ISO 27001 จะถือว่าเป็น Version 2022 หรือไม่ หรือยังเป็น Version 2013 แล้วมีส่วนเพิ่มเติมเข้ามาเท่านั้น

BSI: ต้องรอทาง ISO ประกาศอีกทีครับ แต่ที่ปรับเปลี่ยนคือ Annex A และ note เล็กๆ ในข้อ 6.1.3 (ผมอ้างอิงจาก version CD นะครับ)

11. ISO/IEC 27001:2022 จะสรุปประกาศเป็นทางการ เมื่อไร

BSI: ต้องรอทาง ISO ประกาศครับ อาจเป็น Q2 หรือ Q3 ครับ

12. ปีนี้จะมีการ Recert. ISO 27001 เดือน มิ.ย. ค่ะ มีแนวโน้มว่า จะต้องขอ Recert. รอบถัดไป ก่อนจะหมดอายุ 3 ปี ไหมคะ

BSI: ต้องรอทาง AB ประกาศครับ โดยรายละเอียดรบกวนดูคำถามข้อ 1 ครับ

13. ต้องทำ ISO27001 แล้วถึงจะทำ ISO27701 หรือเปล่าครับ หรือว่า ทำตัว ISO27701 ได้เลยครับ

BSI: การ certify ในscope ของ ISO/IEC 27701 ต้องอยู่ภายใต้ scope ของ ISO/IEC 27001 โดยสามารถตรวจISO/IEC 27701พร้อมกับ ISO/IEC 27001 ได้ หรือ ตรวจหลังจากได้ cert ISO/IEC 27001 แล้ว ก็ได้ครับ

14. ท่านวิทยากรบอกว่า C4-C10 ยังไม่ได้เปลียนใช่ไหมครับ

BSI: ครับผม

15. ขอตัวอย่าง tool or manual process to implement the new controls

BSI: ตอนนี้ยังไม่ได้ทำครับ แต่ในอนาคตต้องลองติดตามทาง BSI นะครับ