คำถามจากสัมมนา เรื่อง Cyber security & PDPA สำหรับ โรงงานผู้ผลิต

ข้อซักถาม	แสดงความเห็นตามข้อซักถาม
1. คิดว่าเราทำระบบนี้ จะต้องมี SIEM เพื่อรวบรวม Log มั้ยครับ	ISO/IEC 27001:2022 ข้อ 1 บอกว่า มาตรฐานนี้ ใช้สำหรับ treatment ความเสี่ยงที่พอดี ๆ กับองค์กร โดยองค์การ เป็นผู้พิจารณาความเสี่ยงเอง ว่า ควรมีการควบคุมด้าน security control อะไรบ้าง ตามความเสี่ยงที่องค์กรยอมรับได้ครับ แต่การมี SIEM หรือไม่ขึ้นอยู่กับองค์กร จะพิจารณาเองครับ
2. Secure Coding เราควรมีเครื่องมือในการตรวจสอบ Code อย่างพวก SonarCube มั้ยครับ	เช่นเดียวกับข้อ 1 องค์กร พิจารณาตามความเสี่ยงครับ ว่าจะ implement มากหรือน้อยแค่ไหน
3. Pentest จำเป็นต้องทำ หรือ ควรทำมั้ยครับ	เช่นเดียวกับข้อ 1 องค์กร พิจารณาตามความเสี่ยงครับ ว่าจะ implement มากหรือน้อยแค่ไหน พิจารณาเองว่าต้องมี Pentest ไหมครับ
4. หน่วยงานหรือธุรกิจแบบไหนที่จำเป็นต้อง implement ISO 27001/27002 ครับ	สามารถใช้กับ หน่วยงาน ทุกหน่วยงานที่ต้องการควบคุมข้อมูลสารสนเทศให้ปลอดภัย เช่น โรงงาน, service provider, หน่วยงานราชการ หรือเอกชนครับ
5. ถ้าต้องเขียน manual ของระบบนี้ สามารถเขียนรวมกับ ISO9001 ได้ใช่ไหมครับ	ได้ครับ เพราะข้อกำหนดที่เป็น Framework ข้อ 4-10 คล้ายกับ ISO 9001 ครับ แต่ข้อ security control ตาม Annex A ก็อาจแทรกใน operational control procedure ที่เกี่ยวข้องได้ครับผม
6. รบกวนขอคำแนะนำครับ ผมทำงานในส่วน HR อยากได้คำแนะนำว่าต้องเช็คหรือปรับปรุงส่วนไหนบ้างครับ	หากเป็น ISO/IEC 27001:2022 HR อาจต้องดูในข้อ 7.2 (Competency), 7.3 (Awareness), 7.4 (communication) และ Annex A ข้อ 6 ที่เป็นพวก Background screening, การกำหนด บทลงโทษ ต่าง ๆ ครับ
7. กรณีที่บริษัทรปภ.เก็บข้อมูลจากการเสียบบัตรประชาชนของลูกค้า หรือ ผู้มาติดต่อ บริษัทถือเป็น Controller ใช่ไหม ถ้าใช่องค์กรต้องมีการตรวจสอบการเก็บระยะเวลาการเก็บข้อมูลด้วยใช่ไหม	ใช่ครับ กรณีนี้ องค์กร จะเป็น controller เพราะทำหน้าที่ในการกำหนดวัตถุประสงค์การเก็บ เมื่อองค์กรเป็น Controller แล้ว องกรณ์ต้องทำตามกฎหมาย PDPA หรือ ISO/IEC 27701 ข้อ 8 เช่น ต้องกำหนดฐานการเก็บ, แจ้งเจ้าของข้อมูลให้ทราบตามกฎหมาย, ต้องควบคุมเรื่อง security, etc.
8. PII Transfer on Cloud มีข้อแนะนำการ Imp PDPA (27001:2022) อย่างไรบ้างครับ	ISO/IEC 27001:2022 มี control 5.23 Information security for use of cloud services ที่พูดถึง Security control ของการใช้ cloud ให้ ครอบคลุม lifecycle ของการใช้ cloud ตั้งแต่การเลือกใช้บริการ จนถึงหากเรายกเลิกทางผู้ให้บริการจะมีการดูแลข้อมูลเราอย่างไร ลบอย่างไร แค่ไหน แต่หากเป็น ข้อมูลส่วนบุคคล อาจต้องพิจารณา ประเทศที่เขาเก็บข้อมูลเราตามกฎหมาย PDPA บ้านเราครับ
9. หากทำ ISO27701 เรียบร้อยแล้ว จะต้องทำ PDPA ต่างหากอีกมั้ยคะ สามารถ Comply ได้เลยรึเปล่าคะ	การ implement ISO/IEC 27701 ไม่ได้ แสดงว่าเรา comply PDPA ของเรา แต่ จะทำให้ ระบบการจัดการข้อมูลส่วนบุคคลเรา มีระบบมากขึ้น และข้อกำหนดของ ISO 27701 ก็ใกล้เคียงกับ PDPA ครับ และ การที่จะ certify ISO 27701 จะต้องมีระบบการติดตามกฎหมาย และ comply ตามกฎหมาย ตาม requirement ด้วยครับ