

หลักการและเหตุผล

ในยุคที่ระบบดิจิทัลกลายเป็นโครงสร้างพื้นฐานหลักของทุกองค์กร ความเสี่ยงทางเทคโนโลยีไม่ได้จำกัดอยู่แค่ภัยไซเบอร์อีกต่อไป แต่รวมถึง Disruption, System Failure, Supply Chain Risk, และ AI/Cloud Risk ที่มีผลกระทบต่อความต่อเนื่องของธุรกิจ (Business Continuity) และความเชื่อมั่นของผู้ใช้บริการโดยตรง

การสร้าง Digital Resilience จึงเป็นยุทธศาสตร์สำคัญขององค์กรในศตวรรษที่ 21 — คือความสามารถในการ “คาดการณ์ ป้องกัน ปรับตัว และฟื้นตัวได้อย่างต่อเนื่อง”

หลักสูตรนี้ออกแบบมาเพื่อเสริมสร้างความเข้าใจและทักษะในการบริหารความเสี่ยงเชิงรุก (Continuous Risk Management) โดยผสานแนวคิดจากมาตรฐานสากล เช่น ISO/IEC 27005, ISO 22301, และแนวทาง Digital Operational Resilience (DORA) เพื่อสร้างระบบที่ยืดหยุ่น ปลอดภัย และยั่งยืนในระยะยาว

วัตถุประสงค์:

- เพื่อให้เข้าใจแนวคิดและองค์ประกอบของ Digital Resilience Framework
- เพื่อเรียนรู้การประยุกต์ใช้แนวทาง Continuous Risk Management ในระบบ IT และข้อมูล
- เพื่อเสริมทักษะในการออกแบบและวิเคราะห์ความเสี่ยงแบบเรียลไทม์ (Real-time Risk Analysis)
- เพื่อนำผลการ Resilience เข้ากับกระบวนการปกติ เช่น ITSM, DevOps, และ Data Management

หลักสูตรนี้เหมาะสำหรับ:

- ผู้บริหารด้าน IT, CSOC, Risk, Compliance
- Enterprise Architect / Business Continuity Manager
- IT Security & System Administrator
- บุคลากรที่เกี่ยวข้องกับ Digital Transformation

ความรู้พื้นฐาน:

- ความเข้าใจพื้นฐานด้าน Information Security หรือ Business Continuity
- ความรู้ทั่วไปเกี่ยวกับ ISO/IEC 27001 หรือ NIST Framework

เนื้อหาหลักสูตร:

1. บทนำสู่แนวคิด Digital Resilience

- ความหมายของ Digital Resilience และการเปลี่ยนจากแนวคิด “Protection” สู่ “Adaptation”
- ความแตกต่างระหว่าง Resilience, Continuity, และ Reliability
- Framework สำคัญ: ISO/IEC 27005, ISO 22301, NIST SP 800-160 Vol.2, DORA Framework
- Case Study: เหตุการณ์จริงขององค์กรที่ประสบความสำเร็จในการสร้าง Digital Resilience

2. โครงสร้างของ Continuous Risk Management (CRM)

- หลักการและวงจรของ CRM (Identify → Assess → Control → Monitor → Improve)
- การประยุกต์ใช้ CRM กับระบบ IT และบริการดิจิทัล
- การเชื่อมโยง CRM กับ PDCA และ Integrated Management Systems
- Workshop: การสร้าง Risk Register แบบ Dynamic

3. การผนวกมาตรฐานการจัดการความเสี่ยง (Integration with ISO Frameworks)

มาตรฐาน	ประเด็นสำคัญที่เชื่อมโยง
ISO/IEC 27005	การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
ISO 22301	การวางแผนความต่อเนื่องทางธุรกิจ (BCP/DRP)
ISO 31000	หลักการบริหารความเสี่ยงเชิงองค์กร
ISO/IEC 42001	การบริหารความเสี่ยงด้าน AI และการกำกับดูแลอัลกอริทึม
ISO/IEC 19770	ความเสี่ยงด้านสินทรัพย์ IT และซอฟต์แวร์

4. การระบุและวิเคราะห์ความเสี่ยง (Digital Risk Identification & Analysis)

- เทคนิคการระบุภัยคุกคามสมัยใหม่ (Cyber, Cloud, AI, Supply Chain)
- การวิเคราะห์ผลกระทบและโอกาส (Impact & Likelihood Analysis)
- เครื่องมือและเทคนิค Risk Scoring / Heatmap / Monte Carlo Simulation
- Workshop: สร้าง Digital Risk Map ขององค์กร

5. การออกแบบระบบ Digital Resilience Architecture

- หลักการออกแบบระบบให้มี Resilience by Design
- การใช้ Automation และ AI เพื่อเสริมความยืดหยุ่นของระบบ
- การเชื่อมโยง Resilience กับ Zero Trust, Cloud-native และ Microservices
- ตัวอย่าง Blueprint: Digital Resilience Architecture

6. การตรวจจับและตอบสนองแบบต่อเนื่อง (Continuous Monitoring & Response)

- การสร้าง Early Warning System และ Anomaly Detection
- การใช้ Threat Intelligence และ Risk Sensing
- Integration กับ SOC / SIEM / SOAR
- Workshop: ออกแบบ Dashboard สำหรับ Continuous Risk Monitoring

7. การบริหารความเสี่ยงเชิงกลยุทธ์และ Governance

- การจัดตั้ง Risk Committee และ Resilience Office
- การวัดความพร้อมขององค์กร (Resilience Maturity Model)
- การเชื่อมโยงกับ ESG และ Cyber Governance Framework

8. การทดสอบ ฟื้นฟู และปรับปรุงอย่างต่อเนื่อง

- การจัดทำ Test Plan, Simulation และ Scenario-based Testing
- การประเมินผลลัพธ์ของ Incident / Crisis Response
- การปรับปรุงระบบอย่างต่อเนื่องตาม PDCA
- ตัวอย่างแบบฟอร์ม Test & Improvement Log

9. การวางแผนกลยุทธ์สู่ Digital Resilient Enterprise 2030

- การกำหนด Roadmap ระยะ 3–5 ปี
- การผสาน Continuous Risk Management เข้ากับนโยบายองค์กร
- ตัวชี้วัดสำคัญ: MTTR, MTTR, Resilience Index, Risk Velocity

ผลลัพธ์ที่คาดหวัง (Learning Outcomes)

- เข้าใจแนวคิด Digital Resilience และ Continuous Risk Management Framework
- สามารถออกแบบระบบ Resilience ที่สอดคล้องกับมาตรฐานสากล
- มีทักษะในการวิเคราะห์และจัดการความเสี่ยงแบบต่อเนื่อง
- สามารถเชื่อมโยง Risk Governance กับกลยุทธ์องค์กรและนโยบายด้าน IT

มาตรฐานที่หลักสูตรนี้สอดคล้องและสามารถ Apply ได้

- ISO/IEC 27005: Information Security Risk Management
- ISO 22301: Business Continuity Management
- ISO 31000: Risk Management
- NIST SP 800-160 Vol.2: Developing Cyber-Resilient Systems
- Digital Operational Resilience Act (DORA, EU 2025)

ค่าลงทะเบียนอบรม:	12,000 บาท (ไม่รวมภาษีมูลค่าเพิ่ม)
จำนวนชั่วโมงในการฝึกอบรม:	3 วัน (18 ชั่วโมง)
ช่วงเวลาฝึกอบรม:	9.00 - 16.00 น.
กำหนดการอบรม:	ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

วิทยากร:



อาจารย์ขจร สินอภิรมย์สรานุกุล

- วิทยากรรับเชิญ ประจำสถาบันพัฒนาบุคลากรแห่งอนาคต
- Microsoft Certified Technology Specialist
- Microsoft Certified System Engineer: Security
- Microsoft Certified System Administration: Messaging
- Microsoft Certified Professional
- Microsoft Certified Trainer
- Microsoft Certified IT Professional
- Microsoft Certified Database Administration
- ITIL Foundation V2 & V3, Comtia Security+

หมายเหตุ

- สถาบันฯ มีการจัดเตรียมเครื่องคอมพิวเตอร์ (ในหลักสูตรที่ต้องใช้โปรแกรมคอมพิวเตอร์) เอกสารการอบรม อาหารว่าง และอาหารกลางวัน ให้กับผู้เข้าอบรม
- สถานที่อบรม ห้องอบรม ณ สถาบันพัฒนาบุคลากรแห่งอนาคต อาคาร สวทช. ชั้น 6 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
- เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจและไม่แสวงหากำไร จะได้รับการยกเว้น ภาษีมูลค่าเพิ่ม
- สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3%
- ผู้เข้าร่วมอบรมจากหน่วยงานราชการสามารถเบิกค่าลงทะเบียนจากต้นสังกัดได้ ตามระเบียบกระทรวงการคลัง และไม่ถือเป็นวันลาเมื่อได้รับการอนุมัติจากผู้บังคับบัญชา
- ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของบริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อน ภาษีได้ 200%
- สถาบันฯ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร รูปแบบการอบรม ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม
- สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพ วิดีโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจาก สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

ติดต่อสอบถามรายละเอียด

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)

73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 ต่อ 81886-7
โทรสาร 0 2644 8150
E-mail: training@nstda.or.th
www.career4future.com