ISO/IEC 27001:2022 Revision

Learn from the experts

1. การเปลี่ยนแปลงที่สำคัญในมาตรฐานเวอร์ชั่นใหม่คืออะไร

การเปลี่ยนแปลงที่สำคัญในการแก้ไขมาตรฐานนี้อยู่ใน Annex A ซึ่งสอดคล้องกับการเปลี่ยนแปลงในมาตรฐาน ISO/IEC 27002:2022 การเปลี่ยนแปลงเหล่านี้ได้แก่:

- **โครงสร้างโดยรวมได้รับการปรับปรุงเป็น 4 ส่วนหลัก** : องค์การ ทางบุคคล ทางกายภาพ และเทคโนโลยี แทน 14 ส่วนในฉบับก่อนหน้านี้
- **มาตรการควบคุม (Controls) ลดลงจาก 114 เหลือ 93 รายการ**
- **มีการนำแอททริบิวต์ (Attributes) มาใช้**

นอกจากนี้ยังมีการเปลี่ยนแปลงด้านบทบรรณาธิการได้แก่:

- คำว่า "International standard" แทนที่ด้วยคำว่า "Document" ทั้งหมด
- การจัดเรียงวลีภาษาอังกฤษบางส่วนใหม่เพื่อให้เข้าใจง่ายขึ้น

นอกจากนี้ยังมีการเปลี่ยนแปลงเพื่อให้สอดคล้องกับแนวทาง ISO ได้แก่:

- การจัดโครงสร้างตัวเลขใหม่
- ข้อกำหนดในการกำหนดกระบวนการที่จำเป็นสำหรับการนำ ISMS ไปปฏิบัติและปฏิสัมพันธ์ของกระบวนการเหล่านั้น
- ข้อกำหนดที่ชัดเจนในการสื่อสารบทบาทองค์กรที่เกี่ยวข้องกับความปลอดภัยของข้อมูลภายในองค์กร
- ข้อ 6.3 (ข้อใหม่) – การวางแผนการเปลี่ยนแปลง
- มีข้อกำหนดใหม่เพื่อให้มันใจว่าองค์กรกำหนดวิธีการสื่อสารซึ่งเป็นส่วนหนึ่งของข้อ 7.4
- มีข้อกำหนดใหม่ในการสร้างเกณฑ์สำหรับกระบวนการปฏิบัติงานและการดำเนินการควบคุมกระบวนการ

2. มีการเผยแพร่มาตรฐานในปี 2022 หรือไม่

ใช่ มาตรฐาน ISO 27001:2022 ได้รับการเผยแพร่แล้วเมื่อปลายเดือนตุลาคม ปี 2022

3. การปฏิบัติงานตามมาตรฐาน ISO/IEC 27002:2022 เพื่อปรับเปลี่ยนไปสู่มาตรฐาน ISO/IEC 27001:2022 จำเป็นหรือไม่

แม้ว่าจะไม่จำเป็น แต่การอัปเดตมาตรฐาน ISO/IEC 27002:2022 ในตอนนี้จะทำให้เกิด "heavy lifting" หลายอย่างเกี่ยวกับการจัดกลุ่ม แอททริบิวต์ (Attributes) และคำอธิบายใหม่ ๆ ซึ่งทำให้ง่ายต่อการนำมาตรการควบคุมของ ISO/IEC 27001:2022 ไปใช้อย่างมีประสิทธิภาพและช่วยทำให้มีความสอดคล้องกับกรอบความปลอดภัยทางไซเบอร์และวิธีการจัดการความเสี่ยงอื่น ๆ ได้ง่ายขึ้น

4. หากเรากำลังใช้มาตรฐาน ISO/IEC 27001:2013 เราจะยังสามารถรับรอง ISMS ของเราเป็นเวอร์ชั่น 2013 ได้หรือไม่

ได้ อย่างไรก็ตาม คุณจะต้องดำเนินการภายในวันที่ 31 ตุลาคม ปี 2023 หลังจากนั้น คุณจะต้องเปลี่ยนไปใช้เวอร์ชั่น 2022 ก่อนสิ้นสุดระยะเวลาการปรับเปลี่ยน

5. หากเรามีระยะเวลาในการปรับเปลี่ยนจนถึงเดือนตุลาคม ปี 2025 เหตุใดเราจึงควรดำเนินการในตอนนี้

การปรับเปลี่ยนดังกล่าวจะสะท้อนถึงความก้าวหน้าของวิธีการทำงานของเราและภัยคุกคามที่เกี่ยวข้องอีกทั้งยังทำให้การใช้งานมีความชัดเจนและยืดหยุ่นมากขึ้น ดังนั้นจึงเป็นเรื่องสำคัญที่จะต้องเริ่มต้นการปรับเปลี่ยนโดยเร็วที่สุดเพื่อ:

- ตรวจสอบให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคุณสะท้อนถึง Digital Business Profile ในปัจจุบันของคุณและความเสี่ยงที่เกี่ยวข้อง
- ให้ได้รับประโยชน์สูงสุดจากโครงสร้างการควบคุมที่ยืดหยุ่นมากขึ้น ซึ่งตอนนี้สามารถทำให้สอดคล้องกับกรอบการทำงานด้านการรักษาความปลอดภัยทางไซเบอร์ทั่วโลกได้อย่างง่ายดาย
- ปรับปรุงประสิทธิภาพของระบบบริหารจัดการของคุณโดยทำให้สอดคล้องกับ Harmonized Structure ล่าสุดสำหรับระบบบริหารจัดการ

6. จะมีการจัดการฝึกอบรมหรือไม่ ถ้ามี จะเปิดสอนหลักสูตรใดบ้างและเมื่อไหร่

มีการจัดการฝึกอบรม หลักสูตรใหม่ของเราได้แก่ "ISO/IEC 27001:2022 Auditor Transition" และ "ISO/IEC 27002:2022 Implementing the Changes" ยังมีหลักสูตรการฝึกอบรมแบบ on-demand และหลักสูตร Instructor-Led Training (ILT) นอกจากนี้ หลักสูตรการฝึกอบรม ISO/IEC 27001 ทั้งหมดของเรายังได้รับการปรับปรุงเป็นเวอร์ชั่นปี 2022 แล้ว ดูหลักสูตร ISMS ของเราที่นี่ https://www.bsigroup.com/th-TH/ISOIEC-27001-Information-Security/Training-course/

7. มีระยะเวลาในการปรับเปลี่ยนอย่างไร

จะมีระยะเวลาในการปรับเปลี่ยน 3 ปี เริ่มตั้งแต่ 1 พฤศจิกายน ปี 2022 ถึงวันที่ 31 ตุลาคม ปี 2025

8. การเปลี่ยนแปลงมีผลกระทบต่อ ISMS ของเราอย่างไร

ผลกระทบหลักคือความจำเป็นในการทบทวนการประเมินความเสี่ยงและจัดทำเอกสารแสดงการประยุกต์ใช้เพื่อให้มั่นใจว่าชุดมาตรการควบคุมที่แก้ไขนั้นถูกนำมาใช้อย่างเหมาะสมและมีประสิทธิภาพ ทำให้ ISMS ของคุณสอดคล้องกับความเสี่ยงทางธุรกิจดิจิทัลของคุณ

9. เราควรทำอย่างไรเพื่อปรับเปลี่ยนและอัปเดตใบรับรองของเรา

ต้องมีการตรวจประเมินการปรับเปลี่ยนเพื่อประเมินว่าการเปลี่ยนแปลงได้รับการดำเนินการอย่างมีประสิทธิภาพ อย่างไรก็ตาม การปรับเปลี่ยนที่ประสบความสำเร็จนั้นจำเป็นต้องมีความเข้าใจอย่างถ่องแท้เกี่ยวกับการเปลี่ยนแปลงและผลกระทบที่มีต่อองค์กรของคุณ ควบคู่ไปกับการนำไปปฏิบัติอย่างมีประสิทธิภาพ สถาบันมาตรฐานอังกฤษ (bsi.) ขอแนะนำอย่างยิ่งให้คุณศึกษาเกี่ยวกับมาตรฐาน เข้าร่วมการฝึกอบรม และเตรียมความพร้อมเพื่อให้มั่นใจว่า ISMS ของคุณปกป้องสินทรัพย์สารสนเทศของคุณอย่างมีประสิทธิภาพ และการปรับเปลี่ยนของคุณจะประสบความสำเร็จ