คำถามจากงานสัมมนาออนไลน์

คำถามและคำตอบจากงานสัมมนาออนไลน์เรื่อง เตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์กับ NIST Cybersecurity Framework 2.0

1.ตัว NIST 2.0 จะมีลักษณะคล้ายกับ BOT's CRAF มาก แต่ขอเรียนสอบถามว่า

กรณีความเสี่ยงเกี่ยวกับการใช้บริการจาก 3rd Party ใน NIST 2.0 จะมีแซมอยู่ในหัวข้อต่าง ๆ แล้ว ใช่หรือไม่ครับ

ANSWER. กรณีความเสี่ยงเกี่ยวกับการใช้บริการจาก 3rd Party ใน NIST 2.0 มีกำหนด ในหลายๆ หัวข้อแล้วครับ เช่น

GOVERN (GV) –

- GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.
- GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.
- GV.SC-04: Suppliers are known and prioritized by criticality.
- GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.
- Etc.

และมีข้ออื่นอีกครับผม

2.ปัจจุบันหน่วยงานได้รับการรับรองมาตรฐาน ISO27001 อยู่แล้ว แต่ถ้าหากต้องการทำระบบให้รองรับ พรบ.ไซเบอร์ ได้อย่างครบถ้วน ต้องทำ NIST ในส่วนไหนเพิ่มเติมครับ

ANSWER. องค์กรที่มี ISO/IEC 27001 อยู่แล้ว การที่ทำ NIST CSF ไม่ยากครับ แค่ไป review procedure ให่มีรายละเอียด NIST CSF ครับ เพราะ หากดูข้อกำหนด ของ ISO/IEC 27001 Annex A นั้น จะ ไท่ได้ลงรายละเอียด แต่ NIST CSF จะมีรายละเอียดมากกว่าครับ แค่มาreview ในรายละเอียดครับผม

3.dentify Inventory - The organization's current cybersecurity risks are understood What is the foreign background like?

ANSWER. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization / Asset Management (ID.AM) ข้อนี้ข้อกำหนด IDENTIFY (ID): ให้ องค์กรมองดูตัวเอง ว่าในองค์กรนั้นๆ มีความเสี่ยงด้าน Cyber security อะไรบ้าง โดย Category Asset Management (ID.AM) ให้มีการจัดการ asset โดย subcategory หลายๆ subcategory กำหนดให้มี asset inventory ให้ครอบคลุม หลายๆ information asset เช่น H/W, S/W, Network, System etc. เพื่อจะได้ทราบว่า information asset อะไรบ้างที่ต้อง ควบคุม และ แต่ละ asset มี ความเสี่ยง Cyber อะไรบ้าง

4.เรียนสอบถามอาจารย์ครับ กรณีที่องค์กร Certify ISO27001 & ISO27701 และ PCIDSS 3.2.1 อยู่แล้ว หากต้อง Apply NIST CSF 2.0 เพิ่ม ในมุมมองของอาจารย์มองว่าประเด็นใดที่สำคัญ ที่องค์กรต้อง Imp. เพิ่มเติม

ANSWER. ISO standard, PCIDSS Standard, NIST standard มีการเขียนที่แตกต่างกัน บางstandard ลงรยละเอียดบางเรื่อง ไม่ได้ลงรายละเอียด บางเรื่อง ดังนั้นผมยังแนะนำ ให้เอา NIST CSF มาทำ Gap analysis เพื่อดูว่า มีตัวให้บ้างที่ ยังไม่มีรายละเอียด ในเรื่องใดของ NIST CSF ก็มา review ทำเพิ่ม โดย ส่วยตัว ผมว่าไม่มากครับ แค่มาปรับปรุงรายละเอียดครับผม

5.แปลว่าการขอ Cert NIST เราต้องมี Cert ISO27001 ก่อน ใช่มั๊ยคะ

ANSWER. ใช่ครับ การขอ cert NIST CSF ต้องอยู่ภายใต้ Cert ISO/IEC 27001 ครับ แต่ จะขอ ISO/IEC 27001 certification ก่อน หรือ ขอพร้อมกันก็ได้ครับ