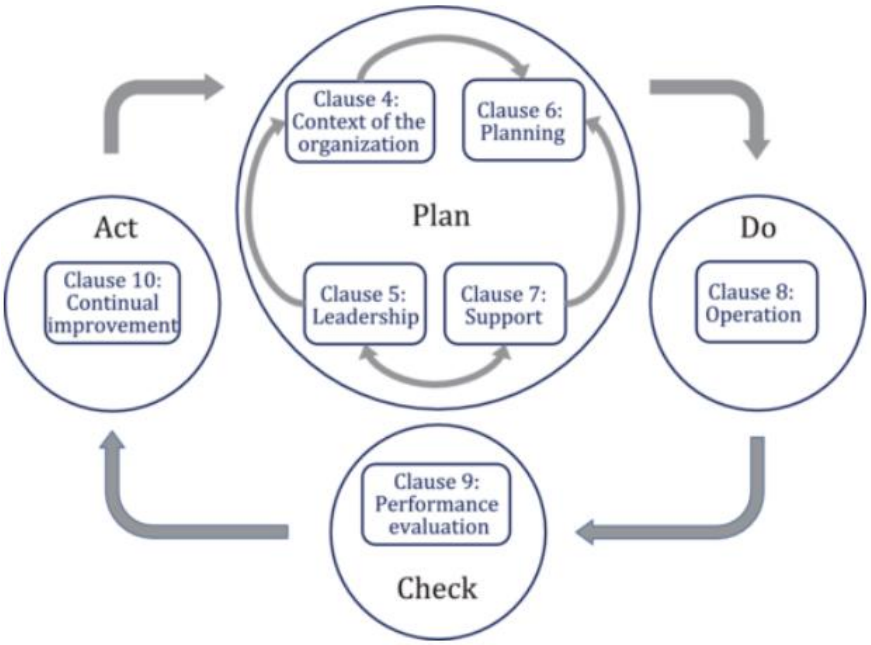
➢ **ISO 28000 : 2022 Security and resilience — Security management systems — Requirements**

มาตรฐานระบบการจัดการความมั่นคงปลอดภัย

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



PDCA Model applied to the security management systems

มาตรฐานนี้ระบุข้อกำหนดสำหรับระบบการจัดการความมั่นคงปลอดภัย รวมถึงประเด็นที่มีความสำคัญต่อการประกันความปลอดภัยของห่วงโซ่อุปทาน ต้องการให้องค์กร:

- ประเมินสภาพแวดล้อมการรักษาความปลอดภัยที่ดำเนินการรวมถึงห่วงโซ่อุปทาน (รวมถึงการพึ่งพาและการพึ่งพาซึ่งกันและกัน)
- พิจารณาว่ามีการใช้มาตรการรักษาความปลอดภัยที่เพียงพอเพื่อจัดการความเสี่ยงด้านความปลอดภัยอย่างมีประสิทธิผลหรือไม่
- จัดการการปฏิบัติตามภาระผูกพันตามกฎหมาย ระเบียบข้อบังคับ และโดยสมัครใจที่องค์กรสมัครเป็นสมาชิก

- จัดแนวกระบวนการและการควบคุมด้านความปลอดภัย รวมถึงกระบวนการต้นน้ำและปลายน้ำที่เกี่ยวข้องและการควบคุมของห่วงโซ่อุปทานเพื่อให้เป็นไปตามวัตถุประสงค์ขององค์กร

มาตรฐานนี้สามารถนำไปใช้กับองคกรใดๆ ทุกสถานที่ตั้ง ขนาด กลุมประเภท รูปแบบการดำเนินธุรกิจ และอุตสาหกรรม (เช่น องค์กรการค้า รัฐบาลหรือหน่วยงานสาธารณะอื่นๆ และองค์กรไม่แสวงหาผลกำไร) และสามารถนำไปใช้กับกิจกรรมใดๆ ทั้งภายในและภายนอก ในทุกระดับ

องค์กรสามารถยืนยันความสอดคล้องกับมาตรโดยการตรวจสอบภายในหรือโดยหน่วยงานรับรองที่เป็นบุคคลที่สามที่ได้รับการรับรอง

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

บทนำ

1. ขอบขาย

2. เอกสารอางอิง (Informative reference) : ISO 22300, Security and resilience - Vocabulary

3. ศัพทและนิยามศัพท : มีจำนวน 21 ข้อ ตาม ISO 22300, Security and resilience - Vocabulary

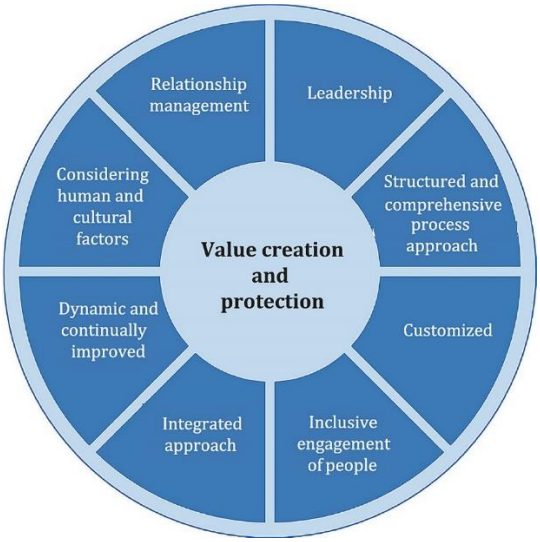
4. บริบทองคกร: การทำความเข้าใจและกำหนดระบบการจัดการความมั่งคงปลอดภัย ที่เหมาะสม โดยองค์กรต้องมี

4.1 การเขาใจบริบทองคกร

4.2 การเขาใจความตองการและความคาดหวังของผูมีสวนได เสีย (ตาม Principles of Value Creation and Protection)

4.3 การกำหนดขอบขายของระบบการจัดการความมั่งคงปลอดภัยขององค์กร

4.4 ระบบการจัดการความมั่งคงปลอดภัยสำหรับองคกร โดยองค์กรต้องจัดทำ นำไปปฏิบัติ คงไว้และปรับปรุงอย่างต่อเนื่อง



Principles of Value Creation and Protection

5. ความเป็นผู้นำ: การทำความเข้าใจบทบาท หน้าที่ความรับผิดชอบ นโยบาย และอำนาจหน้าที่ขององค์กร ต้องรวมถึง

5.1 ความเป็นผู้นำและความมุ่งมั่น โดยผู้บริหารระดับสูงขององค์กรต้องแสดงให้เห็นถึงภาวะผู้นำและความมุ่งมั่นในการยอมรับต่อระบบการจัดการความมั่นคงปลอดภัย

5.2 นโยบาย โดยผู้บริหารระดับสูงต้องกำหนดนโยบายการจัดการความมั่นคงปลอดภัย

5.3 บทบาท ความรับผิดชอบ และอำนาจหน้าที่ โดยผู้บริหารระดับสูงต้องทำให้มั่นใจว่ามีการมอบหมายหน้าที่ความรับผิดชอบและอำนาจหน้าที่ตามบทบาทเกี่ยวข้อง และสื่อสารภายในองค์กร

6. การวางแผน: การทำความเข้าใจความเสี่ยง วัตถุประสงค์เชิงกลยุทธ์ และนโยบายในปัจจุบันครอบคลุมถึง

6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส

6.2 วัตถุประสงค์ความมั่นคงปลอดภัย และการวางแผนเพื่อบรรลุตามวัตถุประสงค์

6.3 แผนของการเปลี่ยนแปลง เมื่อระบบการจัดการความมั่นคงปลอดภัยมีการเปลี่ยนแปลงจะต้องดำเนินการในลักษณะที่วางแผนไว้

7. การสนับสนุน:

7.1 ทรัพยากร : กำหนดและจัดหาทรัพยากรทั้งหมดที่จำเปน สำหรับการจัดทำ นำไปปฏิบัติ รักษาไว และการปรับปรุงอยางตอเนื่องสำหรับระบบการจัดการความมั่นคงปลอดภัย

7.2 ความรู ความสามารถของบุคลากร : ต้องกำหนดความรู ความสามารถที่จำเปนของบุคลากรที่ปฏิบัติงานภายใตการควบคุมขององคกรทีมีผลกระทบต่อผลการดำเนินงานด้านความมั่นคงปลอดภัย ต้องทำให้มั่นใจว่าความสามารถอยู่บนพื้นฐานการศึกษา การฝึกอบรม และประสบการณ์ที่เหมาะสม และต้องมีการประเมินผลความสามารถของบุคลากร

7.3 ความตระหนัก : บุคลากรที่ต่องตระหนักถึงนโยบายความมั่นคงปลอดภัย การสนับสนุนของบุคลากรเพื่อให้เกิดประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัย ความหมายของความไม่สอดคล้องตามข้อกำหนดมาตรฐาน และบทบาทหน้าที่ในการทำให้บรรลุตามนโยบาย ข้อปฏิบัติ และการเตรียมความพร้อมต่อสถานการณ์ฉุกเฉินและการตอบสนอง

7.4 การสื่อสาร: กำหนดกความต้องการของสื่อสารภายในและภายนอกที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัย รวมถึง ข้อมูลอะไรที่จะสื่อสาร จะสื่อสารเมื่อไหร่ จะสื่อสารข้อมูลกับใคร วิธีการสื่อสารคืออะไร และการเรียงลำดับความสำคัญของข้อมูลที่จะสื่อสาร

7.5 เอกสารสารสนเทศ: ต่องรวมถึงเอกสารสารสนเทศที่กำหนดโดยมาตรฐานนี้ และเอกสารสารสนเทศที่กำหนดโดยองค์กรว่าจำเป็นต่อประสิทธิผลของระบบการจัดการความมั่นคงปลอดภัย การจัดทำและปรับปรุงใหทันสมัย และการควบคุมเอกสารสารสนเทศ

8. การดำเนินการ

8.1 การวางแผนและควบคุมการปฏิบัติงาน: องค์กรต้องวางแผน นำไปปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้เป็นไปตามข้อกำหนดและเพื่อนำการดำเนินงานต่างๆไปปฏิบัติตามที่กำหนดไว้

8.2 การระบุกระบวนการและกิจกรรมที่จำเป็นเพื่อให้บรรลุความสอดคล้องกับนโยบายความมั่นคงปลอดภัย และกฎหมาย กฎระเบียบ และข้อกำหนดด้านความมั่นคงปลอดภัย วัตถุประสงค์ของการจัดการความมั่นคงปลอดภัย การส่งมอบของระบบการจัดการความมั่นคงปลอดภัย และระดับความต้องการด้านความปลอดภัยในห่วงโซ่อุปทาน

8.3 การประเมินความเสี่ยงและการแก้ไข โดยต้องมีกระบวนการจัดการตามที่ระบุใน ISO 31000

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

8.5 กลยุทธ์ความมั่นคงปลอดภัย ขั้นตอนดำเนินการ กระบวนการ และการดูแลรักษา

8.6 แผนความมั่นคงปลอดภัย

9. การประเมินสมรรถนะ: การเปรียบเทียบกับมาตรฐาน การเฝ้าระวัง และการปฏิบัติตามข้อกำหนดที่เป็นเป้าหมาย ประกอบด้วย

9.1 การตรวจติดตาม การตรวจวัด การวิเคราะห และการประเมินผล

9.2 การตรวจประเมินภายใน

9.3 การทบทวนฝ่ายบริหาร

10. การปรับปรุง: ประกอบด้วย

10.1 การปรับปรุงอย่างต่อเนื่อง สำหรับความเหมาะสม ความเพียงพอ และประสิทธิผลของระบบความมั่นคงปลอดภัย

10.2 สิ่งที่ไมเปนไปตามขอกำหนดและการปฏิบัติการแกไข (Nonconformity and corrective action) ต้องมีการจัดการที่เหมาะสม

Standard Warning System ของกฎระเบียบนี้ คือ

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

  ซึ่งเมื่อพิจารณาจากปัจจัยต่างๆ แล้วพบว่ามาตรฐาน ISO 28000:2022 อยู่ใน**ระดับการเตือนภัยที่ต้องเฝ้าระวัง** 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 ซึ่งอาจส่งผลต่อความสามารถของผู้ประกอบการในการปรับเปลี่ยนระบบให้เข้าสู่มาตรฐานที่ประกาศใช้ใหม่ 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 จึงมีระยะเวลาที่เหลือก่อนสิ้นสุดระยะเปลี่ยนถ่าย (Transition Period) มากกว่า 2 ปี	ต่ำ
2. ด้านระดับของการเปลี่ยนแปลงมาตรฐาน	เนื่องจากมาตรฐานนี้ มีการกำหนดระยะเวลาเปลี่ยนถ่าย (Transition Period) จากมาตรฐานเดิมเพื่อเข้าสู่มาตรฐานฉบับใหม่ไว้ที่ 3 ปี จึงพิจารณาได้ว่ามาตรฐานที่ประกาศใช้ใหม่มีการเปลี่ยนแปลงเนื้อหา โครงสร้างของมาตรฐานอย่างมีนัยสำคัญ ซึ่งอาจส่งผลต่อความสามารถของผู้ประกอบการในการปรับเปลี่ยนระบบให้เข้าสู่มาตรฐานที่ประกาศใช้ใหม่	สูง

ระดับของการเปลี่ยนแปลงมาตรฐาน

ระดับผลกระทบ	ต่ำ	ปานกลาง	สูง
สูง			
ปานกลาง			
ต่ำ			ISO 28000:2022

ภาพ Warning Sign แสดง ระดับการเตือนภัยของมาตรฐาน ISO 28000:2022