ISO/IEC 27001:2022

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ข้อกำหนดหลัก: ข้อ 4-5

ข้อ 4: บริบทขององค์กร

กำหนดปัจจัยภายใน/ภายนอก ระบุผู้มีส่วนได้ส่วนเสีย และกำหนดขอบเขต ISMS อย่างชัดเจน

ข้อ 5: ภาวะผู้นำ

ผู้บริหารระดับสูงแสดงความมุ่งมั่น กำหนดนโยบาย และมอบหมายบทบาทหน้าที่อย่างชัดเจน

ข้อกำหนดหลัก: ข้อ 6-7

ข้อ 6: การวางแผน

- ประเมินและจัดการความเสี่ยง
- จัดทำ Statement of Applicability (SOA)
- กำหนดวัตถุประสงค์ที่วัดผลได้

ข้อ 7: การสนับสนุน

- จัดสรรทรัพยากรที่จำเป็น
- พัฒนาสมรรถนะบุคลากร
- สร้างความตระหนักรู้
- จัดการเอกสาร

ข้อกำหนดหลัก: ข้อ 8-10

ข้อ 8: การดำเนินการ

นำแผนงานไปปฏิบัติ ควบคุมกระบวนการ และประเมินความเสี่ยงตามรอบระยะเวลา

ข้อ 9: การประเมินผล

ติดตามวัดผล ดำเนินการตรวจสอบภายใน และให้ผู้บริหารทบทวน

ข้อ 10: การปรับปรุง

ปรับปรุงและพัฒนาอย่างต่อเนื่อง แก้ไขความไม่สอดคล้องเพื่อป้องกันการเกิดซ้ำ

มาตรการควบคุม: หมวด 1-2

1. มาตรการขององค์กร

นโยบาย บทบาทหน้าที่ การบริหารบัญชีทรัพย์สิน การควบคุมสิทธิเข้าถึง การจัดการผู้ให้บริการภายนอก การวางแผนเหตุการณ์ ความพร้อม ICT และการปฏิบัติตามกฎหมาย

2. มาตรการด้านบุคลากร

การคัดเลือกและตรวจสอบภูมิหลัง การจัดทำข้อตกลงจ้างงาน การฝึกอบรมและสร้างความตระหนักรู้ การกำหนดกระบวนการทางวินัย มาตรการการทำงานระยะไกล และช่องทางการรายงานเหตุการณ์

มาตรการควบคุม: หมวด 3-4

3. มาตรการทางกายภาพ

กำหนดพื้นที่ห่วงห้าม ควบคุมการเข้าออก เฝ้าระวังทางกายภาพ บังคับใช้นโยบาย IT และการจัดการสื่อข้อมูลอย่างปลอดภัย

4. มาตรการทางเทคโนโลยี

การเข้าถึง (User endpoint, Privileged access, Authentication) ป้องกัน (Malware, Vulnerability management) เข้ารหัส (Cryptography) สำรองข้อมูล (Backup) พัฒนาระบบ (Secure SDLC) และเครือข่าย/ติดตาม (Network security, Logging)

จุดเด่นที่สำคัญของมาตรฐาน

หลักการ PDCA

ใช้วงจร Plan-Do-Check-Act เป็นแกนหลักในการบริหารจัดการ เพื่อขับเคลื่อนองค์กรไปสู่การพัฒนาอย่างต่อเนื่อง

Risk-Based Approach

เน้นการบริหารจัดการตามความเสี่ยงเป็นหัวใจสำคัญ การเลือกใช้มาตรการควบคุมขึ้นอยู่กับระดับความเสี่ยงที่องค์กรประเมินได้

การบูรณาการ

ด้วยโครงสร้างระดับสูง (High-Level Structure) ทำให้สามารถนำไปบูรณาการร่วมกับระบบบริหารจัดการมาตรฐานอื่น ๆ ของ ISO ได้อย่างลงตัว

ความยืดหยุ่น

องค์กรมีอิสระในการเลือกใช้และปรับเปลี่ยนมาตรการควบคุมใน Annex A ให้เหมาะสมกับบริบทและสภาพแวดล้อมของตนได้อย่างเต็มที่

เอกสารสำคัญที่ต้องจัดทำ

01

นโยบายความมั่นคงปลอดภัยสารสนเทศ

02

รายงานการประเมินความเสี่ยง

03

Statement of Applicability (SOA)

04

ขอบเขต **ISMS**

05

แผนจัดการความเสี่ยง

06

วัตถุประสงค์ด้านความมั่นคงปลอดภัย

07

หลักฐานการฝึกอบรมและสมรรถนะบุคลากร

08

ผลการตรวจประเมินภายใน

ประโยชน์ที่ได้รับ

ปกป้องข้อมูลสำคัญ

ลดความเสี่ยงจากการละเมิดข้อมูลและภัยคุกคามทางไซเบอร์

สร้างความเชื่อมั่น

เพิ่มความมั่นใจให้กับลูกค้าและผู้มีส่วนได้ส่วนเสีย

ปฏิบัติตามกฎหมาย

รองรับการปฏิบัติตามกฎหมาย PDPA และข้อกำหนดอื่น ๆ

ขั้นตอนการนำ ISO 27001 ไปใช้

1. ประเมินสถานการณ์ปัจจุบัน

วิเคราะห์ความต้องการและกำหนดกรอบการทำงาน

2. จัดทำเอกสาร

เตรียมเอกสารและมาตรการควบคุมที่จำเป็น

3. ฝึกอบรมและปฏิบัติ

พัฒนาสมรรถนะและสร้างความตระหนักรู้

4. ตรวจสอบและปรับปรุง

ดำเนินการตรวจสอบภายในและปรับปรุงอย่างต่อเนื่อง