INFORMATION
SECURITY
ISO27001
ISMS

เรียนรู้มาตรฐาน ISO 27001

มาตรฐานความปลอดภัยของข้อมูล

Information **SECURITY**
Management System (ISMS)
การบริหารจัดการมาตรฐาน ความปลอดภัยของข้อมูล

เรียนรู้มาตรฐาน ISO 27001 :2013

Information Security Managment System (ISMS) Standard หรือที่รู้จักกันในนาม ISO 27001 เป็นมาตรฐานเกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย โดยจะต้องให้ความสำคัญในส่วนของบุคลากร เรื่องกฎระเบียบขององค์กรเรื่องจัดซื้อจัดจ้างเรื่องการฝึกอบรมพนักงาน เป็นต้น

การจัดทำระบบบริหารจัดการ (Management System) จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง

- การบริหารคน (ภายในองค์กรและภายนอก เช่น Outsource)
- กระบวนการและเทคโนโลยี (เข้าใจกระบวนการทำงานและเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน)
- บริหารงบประมาณ (การลงทุนที่คุ้มค่า)

ซึ่งต้องเข้าใจทั้ง 3 ด้านข้างต้น เพื่อที่จะหาจุดสมดุลย์และเกิดประโยชน์สูงสุดโดยจะต้องวางแนวทางปฏิบัติให้เหมาะสม ไม่เข้มงวดเกินไป ซึ่งจะทำให้ส่งผลต่อการทำงานได้

ISO27001 มาตรฐานสากลที่ทั่วโลกยอมรับ

องค์กร ISO - International Organization for Standardization เป็นหน่วยงานที่ให้กำเนิดมาตรฐาน ISO 27001 โดยเวอร์ชั่นล่าสุดคือ ISO 27001 : 2013 ประกาศเมื่อ 1 ต.ค. 2013 ส่วนเวอร์ชั่นแรกประกาศใช้ครั้งแรกเมื่อปี 2550 (ISO 27001:2005) หลังจากประกาศใช้ ก็ได้รับความสนใจจากองค์กร ทั้งภาครัฐและเอกชนทั่วโลก นำมาใช้งานและขอการรับรอง (Certification) ซึ่งในปัจจุบันกรมการพัฒนาชุมชน ในส่วนของ“ศูนย์ควบคุมระบบคอมพิวเตอร์ (Server and Control Room) ผ่านการตรวจประเมินรับรองมาตรฐาน ISO 27001 : 2013 เป็นที่เรียบร้อยเมื่อวันที่ 25 กรกฎาคม 2561

ISO 27001 มีประโยชน์อย่างไร

- เพิ่มความเชื่อมั่นให้กับประชาชนผู้มาใช้บริการกับทางหน่วยงาน
- ลดค่าใช้จ่ายในการดูแลรักษาระบบสารสนเทศ
- มั่นใจได้ว่าข้อมูลถูกเก็บรักษาเป็นความลับ
- มีการปรับปรุงระบบสารสนเทศอย่างต่อเนื่อง

ISO 27001 ทำยากไหม?

ในการจะจัดทำ ISO 27001 ต้องมีความรู้และความเข้าใจ 2 เรื่องใหญ่ๆ คือ

1. เข้าใจองค์กรตัวเอง
2. เข้าใจมาตรฐานว่าต้องทำอะไรบ้าง

1. เข้าใจองค์กรตนเอง :

ต้องสำรวจข้อมูล ซอฟแวร์ ฮาร์ดแวร์ บุคลากร ในขอบเขตที่จัดทำระบบ หากหน่วยงานของท่านเป็นราชการ บัญชีครุภัณฑ์เป็นจุดเริ่มต้นที่ดีในการรวบรวมข้อมูล Hardware และ Software เข้าใจภารกิจขององค์กรรู้ว่าระบบงานใดสำคัญที่สุดและระบบงานต่างๆ มีข้อจำกัดและจุดอ่อนอะไรบ้าง เพื่อที่จะไปกำหนดมาตรการมาจัดการกำจัดจุดอ่อน เช่น ระบบฐานข้อมูลทำงานอยู่บนเครื่อง Server ที่ใช้งานมานาน ไม่มี Spare part หาก Server นี้พังไปก็ทำให้ระบบล่ม ในกรณีนี้จุดอ่อนก็คือ Server มีความเสี่ยงที่จะเสียหายไปเมื่อไหร่ก็ได้ ดังนั้นเราก็ต้องหามาตรการมาจัดการความเสี่ยงนี้ โดยจัดหาเครื่องใหม่หรือกำหนดมาตรการในการจัดการกับความเสี่ยงนี้ ทั้งนี้ก็แล้วแต่แนวทางและขีดความสามารถของแต่ละองค์กร

2. เข้าใจมาตรฐาน :

จะนำมาตรฐาน ISO 27001 มาใช้งาน ก็ต้องทำความเข้าใจในตัวมาตรฐาน ว่าต้องทำอะไรบ้างทั้งเรื่องเอกสาร (Documents) และการนำไปใช้งานจริง (Implementation)

เริ่มต้นอย่างไรดี?

Step1 : ต้องกำหนดขอบเขต (Scope) ที่จะทำ ISO 27001 ว่าระบบงานหรือกิจกรรมอะไรบ้างที่จะถูกควบคุมดูแลภายใต้ ISO 27001 เพื่อให้มั่นใจว่าสารสนเทศของระบบงาน หรือกิจกรรมนั้นๆ มีความมั่นคงปลอดภัย

Step2 : ทำการประเมินองค์กรเบื้องต้นให้รู้ว่าองค์กรยังขาดอะไรเมื่อเทียบกับสิ่งที่ต้องมีตามมาตรฐาน ISO 27001 ขั้นตอนนี้องค์กรจะต้องมีความรู้ในข้อกำหนดของ ISO 27001 ถึงจะประเมินได้อย่างถูกต้อง

สำหรับการเริ่มต้นมี 2 Step ข้างต้น หลังจากการประเมินองค์กรเบื้องต้นใน Step 2 องค์กรจะรู้ว่ายังขาดอะไรบ้าง มีประเด็นอะไรที่ยังไม่สอดคล้องตามกฎหมายหรือไม่ ถ้ามีให้สรุปประเด็นเสนอผู้บริหารเพื่อดำเนินการต่อไป

การนำมาตรฐาน ISO 27001 มาใช้งาน

1. **จัดทำระบบ (Establish)** การเตรียมการ วางแผนเพื่อปกป้องสารสนเทศ
2. **นำไปปฏิบัติ (Implement)** ทำตามเอกสารคู่มือและลงบันทึกในแบบฟอร์ม
3. **รักษาไว้ (Maintain)** ปฏิบัติควบคู่ไปกับการทำงานปกติ
4. **ปรับปรุงอย่างต่อเนื่อง (Continual Improvement)** ทบทวนผลการทำระบบและหาจุดปรับปรุงอย่างต่อเนื่อง

หลักการ CIA ใน ISO 27001

เน้นการปกป้องข้อมูลสารสนเทศ (Information) ให้มีคุณสมบัติ 3 ประการคือ

CONFIDENTIALITY ความลับ

INTEGRITY ความถูกต้องสมบูรณ์

AVAILABILITY ความพร้อมใช้

- **Confidentiality:** การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ ผู้ที่ไม่มีสิทธิเข้าถึงข้อมูลต้องไม่สามารถได้รับข้อมูลโดยเด็ดขาด
- **Integrity:** ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูล เป็นต้น
- **Availability:** สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน

การปกป้องข้อมูล (Information) จะเข้มงวดมากหรือน้อย ขึ้นอยู่กับ ***" ความเสี่ยง "*** หลักการคือ ข้อมูลใดที่เสี่ยงสูงย่อมต้องมีมาตรการปกป้องเข้มงวดกว่าข้อมูลที่มีความเสี่ยงต่ำ ตัวอย่างเช่น ข้อมูล username & password สำหรับเข้าสู่ระบบสารสนเทศขององค์กร ต้องมีมาตรการปกป้องที่เข้มงวดไม่น้อยกว่าข้อมูลทั่วไปที่ประกาศในเวบไซท์องค์กร เป็นต้น

ประเมินความเสี่ยงนั้นสำคัญอย่างไร

"การประเมินความเสี่ยงของสารสนเทศ (Information Security Risk Assessment)" เป็นหัวใจสำคัญของการทำระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO 27001 นั่นคือ หากเราประเมินความเสี่ยงไม่ถูกต้อง หรือไม่ครอบคลุมก็จะทำให้การจัดการความเสี่ยงที่ไม่ตรงจุด และไม่ครอบคลุม เปรียบเหมือนการตรวจร่างกาย ถ้าตรวจไม่ครบหรือตรวจไม่ละเอียดก็ไม่พบอาการป่วยและไม่ได้ทำการรักษา และเกิดผลรุนแรงตามมา

แนวทางจัดการความเสี่ยง

เมื่อประเมินความเสี่ยงของสารสนเทศ จนทราบแล้วว่ามีเรื่องอะไรบ้างที่มีความเสี่ยงทุกความเสี่ยงต้องมีคำตอบรองรับว่าความเสี่ยงแต่ละระดับจะจัดการอย่างไร โดยทั่วไปความเสี่ยงสูงจะมีการทำแผนงานจัดการความเสี่ยง (Risk Treatment) โดยมีมาตรการต่างๆ มาดูแลจัดการ จากนั้นเขียนเป็นคู่มือการปฏิบัติเพื่อให้ผู้ที่เกี่ยวข้องนำไปปฏิบัติให้ถูกต้องโดยประเด็นเรื่องกฎหมายเป็นหัวข้อหนึ่งที่สำคัญในการประเมินความเสี่ยง หากพบว่าประเมินความเสี่ยงแล้วพบว่าเป็นเรื่องผิดกฎหมายจะถือว่าเป็นความเสี่ยงสูงต้องรีบแก้ไขโดยด่วน

Information Security Management System (ISMS) Standard

หรือที่รู้จักกันในนาม ISO 27001 มีโครงสร้างข้อกำหนดทั้งหมด 10 ข้อดังนี้

ข้อ 0 บทนำ
ข้อ 1 ขอบข่าย
ข้อ 2 อ้างอิง
ข้อ 3 นิยามและคำจำกัดความ
ข้อ 4 บริบทองค์กร (Context of the organization)
ข้อ 5 ภาวะผู้นำ (Leadership)
ข้อ 6 การวางแผน (Planning)
ข้อ 7 การสนับสนุน (Support)
ข้อ 8 การดำเนินการ (Operation)
ข้อ 9 การประเมินสมรรถนะ (Performance evaluation)
ข้อ 10 การปรับปรุง (Improvement)

มีการให้แต่ละองค์กรนำข้อกำหนดไปปฏิบัติในข้อ 4-10 ดังนี้

ข้อ 4 บริบทขององค์กร (Context of the Organization)

4.1 ทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context) พื้นฐานสำคัญในการวางระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ ISO27001:2013 คือความเข้าใจบริบทขององค์กร โดยต้องระบุประเด็นภายใน (Internal issues) และประเด็นภายนอก (External issues) นำทั้ง2ประเด็นนี้มาพิจารณาในการวางระบบให้ครอบคลุมอย่างเหมาะสมไม่ตกหล่นประเด็นสำคัญ

4.2 กำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties) ในการทำ ISO 27001 จะต้องรู้ว่าใครคือผู้เกี่ยวข้อง (Interested parties) และพวกเขามีความต้องการและคาดหวังอะไร (needs and expectations) จากองค์กรของเรา ระบบงานใด มีความสำคัญเพราะเป็นงานที่เกี่ยวข้องกับความปลอดภัยหรือบริการให้กับผู้เกี่ยวข้อง

4.3 การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system) ขอบเขต (Scope) ของการทำ ISO27001:2013 ต้องพิจารณาถึงข้อกำหนดและความต้องการของผู้เกี่ยวข้อง(Interested parties) ตรงนี้เป็นเงื่อนไขสำคัญที่องค์กรต้องทำความเข้าใจและกำหนดขอบเขตให้เหมาะสมและเพียงพอ คือไม่กำหนดขอบเขตเล็กเกินไปจนตกหล่นผู้เกี่ยวข้อง หรือขอบเขตกว้างเกินกว่าความสามารถในการบริหารจัดการส่งผลให้ระบบขาดประสิทธิภาพ

4.4 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security management system) จัดทำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยจัดทำเอกสารที่เกี่ยวข้อง นำไปปฏิบัติและรักษาไว้ รวมถึงปรับปรุงอย่างต่อเนื่อง โดยISMSต้องสอดคล้องตามข้อกำหนดของ ISO27001:2013 Information Security Management System

ข้อ 5 ภาวะผู้นำ (Leadership)

5.1 ภาวะผู้นำและการให้ความสำคัญ (Leadership and commitment)

ผู้บริหารระดับสูงต้องแสดงให้เห็นถึงภาวะผู้นำและให้ความสำคัญต่อระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) เพื่อให้มั่นใจว่า มีการสื่อสารและนำข้อกำหนด ISMSมาเป็นส่วนหนึ่งของกระบวนการในองค์กรเพื่อให้ประสบความสำเร็จตามนโยบาย และวัตถุประสงค์ด้านความปลอดภัยของข้อมูล

5.2 นโยบาย (Policy)

ผู้บริหารระดับสูงกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับจุดประสงค์ขององค์กรเป็นเอกสารและสื่อสารนโยบายให้ผู้มีส่วนได้ส่วนเสียได้รับทราบ

5.3 บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ (Organizational roles, responsibilities and authorities) กำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยของสารสนเทศให้คนในองค์กรได้ทราบ

ข้อ 6 การวางแผน (Planning)

6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to Address Risks and Opportunities)

6.1.1 การวางแผนงานสำหรับระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ จะต้องพิจารณาถึงบริบทขององค์กร พิจารณาความเสี่ยงที่เกี่ยวข้องจากนั้นวางแนวทางจัดการอย่างเหมาะสม

6.1.2 การประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลตามลำดับ
- จัดตั้งเกณฑ์ในการประเมินความเสี่ยง
- หาความเสี่ยงว่ามีอะไรบ้าง ส่งผลกระทบทางด้าน CIA อย่างไร
- ประเมินความเสี่ยงว่าอยู่ในระดับใด (สูง,กลาง,ต่ำ)

6.1.3 การจัดการความเสี่ยง (Risk Treatment)
- ดูว่าปัจจุบันความเสี่ยงที่วิเคราะห์มา มีการควบคุมอะไรแล้วบ้าง
- จัดทำ Statement of Applicability (SOA) สำหรับการควบคุมที่จำเป็นตามข้อกำหนด
- หาแผนการจัดการความเสี่ยงที่ยังไม่ถูกควบคุม

6.2 วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information Security Objectives and Plans to Achieve Them) กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Objectives) และแผนการบรรลุวัตถุประสงค์โดยวัตถุประสงค์นี้จะต้องวัดผลได้และสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy)

ข้อ 7 การสนับสนุน (Support)

7.1 ทรัพยากร (Resources)

การทำระบบให้สำเร็จจำเป็นต้องมีทรัพยากรเพียงพอและเหมาะสม ประกอบด้วย บุคลากร เวลา งบประมาณและการสนับสนุนจากผู้บริหารอย่างเป็นรูปธรรม

7.2 ความสามารถ (Competence)

บุคลากรที่มีส่วนร่วมในการจัดทำระบบจะต้องมีความรู้ความสามารถซึ่งต้องมีการให้ความรู้ที่ตรงกับภาระหน้าที่เพื่อให้บุคลากรสามารถปฏิบัติได้อย่างถูกต้อง และต้องมีการเก็บบันทึกหลักฐานความสามารถเอาไว้

7.3 การสร้างความตระหนัก (Awareness)

ความตระหนักเป็นเรื่องสำคัญในด้านความมั่นคงปลอดภัยของสารสนเทศเพราะหากบุคลากรมีความตระหนักที่เพียงพอย่อมจะลดความเสี่ยงได้โดยปริยาย เช่น เรื่องการใช้รหัสผ่านที่แข็งแรงเดายากถ้าบุคลากรมีความตระหนักก็จะเข้าใจและปฏิบัติตามส่งผลการความเสี่ยงลดลง

7.4 การสื่อสาร (Communication)

การสื่อสารประกอบด้วยสื่อสารภายใน (Internal Communication) และการสื่อสารภายนอก (External Communication) เพื่อให้ความรู้ในความปลอดภัยของข้อมูล เป็นวิธีในการสร้างความตระหนักที่ได้ผลดี

7.5 เอกสารสารสนเทศ (Documented Information)

เอกสารมีความจำเป็นในการทำงานร่วมกันเพื่อให้เกิดความชัดเจนแก่ผู้ปฏิบัติและผู้ตรวจสอบ (Auditor) เอกสาร

ข้อ 8 การดำเนินการ (Operation)

8.1 การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational Planning and Control)
ข้อนี้กล่าวถึงการปฏิบัติตามแผนที่วางไว้ โดยลงมือปฏิบัติตามแผนจัดการความเสี่ยง

8.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessment)
ประเมินความเสี่ยงต้องทำเป็นระยะ ไม่ใช่ทำครั้งเดียวจบ เพราะเมื่อเวลาผ่านไปก็จะมีความเสี่ยงใหม่เกิดขึ้นมาไม่ว่าจะเป็นความเสี่ยงจากเทคโนโลยีใหม่ๆ หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบกับความปลอดภัยของข้อมูล

8.3 การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Treatment)
Information Security Risk Treatment เป็นเครื่องมือการจัดการความเสี่ยงที่จัดทำขึ้นภายหลังการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ โดยกำหนดรายละเอียด ขั้นตอนวิธีการต่างๆ เพื่อนำไปปฏิบัติให้ได้ผลลัพธ์ตามที่กำหนดไว้

ข้อ 9 การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

9.1 การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมิน (Monitoring, Measurement, Analysis and Evaluation)
เรื่องสำคัญที่พลาดไม่ได้คือ การเฝ้าระวัง (Monitor) การวัด (Measure) การวิเคราะห์ (Analyse) และการประเมิน (Evaluate) performance ของระบบ ทำให้รู้ได้ว่าผลลัพธ์เป็นไปตามที่วางแผนหรือไม่อย่างไร

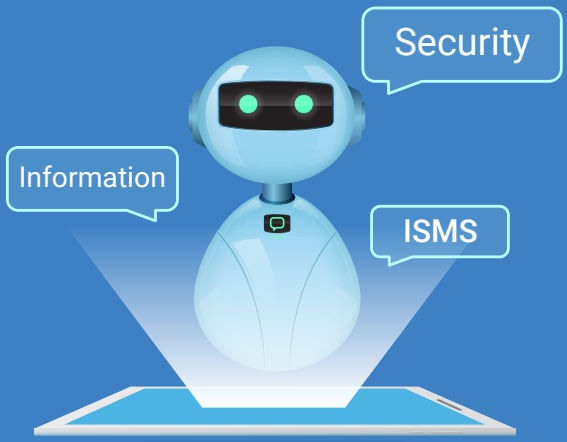
9.2 การตรวจประเมินภายใน (Internal Audit)
การตรวจประเมินภายใน (Internal Audit) เป็นเครื่องมือสำคัญที่ทำให้รู้ว่าระบบที่เราจัดทำขึ้นมานั้นมีความสมบูรณ์จัดทำครบถ้วนตามข้อกำหนด มีการนำไปปฏิบัติหรือไม่ และได้ผลลัพธ์เป็นอย่างไร ตรวจสอบความเข้าใจการปฏิบัติและเอกสารบันทึกที่เกี่ยวข้อง

9.3 การทบทวนของผู้บริหาร (Management Review)
Management Review เป็นการประชุมเพื่อรายงานผลของการจัดทำระบบ ISO 27001 : 2013 Information Security Management (ISMS) ต่อผู้บริหารระดับสูง (Top Management) โดยรายงานถึงการเปลี่ยนแปลงภายในและภายนอกที่มีผลกระทบต่อระบบฯ ผลการประเมินความเสี่ยงและการจัดการความเสี่ยง ผลการเฝ้าระวังด้าน Information Security ผลการตรวจประเมินภายใน (Internal Audit) ข้อบกพร่องจากการตรวจประเมินภายในและผลสะท้อนกลับจากผู้มีส่วนได้ส่วนเสีย

ข้อ 10 การปรับปรุง (Improvement)

10.1 ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and Corrective Action)
การระบุความไม่สอดคล้อง (Nonconformity) และแก้ไขความไม่สอดคล้อง (Corrective action) อย่างเป็นระบบ มีผู้รับผิดชอบและมีบันทึกที่เป็นลายลักษณ์อักษรเกี่ยวกับความไม่สอดคล้องและแนวทางการแก้ไข รวมทั้งทบทวนประสิทธิผลหลังการแก้ไข

10.2 การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)
องค์กรต้องปรับปรุงระบบให้มีความเหมาะสม เพียงพอ และมีการปรับปรุงอย่างต่อเนื่องเพื่อให้มีความปลอดภัยของข้อมูลเพิ่มมากขึ้น



0 - 2141 - 6282
itcenter@cdd.mail.go.th
www.cdd.go.th
กรมการพัฒนาชุมชน
กระทรวงมหาดไทย