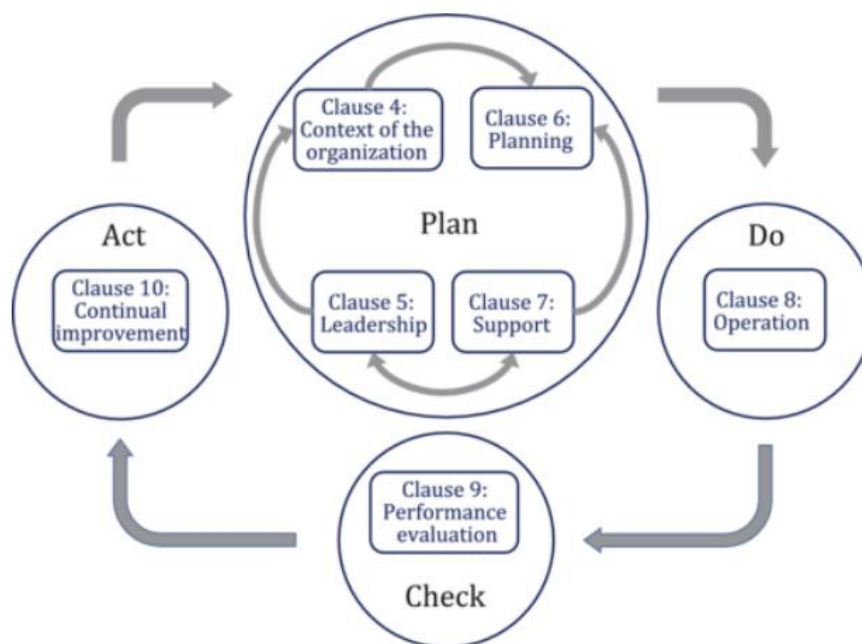


➤ ISO 28000 : 2022 Security and resilience — Security management systems — Requirements

มาตรฐานระบบการจัดการความมั่นคงปลอดภัยในโซ่อุปทาน

ISO 28000 เป็นมาตรฐานระบบการจัดการความมั่นคงปลอดภัย โดยมีการปรับเปลี่ยนโครงสร้างของมาตรฐานให้สอดคล้องไปกับมาตรฐานระบบการจัดการอื่นที่ประกาศใช้ในปัจจุบัน ตามหลัก PDCA เช่น ระบบการจัดการคุณภาพ ระบบการจัดการสิ่งแวดล้อม และสามารถขอการรับรองจากหน่วยรับรองระบบ (Certification Body) ที่ให้บริการได้



PDCA Model applied to the security management systems

มาตรฐานนี้ระบุข้อกำหนดสำหรับระบบการจัดการความมั่นคงปลอดภัย รวมถึงประเด็นที่มีความสำคัญต่อการประกันความปลอดภัยของห่วงโซ่อุปทาน โดยระบุให้องค์กร:

- ประเมินสภาพแวดล้อมของความมั่นคงปลอดภัยที่องค์กรดำเนินการเอง รวมถึงในห่วงโซ่อุปทาน
- พิจารณาว่ามีการใช้มาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอเพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยอย่างมีประสิทธิภาพหรือไม่
- บริหารจัดการการปฏิบัติให้สอดคล้องตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดแบบสมัครใจ ที่องค์กรติดตามหรือเป็นสมาชิก

- ถ่ายทอดแนวทางการดำเนินกระบวนการและมาตรการควบคุมด้านความมั่นคงปลอดภัย ที่รวมถึงกระบวนการต้นน้ำและปลายน้ำที่เกี่ยวข้อง และการควบคุมของห่วงโซ่อุปทาน เพื่อให้เป็นไปตามวัตถุประสงค์ขององค์กร

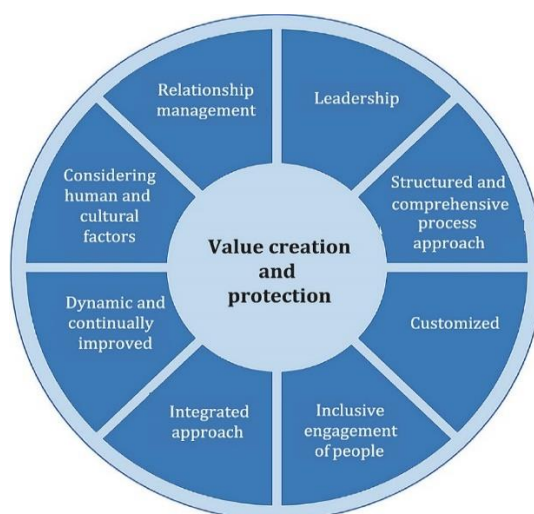
มาตรฐานนี้สามารถนำไปใช้กับองค์กรใดๆ ทุกสถานที่ตั้ง ขนาด กลุ่มประเภท รูปแบบการดำเนินธุรกิจ และอุตสาหกรรม (เช่น องค์กรการค้า รัฐบาลหรือหน่วยงานสาธารณะอื่นๆ และองค์กรไม่แสวงหาผลกำไร) และสามารถนำไปใช้กับกิจกรรมใดๆ ทั้งภายในและภายนอก ในทุกระดับ

องค์กรสามารถยืนยันความสอดคล้องกับมาตรฐานโดยการตรวจประเมินภายในหรือโดยหน่วยรับรองที่เป็นบุคคลที่สาม

มาตรฐานนี้ ประกอบด้วย ส่วนที่เป็นข้อกำหนดทั่วไป คือ ข้อ 1 – ข้อ 3 และส่วนที่เป็นข้อกำหนดสำหรับนำไปปฏิบัติ คือ ข้อ 4 – ข้อ 10 และภาคผนวก (Annex) ดังนี้

บทนำ

1. ขอบข่าย
2. เอกสารอ้างอิง (Informative reference)
3. ศัพท์และนิยามศัพท์ : มีจำนวน 21 รายการ
4. บริบทองค์กร การทำความเข้าใจและกำหนดระบบการจัดการความมั่นคงปลอดภัย ที่เหมาะสม โดยองค์กรต้องมี
 - 4.1 การเข้าใจบริบทองค์กร
 - 4.2 การเข้าใจความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย (ตาม Principles of Value Creation and Protection)
 - 4.3 การกำหนดขอบข่ายของระบบการจัดการความมั่นคงปลอดภัยขององค์กร
 - 4.4 ระบบการจัดการความมั่นคงปลอดภัยสำหรับองค์กร โดยองค์กรต้องจัดทำ นำไปปฏิบัติ คงไว้ และปรับปรุงอย่างต่อเนื่อง



Principles of Value Creation and Protection

5. ความпенผู้นำ การทำความเข้าใจบทบาท หน้าที่ความรับผิดชอบ นโยบาย และอำนาจหน้าที่ขององค์กร ต้องรวมถึง

5.1 ความпенผู้นำและความมุ่งมั่น โดยผู้บริหารระดับสูงขององค์กรต้องแสดงให้เห็นถึงภาวะผู้นำและความมุ่งมั่นในการยอมรับต่อระบบการจัดการความมั่นคงปลอดภัย

5.2 นโยบาย โดยผู้บริหารระดับสูงต้องกำหนดนโยบายการจัดการความมั่นคงปลอดภัย

5.3 บทบาท ความรับผิดชอบ และอำนาจหน้าที่ โดยผู้บริหารระดับสูงต้องทำให้มั่นใจว่ามีการมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทที่เกี่ยวข้อง และสื่อสารภายในองค์กร

6. การวางแผน การทำความเข้าใจความเสี่ยง วัตถุประสงค์เชิงกลยุทธ์ และนโยบายในปัจจุบันครอบคลุมถึง

6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส

6.2 วัตถุประสงค์ความมั่นคงปลอดภัย และการวางแผนเพื่อบรรลุตามวัตถุประสงค์

6.3 แผนรองรับการเปลี่ยนแปลง เมื่อระบบการจัดการความมั่นคงปลอดภัยมีการเปลี่ยนแปลงจะต้องดำเนินการในลักษณะที่วางแผนไว้

7. การสนับสนุน

7.1 ทรัพยากร : กำหนดและจัดหาทรัพยากรทั้งหมดที่จำเป็น สำหรับการจัดทำ นำไปปฏิบัติ รักษาไว้ และการปรับปรุงอย่างต่อเนื่องสำหรับระบบการจัดการความมั่นคงปลอดภัย

7.2 ความรู้ ความสามารถของบุคลากร : ต้องกำหนดความรู้ ความสามารถที่จำเป็นของบุคลากรที่ปฏิบัติงานภายใต้การควบคุมขององค์กรที่มีผลกระทบต่อผลการดำเนินงานด้านความมั่นคงปลอดภัย ต้องทำให้มั่นใจว่าความสามารถอยู่บนพื้นฐานการศึกษา การฝึกอบรม และประสบการณ์ที่เหมาะสม และต้องมีการประเมินผลความสามารถของบุคลากร

7.3 ความตระหนัก : บุคลากรที่ต้องตระหนักถึงนโยบายความมั่นคงปลอดภัย การสนับสนุนของบุคลากรเพื่อให้เกิดประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัย ความหมายของความไม่สอดคล้องตามข้อกำหนดมาตรฐาน และบทบาทหน้าที่ในการทำให้บรรลุตามนโยบาย ข้อปฏิบัติ และการเตรียมความพร้อมต่อสถานการณ์ฉุกเฉินและการตอบสนอง

7.4 การสื่อสาร: กำหนดความต้องการของการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัย รวมถึง ข้อมูลอะไรที่จะสื่อสาร จะสื่อสารเมื่อใด จะสื่อสารข้อมูลกับใคร ใช้วิธีการสื่อสารอะไร และการเรียงลำดับความสำคัญของข้อมูลที่จะสื่อสาร

7.5 เอกสารสารสนเทศ: ต้องรวมถึงเอกสารสารสนเทศที่กำหนดโดยมาตรฐานนี้ และเอกสารสารสนเทศที่กำหนดโดยองค์กรว่าจำเป็นต่อประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัย การจัดทำ และปรับปรุงให้ทันสมัย และการควบคุมเอกสารสารสนเทศ

8. การดำเนินการ

8.1 การวางแผนและควบคุมการปฏิบัติงาน: องค์กรต้องวางแผน นำไปปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้เป็นไปตามข้อกำหนดและเพื่อนำการดำเนินงานต่างๆ ไปปฏิบัติตามที่กำหนดไว้



8.2 การระบุกระบวนการและกิจกรรมที่จำเป็นเพื่อให้บรรลุความสอดคล้องกับนโยบายความมั่นคงปลอดภัย และกฎหมาย กฎระเบียบ และข้อกำหนดด้านความมั่นคงปลอดภัย วัตถุประสงค์ของการจัดการความมั่นคงปลอดภัย การส่งมอบกิจกรรมต่างๆ ของระบบการจัดการความมั่นคงปลอดภัย และระดับความต้องการด้านความปลอดภัยในห่วงโซ่อุปทาน

8.3 การประเมินความเสี่ยงและการแก้ไข โดยต้องมีกระบวนการจัดการตามที่อยู่ใน ISO 31000

8.4 การควบคุม: ตามกระบวนการควบคุมในข้อ 8.2 จะต้องรวมถึงการควบคุมการจัดการทรัพยากรมนุษย์ การออกแบบ การติดตั้ง การดำเนินการ การทำใหม่ และการปรับปรุงเปลี่ยนแปลง ของอุปกรณ์ เครื่องมือ และสารสนเทศ ที่เกี่ยวข้องกับความปลอดภัยอย่างเหมาะสม

8.5 กลยุทธ์ความมั่นคงปลอดภัย ขั้นตอนดำเนินการ กระบวนการ และการดูแลรักษา

8.6 แผนความมั่นคงปลอดภัย

9. การประเมินสมรรถนะ โดยเปรียบเทียบกับมาตรฐาน การเฝ้าระวัง และการปฏิบัติตามข้อกำหนดที่เป็นเป้าหมาย ประกอบด้วย

9.1 การตรวจติดตาม การตรวจวัด การวิเคราะห์ และการประเมินผล

9.2 การตรวจประเมินภายใน

9.3 การทบทวนฝ่ายบริหาร

10. การปรับปรุง ประกอบด้วย

10.1 การปรับปรุงอย่างต่อเนื่อง สำหรับความเหมาะสม ความเพียงพอ และประสิทธิผลของระบบความมั่นคงปลอดภัย

10.2 สิ่งที่ไม่เป็นไปตามข้อกำหนดและการปฏิบัติการแก้ไข (Nonconformity and corrective action) ต้องมีการจัดการที่เหมาะสม

Standard Warning System ของกฎระเบียบนี้ คือ



- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้น โดยพิจารณาจากเกณฑ์ระยะเวลาที่เหลือน้อยกว่าที่จะสิ้นสุดระยะเปลี่ยนถ่าย (Transition Period) ของมาตรฐานที่มีการประกาศใช้ใหม่ เพื่อให้ผู้ประกอบการสามารถปรับตัวเข้าสู่มาตรฐานที่ประกาศใช้ใหม่ได้ภายในระยะเวลาที่กำหนด และเกณฑ์ระดับของการเปลี่ยนแปลงมาตรฐาน ซึ่งจะพิจารณาจากสาระสำคัญของมาตรฐานที่มีการปรับปรุง เปลี่ยนแปลง ว่าอยู่ในระดับที่มีนัยสำคัญมากน้อยเพียงใด ซึ่งจะส่งผลกระทบต่อความสามารถ และทรัพยากรที่ใช้ในการปรับเปลี่ยนระบบเพื่อเข้าสู่มาตรฐานฯ ที่มีการประกาศใช้ใหม่

ซึ่งเมื่อพิจารณาจากปัจจัยต่างๆ แล้วพบว่ามาตรฐาน ISO 28000:2022 อยู่ในระดับการเตือนภัยที่ต้องเร่งดำเนินการ ซึ่งเป็นผลมาจาก

- มาตรฐานฉบับนี้ ประกาศใช้แล้ว เมื่อวันที่ 15 มีนาคม 2565 และมีระยะเวลาเปลี่ยนถ่าย (Transition Period) 3 ปี ซึ่งจะสิ้นสุดระยะเวลาเปลี่ยนถ่ายในวันที่ 14 มีนาคม 2568
- สำหรับมาตรฐานฉบับปรับปรุงปี 2022 มีการเปลี่ยนแปลงโครงสร้างของข้อกำหนดมาตรฐาน โดยให้เป็นโครงสร้างเดียวกันกับมาตรฐานระบบการจัดการอื่นๆ เช่น ISO 9001, ISO 14001, ISO 45001 เพื่อให้องค์กรที่มีการประยุกต์ใช้หลายมาตรฐานสามารถบูรณาการระบบเข้าด้วยกันได้ และมีการปรับบางข้อกำหนดให้สอดคล้องกับมาตรฐานด้านการจัดการความเสี่ยง (ISO 31000) และการบริหารความต่อเนื่องทางธุรกิจ (ISO 22301) การเปลี่ยนแปลงดังกล่าวจึงพิจารณาว่าอยู่ในระดับมีนัยสำคัญ ซึ่งอาจส่งผลกระทบต่อความสามารถของผู้ประกอบการในการปรับเปลี่ยนระบบให้เข้าสู่มาตรฐานที่ประกาศใช้ใหม่ ผลการประเมินในแต่ละมุมมองผลกระทบมีรายละเอียดดังตาราง

องค์ประกอบ	การวิเคราะห์	ระดับผลกระทบ (สูง-ปานกลาง-ต่ำ)
1. ด้านระยะเวลา	ISO 28000:2022 ประกาศใช้ เมื่อวันที่ 15 มีนาคม 2565 และมีระยะเวลาเปลี่ยนถ่าย (Transition Period) 3 ปี ซึ่งจะสิ้นสุดระยะเวลาเปลี่ยนถ่ายในวันที่ 14 มีนาคม 2568 จึงมีระยะเวลาที่เหลือก่อนสิ้นสุดระยะเวลาเปลี่ยนถ่าย (Transition Period) ภายใน 1-2 ปี	ปานกลาง
2. ด้านระดับของการเปลี่ยนแปลงมาตรฐาน	เนื่องจากมาตรฐานนี้ มีการกำหนดระยะเวลาเปลี่ยนถ่าย (Transition Period) จากมาตรฐานเดิมเพื่อเข้าสู่มาตรฐานฉบับใหม่ไว้ที่ 3 ปี จึงพิจารณาได้ว่ามาตรฐานที่ประกาศใช้ใหม่มีการเปลี่ยนแปลงเนื้อหา โครงสร้างของมาตรฐาน อย่างมีนัยสำคัญ ซึ่งอาจส่งผลกระทบต่อความสามารถของผู้ประกอบการในการปรับเปลี่ยนระบบให้เข้าสู่มาตรฐานที่ประกาศใช้ใหม่	สูง

ระดับของการเปลี่ยนแปลงมาตรฐาน

	ต่ำ	ปานกลาง	สูง
สูง			
ปานกลาง			ISO 28000:2022
ต่ำ			

ภาพ Warning Sign แสดง ระดับการเตือนภัยของมาตรฐาน ISO 28000:2022