- **ISO/IEC 27001 : 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements**

  มาตรฐานระบบการจัดการความมั่นคงปลอดภัยของข้อมูล

ISO/IEC 27001 เป็นมาตรฐานระบบการจัดการระบบการจัดการความปลอดภัยของข้อมูล เพื่อรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล โดยใช้กระบวนการจัดการความเสี่ยง และให้ความมั่นใจแก่ผู้มีส่วนได้ส่วนเสียว่าความเสี่ยงจะได้รับการจัดการอย่างเพียงพอ มาตรฐานนี้สามารถขอการรับรองจากหน่วยรับรองระบบ (Certification Body) ที่ให้บริการได้ โดยเป็นมาตรฐานสากลที่องค์กรธุรกิจทั่วโลกให้ความสำคัญ และสามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกประเภท ขนาด หรือลักษณะการดำเนินธุรกิจ เช่น ภาคการค้า หน่วยงานภาครัฐ และองค์กรไม่แสวงหากำไร

มาตรฐานนี้ ระบุข้อกำหนดสำหรับการจัดทำ นำไปปฏิบัติ รักษาไว้ และปรับปรุงระบบการจัดการความปลอดภัยของข้อมูลอย่างต่อเนื่องภายในบริบทขององค์กร เอกสารนี้ยังรวมถึงข้อกำหนดสำหรับการประเมินและการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลที่ปรับให้เหมาะกับความต้องการขององค์กร ข้อกำหนดที่กำหนดไว้ในเอกสารนี้เป็นข้อกำหนดทั่วไปและมุ่งหมายให้ใช้ได้กับทุกองค์กร โดยมีแนวคิดตามหลัก Plan-Do-Check-Act (PDCA)

ข้อกำหนดสำหรับการนำไปปฏิบัติ ประกอบด้วย

- ข้อ 4 บริบทขององค์กร (Context of the organization) : การจัดทำระบบการจัดการความมั่นคงปลอดภัยของข้อมูล (ISMS) องค์กรต้องเข้าใจบริบทองค์กร ความต้องการของผู้มีส่วนได้ส่วนเสีย และกำหนดขอบข่ายการจัดทำระบบ นโยบาย การระบุและประเมินความเสี่ยงขององค์กร ระบุแนวทางการจัดการกับความเสี่ยง เลือกวิธีการควบคุมและจัดการความเสี่ยง และจัดเตรียมคำชี้แจงการนำไปประยุกต์ใช้

- ข้อ 5 ภาวะผู้นำ (Leadership) : ความรับผิดชอบของฝ่ายบริหาร โดยการแสดงความมุ่งมั่นการให้ความสำคัญต่อระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล กำหนดนโนบาย และกำหนดบทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ขององค์กร

- ข้อ 6 การวางแผน (Planning) : การจัดทำแผนและดำเนินการ โดยการดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในฟังก์ชันและระดับงานที่เกี่ยวข้อง และการวางแผนรองรับการเปลี่ยนแปลง (กรณีที่มีการเปลี่ยนแปลง)

- ข้อ 7 การสนับสนุน (Support) : กำหนดและจัดสรรทรัพยากรที่จำเป็นสำหรับการกำหนด การนำข้อกำหนดไปสู่การปฏิบัติ การรักษาไว้ และการปรับปรุงอย่างต่อเนื่องสำหรับระบบ ISMS การกำหนดสมรรถนะและการพัฒนาบุคลากร และมีความตระหนักต่อการดำเนินงานของระบบ ISMS และการสื่อสารให้ทราบทั้งภายในและภายนอกองค์กร การจัดเตรียม ควบคุมบันทึกและเอกสาร และการจัดเก็บ

- ข้อ 8 การดำเนินการ (Operation) : การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม การประเมินความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล การจัดการกับความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล

- ข้อ 9 การประเมินสมรรถนะของการดำเนินงาน (Performance evaluation) : การเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมินผลการดำเนินงานเปรียบเทียบกับระบบ ISMS ที่กำหนด การตรวจประเมินภายในและการทบทวนของฝ่ายบริหาร

- ข้อ 10 การปรับปรุงอย่างต่อเนื่อง (Continual improvement) : การปรับปรุงความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผลของระบบ ISMS อย่างต่อเนื่อง และดำเนินการกับความไม่สอดคล้อง และการปฏิบัติการแก้ไข

Standard Warning System ของกฎระเบียบนี้ คือ

- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้น โดยพิจารณาจาก**เกณฑ์ระยะเวลาที่เหลือก่อนที่จะสิ้นสุดระยะเปลี่ยนถ่าย (Transition Period)** ของมาตรฐานที่มีการประกาศใช้ใหม่ เพื่อให้ผู้ประกอบการสามารถปรับตัวเข้าสู่มาตรฐานที่ประกาศใช้ใหม่ได้ภายในระยะเวลาที่กำหนด และ**เกณฑ์ระดับของการเปลี่ยนแปลงมาตรฐาน** ซึ่งจะพิจารณาจากสาระสำคัญของมาตรฐานที่มีการปรับปรุง เปลี่ยนแปลง ว่าอยู่ในระดับที่มีนัยสำคัญมากน้อยเพียงใด ซึ่งจะส่งผลต่อความสามารถ และทรัพยากรที่ใช้ในการปรับเปลี่ยนระบบเพื่อเข้าสู่มาตรฐานฯ ที่มีการประกาศใช้ใหม่

ซึ่งเมื่อพิจารณาจากปัจจัยต่างๆ แล้วพบว่ามาตรฐาน ISO/IEC 27001:2022 อยู่ใน**ระดับการเตือนภัยที่ต้องเฝ้าระวัง** ซึ่งเป็นผลมาจาก

- มาตรฐานฉบับนี้ ประกาศใช้แล้ว เมื่อวันที่ 10 ตุลาคม 2565 และมีระยะเวลาเปลี่ยนถ่าย (Transition Period) 3 ปี ซึ่งจะสิ้นสุดระยะเวลาเปลี่ยนถ่ายในวันที่ 24 ตุลาคม 2568

  สำหรับมาตรฐานฉบับปรับปรุงปี 2022 มีการเปลี่ยนแปลงโครงสร้างของข้อกำหนดมาตรฐาน โดยให้เป็นโครงสร้างเดียวกันกับมาตรฐานระบบการจัดการอื่นๆ เช่น ISO 9001, ISO 14001, ISO 45001 เพื่อให้องค์กรที่มีการประยุกต์ใช้หลายมาตรฐานสามารถบูรณาการระบบเข้าด้วยกันได้ การเพิ่มข้อกำหนดย่อยเกี่ยวกับการวางแผนการเปลี่ยนแปลง ข้อกำหนดใหม่ในการสร้างเกณฑ์สำหรับกระบวนการปฏิบัติงานและการดำเนินการควบคุมกระบวนการ และการเปลี่ยนแปลงที่สำคัญใน Annex โดยมีการรวมมาตรการควบคุม (Controls) บางตัว และบางตัวถูกลบออก มีการแนะนำมาตรการควบคุมใหม่ และส่วนอื่น ๆ ที่ปรับให้เป็นปัจจุบัน

- การเปลี่ยนแปลงดังกล่าวจึงพิจารณาว่าอยู่ในระดับมีนัยสำคัญ ซึ่งอาจส่งผลต่อความสามารถของผู้ประกอบการในการปรับเปลี่ยนระบบให้เข้าสู่มาตรฐานที่ประกาศใช้ใหม่ ผลการประเมินในแต่ละมุมมองผลกระทบมีรายละเอียดดังตาราง

องค์ประกอบ	การวิเคราะห์	ระดับผลกระทบ (สูง-ปานกลาง-ต่ำ)
1. ด้านระยะเวลา	ISO/IEC 27001:2022 ประกาศใช้ เมื่อวันที่ 10 ตุลาคม 2565 และมีระยะเวลาเปลี่ยนถ่าย (Transition Period) 3 ปี ซึ่งจะสิ้นสุดระยะเวลาเปลี่ยนถ่ายในวันที่ 24 ตุลาคม 2568 จึงมีระยะเวลาที่เหลือก่อนสิ้นสุดระยะเปลี่ยนถ่าย (Transition Period) มากกว่า 2 ปี	ปานกลาง
2. ด้านระดับของการเปลี่ยนแปลงมาตรฐาน	เนื่องจากมาตรฐานนี้ มีการกำหนดระยะเวลาเปลี่ยนถ่าย (Transition Period) จากมาตรฐานเดิมเพื่อเข้าสู่มาตรฐานฉบับใหม่ไว้ที่ 3 ปี จึงพิจารณาได้ว่ามาตรฐานที่ประกาศใช้ใหม่มีการเปลี่ยนแปลงเนื้อหา โครงสร้างของมาตรฐานอย่างมีนัยสำคัญ ซึ่งอาจส่งผลต่อความสามารถของผู้ประกอบการในการปรับเปลี่ยนระบบให้เข้าสู่มาตรฐานที่ประกาศใช้ใหม่	สูง

ระดับของการเปลี่ยนแปลงมาตรฐาน

ระดับความรุนแรง	ต่ำ	ปานกลาง	สูง
สูง			
ปานกลาง			ISO/IEC 27001:2022
ต่ำ			

ภาพ Warning Sign แสดง ระดับการเตือนภัยของมาตรฐาน ISO/IEC 27001:2022