คำถามจากสัมมนา "ยกระดับ Data Center ด้วยมาตรฐาน ISO27001:2022"

1. สมมุติว่าผม เช่าห้อง Data Center มาแห่งหนึ่ง ระหว่างทางผู้เช่า ต้องมีข้อมูลอะไรที่จำเป็นต้องใช้งาน ISO27001 บ้าง กับผู้ให้เช่าห้อง Data Center ต้องมีข้อมูล ISO27001 อะไรบ้างที่ต้องแจ้งทางผู้เช่ารับทราบ
Ans. เนื่องจากเป็นการเช่าห้อง Data center ผู้เช่าและผู้ให้เช่าสามารถพิจารณาตามข้อกำหนด Annex A.5.22 ซึ่งควรมีข้อมูลตามเงื่อนไขข้อตกลงหรือสัญญา เช่น SLA อาจจะประกอบด้วย % Availability ของการให้บริการ DC, Physical access log การเข้าถึงเครื่อง server ของผู้เช่า, รายงานการควบคุมอุณหภูมิความชื้น และปริมาณการควบคุมการใช้กระแสไฟฟ้าของตู้ Rack เป็นต้น

2. Risk ในข้อ 6 หมายถึง Risk ทางด้าน Physical หรือ กระบวนการเข้าถึงข้อมูลที่จัดเก็บภายใน DC ครับ
Ans. สามารถตอบได้ว่ามีความสัมพันธ์กันทั้งทางด้านกายภาพและกระบวนการเข้าถึงข้อมูลที่จัดเก็บภายใน DC ตามข้อกำหนดข้อ 6 มีการกำหนดพิจารณาความเสี่ยงอยู่ 2 หัวข้อหลัก ดังนี้

ข้อกำหนด 6.1.1 การพิจารณาความเสี่ยงและโอกาสตามข้อกำหนด 4.1 (ปัจจัยภายในและปัจจัยภายนอก) และ 4.2 (ความต้องการผู้มีส่วนได้ส่วนเสีย) โดยการพิจารณาความเสี่ยงและโอกาสนั้นควรทำให้มั่นใจได้ว่าการบริหารจัดการ ISMS ขององค์กรสามารถบรรลุผลลัพธ์ตามที่ตั้งใจไว้

ข้อกำหนด 6.1.2 สามารถพิจารณาบ่งชี้ความเสี่ยงความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับการสูญเสียความลับ (Confidential) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) ภายในขอบเขต ISMS ดังนั้นไม่เพียงแค่การพิจารณากระบวนการเข้าถึงข้อมูลที่จัดเก็บใน DC เท่านั้น ควรพิจารณาด้านกายภาพอื่นๆที่อาจมีความเสี่ยงให้เกิดความสูญเสียของ CIA ได้

3. Control Data Center กับ DR site ต้องเหมือนกันไหมคะ
Ans.การควบคุม Data center กับ DR site สามารถเหมือนหรือแตกต่างกันได้ ขึ้นอยู่กับการพิจารณาความเสี่ยงของแต่ละองค์กร

4. Gap ระหว่าง ISO27001 Version 2013 กับ ISO27001 Version 2022 ในส่วนของ Data Center ที่ต้องดำเนินการเพิ่มครับ
Ans. อ้างอิงตามข้อกำหนด ISO/IEC27001:2022 สำหรับภาพรวมการบริหารจัดการ มีข้อกำหนดเพิ่มเติมในข้อที่ 6.3 Planning of change เมื่อองค์กรมีการเปลี่ยนแปลงใดๆที่ส่งผลต่อระบบการบริหารจัดการ ISMS การเปลี่ยนแปลงนั้นต้องดำเนินการตามแผนที่วางไว้

สำหรับข้อกำหนดใหม่ในส่วนของมาตรการควบคุมตาม Annex A มีข้อกำหนดใหม่เพิ่มเติม 11 ข้อ ดังนี้
5.7 Threat intelligence
5.23 Information security for use of cloud services
5.30 ICT readiness for business continuity
7.4 Physical security monitoring
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.16 Monitoring activities
8.23 Web filtering
8.28 Secure coding
องค์กรสามรถนำมาพิจารณาความเกี่ยวข้องในส่วน Data center ได้ เช่น ข้อกำหนด Annex A 7.4 Physical security monitoring เช่น CCTV, Sensor แจ้งเตือนหากมีผู้บุกรุก หรือระบบอื่นๆที่ใช้ในการเฝ้าระวังที่สามารถตรวจจับผู้บุกรุกได้ และสามารถพิจารณาเพิ่มเติมที่เกี่ยวข้องด้านอื่นได้ อย่าง Annex A 8.10 Information deletion เช่น กำหนดวิธีการลบบันทึกข้อมูลเข้า-ออก Data center อย่างมีประสิทธิภาพ และ Annex A 8.11 Data masking เช่น การปกปิดข้อมูลโดยเฉพาะข้อมูลส่วนบุคคลของผู้ใช้บริการ Data Center หรือแม้แต่

Annex A 5.23 Information security for use of cloud services หากมีการใช้ระบบ Cloud ของผู้ให้บริการภายนอกในการบันทึกภาพของ CCTV ก็สามารถนำมาพิจารณาได้เช่นกัน

สามารถดูรายละเอียดเพิ่มเติมได้จาก BSI Webinar สำหรับเวอร์ชั่นใหม่ ISO/IEC27001:2022

5. การเข้าพื้นที่ data center ที่มีการดูระหว่างระบบโทรศัพท์ และ server เป็นคนละหน่วยงาน ตามหลักการ ISO เราเสนอการจัดการ server ไว้ในการเข้าถึงได้ระบุผู้เข้าตามหน้าที่จะจัดการอย่างไรเพื่อให้สอดคล้องตามมาตรฐาน ISO ครับ
Ans. จากคำถามเข้าใจว่าผู้ถามต้องการทราบถึงการควบคุมการเข้าพื้นที่ Data center ที่มี ระบบโทรศัพท์ และระบบ server อยู่ในพื้นที่เดียวกัน โดยได้กำหนดผู้ที่สามารถเข้าถึง ระบบ server ไว้แล้วตามภาระหน้าที่ แต่ยังคงมีผู้ดูแลระบบโทรศัพท์สามารถเข้าพื้นที่ดังกล่าวได้เช่นเดียวกัน ดังนั้นหากต้องการทำให้มั่นใจได้ว่าการควบคุมการเข้าพื้นที่สอดคล้องกับ ISO องค์กรควรพิจารณาว่ามีความเสี่ยงที่ผู้เข้าถึงพื้นที่สามารถเข้าถึงระบบของอีกฝ่ายที่ไม่เกี่ยวข้องได้แค่ไหน ตัวอย่างเช่น มีการป้องกันการเข้าถึงโดยมีตู้ Rack ล็อคอีกชั้นหนึ่ง นั้นเพียงพอในการยอมรับความเสี่ยงที่หลงเหลืออยู่หรือไม่ หากการควบคุมนี้ยังไม่เพียงพอ สามารถพิจารณาเพิ่มเติมในการแยกโซนแยกห้องหรือกั้นพื้นที่ทั้งสองระบบออกจากกัน เพื่อลดความเสี่ยงการเข้าถึงระบบเชิงกายภาพจากผู้ที่ไม่เกี่ยวข้องได้ ทั้งนี้การควบคุมจะมากหรือน้อยขึ้นอยู่กับความเสี่ยงที่องค์กรยอมรับได้

6. กรณีใช้ Data Center on cloud ช่วยแนะนำแนวทางปฏิบัติสำหรับผู้ใช้บริการด้วยครับ
Ans.กรณีนี้ถือเป็นการใช้ Infrastructure as a service (IaaS) สามารถนำข้อกำหนด Annex A 5.23 Information security for use of cloud services องค์กรควรกำหนด กระบวนการในการจัดหา การใช้ การจัดการ และการยกเลิกการใช้บริการคลาวด์ และจะต้องจัดทำขึ้นตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

7. หากมี datacenter ของตัวเอง ห้องจะอยู่ใกล้ห้องทำงานของ พนักงานที่เกี่ยวข้องได้ไหมครับ
Ans. การตั้งห้อง data center ควรพิจารณาตามความเสี่ยงตามข้อกำหนด 6.1.2 ทั้งด้านสถานที่ตั้งและการจัดวางที่เหมาะสมของ Infrastructure ที่ไม่ก่อให้เกิดการสูญเสียต่อ CIA

8. อธิบายคร่าวๆ ในประเด็นเรื่อง Climate Change ที่ทาง ISO เพิ่งจะประกาศออกมาเพิ่มครับ
Ans. สามารถดูข้อมูลเพิ่มเติมเรื่องของ Climate Change ใน ISO 27001 ได้ที่นี่

9. อยากทราบมาตราฐานที่ Data Center ต้องมี เนื่องจากทางบริษัทมีการเช่าใช้งาน Sever รูปแบบ Cloud Service อยู่ครับ
Ans.มาตรฐานที่สามารถเกี่ยวข้องกับ Data Center มีดังนี้
- ISO/IEC27001:2022 สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านความมั่นคงปลอดภัยของข้อมูล
- ISO22301:2019 สำหรับการบริหารความต่อเนื่องทางงธุรกิจ
- ISO/IEC20000-1 สำหรับระบบบริหารการบริการทางด้านไอที
- CSA-STAR มาตรฐานที่เกี่ยวข้องกับผู้ให้บริการ Cloud

10. หัวข้อที่ต้องมีการขอข้อมูลจากการไฟฟ้า เช่น มี capacity อย่างไร, มีการดำเนินการใน PM อย่างไร ทางเราควรต้องปฏิบัติอย่างไรหรือวิธีการเพื่อให้ได้ข้อมูล เพราะปกติแล้วทางการไฟฟ้าจะไม่เปิดเผยข้อมูลให้ทราบ
Ans. ตามที่ได้บรรยายไว้ในส่วนของข้อมูลเกี่ยวกับการไฟฟ้านั้น หมายถึงข้อมูลการควบคุมการใช้ไฟฟ้าของ Data center นั้นมีการควบคุม Capacity อย่างไร เช่น % UPS Load และ การควบคุมปริมาณกาใช้กระแสไฟฟ้าของแต่ละ rack เป็นต้น ตลอดจนการรายงานผลการตรวจสอบเฝ้าระวังและการทำ PM ซึ่งสามารถขอข้อมูลได้จากผู้ให้บริการ Data center

11. ในข้อกำหนด 7.4 Physical security monitoring จำเป็นจะต้องมี motion detection , sensor และ Alarm of accessible windows ครบทั้ง 3 หัวข้อไหมคะ หรือแค่อย่างใดอย่างหนึ่งก็ได้
Ans.การกำหนดมาตรการควบคุมของแต่ละองค์กรอาจมากหรือน้อยแตกต่างกันได้ขึ้นอยู่กับการพิจารณาความเสี่ยงและการยอมรับความเสี่ยงที่หลงเหลืออยู่ได้

12. การ certify data center ใช้แค่ ISO27001:2022 พอไหมคะ หรือต้องมีมาตรฐานอื่นด้วย
Ans.มาตรฐานที่สามารถเกี่ยวข้องกับ Data Center มีดังนี้
- ISO/IEC27001:2022 สำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านความมั่นคงปลอดภัยของข้อมูล
- ISO22301:2019 สำหรับการบริหารความต่อเนื่องทางงธุรกิจ
- ISO/IEC20000-1 สำหรับระบบบริหารการบริการทางด้านไอที
- CSA-STAR มาตรฐานที่เกี่ยวข้องกับผู้ให้บริการ Cloud
ดังนั้นขึ้นอยู่กับความต้องการขององค์กรและความต้องการของผู้ใช้งานเพื่อยืนยันการดำเนินงานของ Data Center นั้นเป็นมาตรฐานสากลในด้านต่างๆได้