ไอทีจีเนียส เอ็นจิเนียริ่ง
IT GENIUS ENGINEERING CO., LTD.

COURSE ID
CYC-03
CYBERSECURITY / ISMS

COURSE OUTLINE · รายละเอียดหลักสูตรอบรม

ISO/IEC 27001 ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

- 12 ชั่วโมง
- 2 วัน
- ไม่ต้องมีพื้นฐาน ISMS
- ระดับ Beginner - Inter

ระยะเวลา: 2 วัน
12 ชั่วโมง (2 วัน วันละ 6 ชม.) · 09:00-16:00 น.

รูปแบบ: Classroom / Hybrid
Onsite หรือ Online ผ่าน Microsoft Teams · Public / In-house

รายละเอียดหลักสูตร
www.itgenius.co.th

องค์กรจำนวนมากถูกคู่ค้าหรือลูกค้าถามหาใบรับรอง ISO/IEC 27001 แต่พอเริ่มลงมือกลับพบว่ามาตรฐานอ่านยาก เต็มไปด้วยศัพท์เฉพาะ และไม่บอกตรง ๆ ว่าองค์กรต้องทำอะไรบ้าง หลายแห่งจึงจ้างที่ปรึกษามาทำเอกสารให้แล้วได้ใบรับรองที่ไม่สะท้อนการทำงานจริง สุดท้ายก็ดูแลต่อไม่ได้และเสียงบประมาณไปเปล่า

หลักสูตรนี้อธิบายมาตรฐานให้เข้าใจในภาษาที่ใช้งานได้จริง แล้วพาลงมือทำทีละขั้นตามลำดับที่องค์กรควรทำจริง ครอบคลุมแนวคิดระบบบริหารความมั่นคงปลอดภัยสารสนเทศ, โครงสร้างข้อกำหนดตั้งแต่ข้อ 4 ถึงข้อ 10, การกำหนดขอบเขตให้เหมาะกับองค์กร, การประเมินและจัดการความเสี่ยงอย่างเป็นระบบ, การเลือกมาตรการควบคุมจาก Annex A ทั้งสี่กลุ่มและการเขียน Statement of Applicability, เอกสารและบันทึกที่ต้องมีจริง, การตรวจติดตามภายในและการทบทวนของฝ่ายบริหาร ไปจนถึงขั้นตอนการขอการรับรองและสิ่งที่ผู้ตรวจประเมินมักถาม โดยเชื่อมโยงกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของไทยด้วย (อบรม 2 วัน วันละ 6 ชั่วโมง รวม 12 ชั่วโมง ไม่ต้องมีพื้นฐาน ISMS มาก่อน)

เครื่องมือ
- ISO 27001
- Annex A
- ISMS
- Risk
- Audit

ราคาค่าอบรม · PUBLIC / IN-HOUSE

9,500 บาท / ท่าน

ราคายังไม่รวมภาษีมูลค่าเพิ่ม (VAT 7%) · รวมเอกสารประกอบการอบรม ชุด Template ทะเบียนความเสี่ยง SoA และ Checklist ตรวจติดตาม อาหารกลางวันและอาหารว่าง และ Certificate · ผู้เรียนได้ทะเบียนความเสี่ยงและร่าง SoA ขององค์กรกลับไป · รับจัด In-house ขอใบเสนอราคาได้

เพิ่มเพื่อน LINE

02-570-8449 · 088-807-9770 · @itgenius · www.itgenius.co.th

01 วัตถุประสงค์ Objectives

- เข้าใจแนวคิดระบบบริหารความมั่นคงปลอดภัยสารสนเทศและประโยชน์ที่แท้จริงต่อองค์กร
- อธิบายโครงสร้างข้อกำหนดของ ISO/IEC 27001 ตั้งแต่ข้อ 4 ถึงข้อ 10 ได้
- กำหนดขอบเขตของระบบให้เหมาะกับขนาดและลักษณะขององค์กร
- ระบุสินทรัพย์สารสนเทศและประเมินความเสี่ยงอย่างเป็นระบบและทำซ้ำได้
- เลือกมาตรการควบคุมจาก Annex A ให้ได้สัดส่วนกับความเสี่ยงและเขียน SoA ได้
- จัดทำเอกสารและบันทึกที่มาตรฐานกำหนดโดยไม่สร้างเอกสารเกินจำเป็น
- วางแผนและดำเนินการตรวจติดตามภายในและการทบทวนของฝ่ายบริหาร
- เข้าใจขั้นตอนการขอการรับรองและเตรียมองค์กรให้พร้อมรับการตรวจประเมิน
- เชื่อมโยงข้อกำหนดของมาตรฐานเข้ากับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของไทย

02 กลุ่มเป้าหมาย Target Audience

- ผู้บริหารและหัวหน้าฝ่ายไอทีที่ต้องผลักดันโครงการ ISO/IEC 27001 ในองค์กร
- ผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศและทีมบริหารความเสี่ยง
- ผู้ตรวจสอบภายในที่ต้องตรวจติดตามระบบบริหารความมั่นคงปลอดภัย
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่ต้องทำงานเชื่อมกับมาตรการความปลอดภัย
- องค์กรที่ถูกคู่ค้าหรือลูกค้าเรียกร้องให้มีใบรับรองมาตรฐานนี้

03 จุดเด่นของหลักสูตร Highlights

- **อธิบายมาตรฐานให้เข้าใจ** แปลศัพท์เฉพาะเป็นภาษาที่ใช้งานได้
- **ทำตามลำดับที่ถูกต้อง** จากขอบเขตสู่ความเสี่ยงและ SoA
- **ได้เอกสารจริงกลับไป** ทะเบียนความเสี่ยงและร่าง SoA ขององค์กร
- **ครบ Annex A ทั้งสี่กลุ่ม** องค์กร บุคลากร กายภาพ และเทคโนโลยี
- **เชื่อมกับ PDPA ไทย** ใช้ระบบเดียวตอบได้ทั้งสองเรื่อง

04 ความรู้พื้นฐาน Prerequisites

- ไม่ต้องมีพื้นฐานด้านมาตรฐานหรือระบบบริหารมาก่อน
- เข้าใจกระบวนการทำงานและการไหลของข้อมูลในองค์กรของตนเองพอสมควร
- ไม่จำเป็นต้องมีความรู้ด้านเทคนิคเชิงลึก แต่หากมีจะเห็นภาพมาตรการควบคุมได้ชัดขึ้น
- เตรียมข้อมูลระบบงานหลักขององค์กรมาหนึ่งชุดเพื่อใช้ทำ Workshop

05 สิ่งที่ต้องเตรียมและเครื่องมือ Setup & Tools

รายการ	รายละเอียด
อุปกรณ์	Notebook เชื่อมต่ออินเทอร์เน็ตได้ (ใช้ทำ Workshop และร่างเอกสาร)
มาตรฐานอ้างอิง	ISO/IEC 27001 ฉบับล่าสุดและมาตรการควบคุมใน Annex A
แนวปฏิบัติเสริม	ISO/IEC 27002 สำหรับรายละเอียดการนำมาตรการไปใช้
เอกสารประกอบ	Template ทะเบียนสินทรัพย์ ทะเบียนความเสี่ยง SoA และแผนตรวจติดตาม
กฎหมายที่เกี่ยวข้อง	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของไทยและการเชื่อมโยงกับมาตรฐาน

หมายเหตุ: หลักสูตรนี้เป็นการอบรมเชิงระบบบริหารและการกำกับดูแล ไม่ใช่หลักสูตรเทคนิคเชิงลึก จึงไม่ต้องเขียนโปรแกรมหรือตั้งค่าอุปกรณ์ ผู้เรียนสามารถนำระบบงานจริงขององค์กรมาใช้ทำ Workshop ได้โดยไม่ต้องเปิดเผยข้อมูลลับ หลักสูตรนี้เป็นการอบรมความรู้และการเตรียมความพร้อม ไม่ใช่การตรวจประเมินหรือการออกใบรับรอง การขอการรับรองต้องดำเนินการกับหน่วยรับรองที่ได้รับการรับรองระบบงานแยกต่างหาก

06 ภาพรวมการเรียน 2 วัน Big Picture

วัน	หัวข้อหลัก
Day 1 Section 1-5	แนวคิด ISMS, โครงสร้างมาตรฐาน, การกำหนดขอบเขต, การประเมินความเสี่ยง และการเลือกมาตรการควบคุม
Day 2 Section 6-11	มาตรการ Annex A ทั้งสี่กลุ่ม, เอกสารที่ต้องมี, การตรวจติดตามภายใน, การขอการรับรอง และ Workshop

DAY 1

จากมาตรฐานสู่การประเมินความเสี่ยง

เนื้อหาการอบรม · Section 1-5

รวม
6 ชั่วโมง

1 แนวคิดระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

- ความหมายของความมั่นคงปลอดภัยสารสนเทศ: ความลับ ความถูกต้อง และความพร้อมใช้งาน
- ความต่างระหว่างการซื้ออุปกรณ์ความปลอดภัยกับการมีระบบบริหารที่ดูแลต่อเนื่องได้
- ประโยชน์ที่องค์กรได้จริงนอกเหนือจากการมีใบรับรองไปแสดงคู่ค้า
- กับดักที่พบบ่อย: การจ้างทำเอกสารจนได้ระบบที่ไม่สะท้อนการทำงานจริง

2 โครงสร้างข้อกำหนดของมาตรฐาน

- ภาพรวมข้อกำหนดข้อ 4 ถึงข้อ 10 และความเชื่อมโยงเป็นวงจรปรับปรุงต่อเนื่อง
- บทบาทของผู้บริหารระดับสูงและสิ่งที่มาตรฐานเรียกร้องจากฝ่ายบริหารโดยตรง
- ความต่างระหว่างข้อกำหนดที่ต้องทำทุกข้อกับมาตรการควบคุมใน Annex A ที่เลือกได้
- ความสัมพันธ์กับมาตรฐานระบบบริหารอื่นและการใช้ร่วมกันโดยไม่ทำงานซ้ำซ้อน

3 การกำหนดขอบเขตและบริบทขององค์กร

- การวิเคราะห์บริบทภายในและภายนอกและการระบุผู้มีส่วนได้ส่วนเสีย
- การกำหนดขอบเขตของระบบให้ครอบคลุมสิ่งที่สำคัญโดยไม่ใหญ่เกินกำลัง
- การกำหนดนโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยที่วัดผลได้
- Workshop: ร่างขอบเขตระบบและนโยบายความมั่นคงปลอดภัยขององค์กรตนเอง

4 การระบุสินทรัพย์และการประเมินความเสี่ยง

- การจัดทำทะเบียนสินทรัพย์สารสนเทศและการกำหนดเจ้าของสินทรัพย์
- การระบุภัยคุกคามและช่องโหว่และการประเมินโอกาสกับผลกระทบ
- การกำหนดเกณฑ์ยอมรับความเสี่ยงและการจัดลำดับความเสี่ยงที่ต้องจัดการก่อน
- Workshop: ประเมินความเสี่ยงของระบบงานหลักขององค์กรลงในทะเบียนความเสี่ยง

5 การจัดการความเสี่ยงและการเลือกมาตรการควบคุม

- ทางเลือกในการจัดการความเสี่ยง: ลด ยอมรับ โอน หรือเลี่ยง และเกณฑ์การตัดสินใจ
- การเลือกมาตรการควบคุมจาก Annex A ให้ได้สัดส่วนกับความเสี่ยงและงบประมาณ
- การเขียน Statement of Applicability และการให้เหตุผลของมาตรการที่ไม่ใช้
- Workshop: จัดทำร่าง SoA จากผลการประเมินความเสี่ยงที่ทำไว้

DAY 2

มาตรการควบคุม การตรวจติดตาม และการรับรอง

เนื้อหาการอบรม · Section 6-11

รวม
6 ชั่วโมง

6 มาตรการด้านองค์กรและด้านบุคลากร

- นโยบาย บทบาทหน้าที่ และการแบ่งแยกหน้าที่เพื่อลดความเสี่ยงจากคนเดียวทำได้ทุกอย่าง
- การจัดการผู้ให้บริการภายนอกและข้อกำหนดด้านความปลอดภัยในสัญญา
- การจัดการบุคลากรตั้งแต่ก่อนจ้าง ระหว่างทำงาน และเมื่อพ้นสภาพ
- การสร้างความตระหนักและการฝึกอบรมพนักงานให้ได้ผลจริง

7 มาตรการด้านกายภาพและด้านเทคโนโลยี

- การควบคุมการเข้าถึงพื้นที่ ห้องเซิร์ฟเวอร์ และการจัดการอุปกรณ์
- การควบคุมการเข้าถึงระบบ การจัดการสิทธิ์ และการยืนยันตัวตน
- การเข้ารหัสข้อมูล การสำรองข้อมูล และการจัดการช่องโหว่และแพตช์
- การบันทึกและเฝ้าระวังเหตุการณ์ และการควบคุมความปลอดภัยของเครือข่าย

8 เอกสารและบันทึกที่ต้องมี

- รายการเอกสารที่มาตรฐานกำหนดว่าต้องมีและระดับรายละเอียดที่เพียงพอ
- การควบคุมเอกสาร การกำหนดเวอร์ชัน และการเก็บบันทึกเป็นหลักฐาน
- แนวทางไม่ให้เอกสารบานปลายจนไม่มีใครทำตามได้จริง
- Lab: ตรวจสอบเอกสารที่องค์กรมีอยู่เทียบกับรายการที่มาตรฐานกำหนด

9 การตรวจติดตามภายในและการทบทวนของฝ่ายบริหาร

- การวางแผนโปรแกรมตรวจติดตามภายในและการเลือกผู้ตรวจที่เป็นอิสระ
- เทคนิคการตรวจ: การสัมภาษณ์ การขอหลักฐาน และการบันทึกสิ่งที่พบ
- การจัดการสิ่งที่ไม่เป็นไปตามข้อกำหนดและการแก้ไขที่ถึงต้นเหตุ
- Workshop: จำลองการตรวจติดตามภายในและบันทึกผลตาม Checklist

10 การขอการรับรองและการเตรียมรับการตรวจประเมิน

- ขั้นตอนการขอการรับรอง: การตรวจขั้นที่หนึ่ง ขั้นที่สอง และการตรวจติดตามประจำปี
- การเลือกหน่วยรับรองและสิ่งที่ควรถามก่อนตัดสินใจ
- คำถามที่ผู้ตรวจประเมินมักถามและหลักฐานที่ควรเตรียมไว้ล่วงหน้า
- การรักษาระบบให้ใช้งานต่อเนื่องหลังได้ใบรับรองแล้ว

11 การเชื่อมกับ PDPA และแผนนำไปใช้จริง

- จุดที่ข้อกำหนดของมาตรฐานตอบข้อกำหนดด้านความปลอดภัยของ PDPA ได้เลย
- การใช้ทะเบียนสินทรัพย์และทะเบียนความเสี่ยงร่วมกันเพื่อไม่ให้ทำงานซ้ำ
- การประเมินความพร้อมขององค์กรและการวางแผนโครงการตามงบประมาณจริง
- Workshop: วางแผนดำเนินการ 12 เดือนขององค์กรตนเองและนำเสนอร่วมกัน

07 เรียนจบแล้วได้อะไร Outcomes

- **เข้าใจมาตรฐานทั้งฉบับ** อ่านข้อกำหนดแล้วรู้ว่าต้องทำอะไร
- **ประเมินความเสี่ยงเป็น** ทำทะเบียนความเสี่ยงที่ใช้งานได้จริง
- **เขียน SoA ได้** เลือกมาตรการและให้เหตุผลได้ครบ
- **รู้เอกสารที่ต้องมี** ไม่ทำเอกสารเกินและไม่ขาดข้อสำคัญ
- **ตรวจติดตามภายในได้** วางแผนและดำเนินการตรวจเป็น
- **พร้อมขอการรับรอง** รู้ขั้นตอนและสิ่งที่ผู้ตรวจจะถาม

08 สิ่งที่ผู้เรียนจะได้รับ Deliverables

- เอกสารประกอบการอบรมฉบับสมบูรณ์ พร้อมสรุปข้อกำหนดและมาตรการ Annex A ที่อ้างอิงได้
- ชุด Template พร้อมใช้: ทะเบียนสินทรัพย์ ทะเบียนความเสี่ยง Statement of Applicability และแผนตรวจติดตาม
- ทะเบียนความเสี่ยงและร่าง SoA ขององค์กรผู้เรียนที่จัดทำใน Workshop พร้อมแผนดำเนินการ 12 เดือน
- ประกาศนียบัตรจบหลักสูตร (Certificate of Completion) และช่องทางสอบถามวิทยากรหลังจบหลักสูตร

09 ข้อมูลผู้สอน Instructor

อ.สามิตร โกยม ผู้สอนและที่ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศที่มีประสบการณ์กว่า 15 ปี ผ่านการวางระบบและเตรียมองค์กรเข้ารับการตรวจประเมินมาตรฐานหลายแห่ง จุดเด่นคือการแปลข้อกำหนดที่อ่านยากให้เป็นงานที่ทีมลงมือทำได้จริง ชี้ให้เห็นว่าองค์กรมักพลาดตรงไหน และพาผู้เรียนจัดทำเอกสารจนได้ของจริงกลับไปใช้ต่อ

ราคาค่าอบรม 9,500 บาท/ท่าน · สนใจ IN-HOUSE ขอใบเสนอราคา

9,500 บาท / ท่าน (ยังไม่รวม VAT 7%)

02-570-8449 · 088-807-9770
@itgenius · contact@itgenius.co.th

เพิ่มเพื่อน LINE