

AI Governance for IT Leaders

ระยะเวลา 2 วัน

หลักการและเหตุผล

AI กำลังเปลี่ยนจากเครื่องมือช่วยสร้างเนื้อหาไปสู่ระบบที่สามารถเข้าถึงข้อมูล เชื่อมต่อเครื่องมือ สนับสนุนการตัดสินใจ และทำงานในกระบวนการขององค์กรได้ การกำกับดูแล AI จึงต้องครอบคลุมมาตรฐาน การบริหารความเสี่ยง การกำหนดขอบเขตการใช้งาน การควบคุมสิทธิ์ การตรวจสอบโดยมนุษย์ และหลักฐานจากการทำงานของ AI

หลักสูตร AI Governance for IT Leaders ออกแบบสำหรับผู้บริหารและผู้รับผิดชอบด้าน IT ที่ต้องการนำ AI, Generative AI และ

AI Agent มาใช้อย่างเป็นระบบ ปลอดภัย ตรวจสอบได้ และสอดคล้องกับมาตรฐานสากลและบริบทประเทศไทย

ตลอดการอบรม 2 วัน ผู้เรียนจะได้เปรียบเทียบมาตรฐาน AI Governance ที่สำคัญ วิเคราะห์ความท้าทายของ Enterprise AI ประเมินความเสี่ยงของ AI Use Case และออกแบบโครงสร้างนโยบาย AI Governance ที่เหมาะกับองค์กร

วัตถุประสงค์

- อธิบายบทบาทของมาตรฐานและกรอบ AI Governance ที่สำคัญได้
- เลือกใช้ ISO/IEC 42001, ISO/IEC 38507, ISO/IEC 23894, ISO/IEC 42005 และ NIST AI RMF ให้เหมาะกับบริบทองค์กรได้
- อธิบายภาพรวมความเชื่อมโยงของมาตรฐานสากลกับแนวทางของ ETDA, PDPA, Cybersecurity และข้อกำหนดที่เกี่ยวข้องได้
- จัดทำ AI Use Case Inventory และจำแนกระดับความเสี่ยงได้
- ประเมินผลกระทบของ Generative AI และ AI Agent ได้อย่างเป็นระบบ
- กำหนดแนวทางควบคุมตามระดับความเสี่ยงและระดับความสามารถในการดำเนินการของ AI ได้
- ออกแบบโครงสร้าง AI Governance Policy สำหรับองค์กรได้

รายละเอียดหลักสูตร

วันที่ 1 : Standards and Enterprise AI Governance Challenges

Module 1: International Standards and Thailand AI Governance Overview

ส่วนที่ 1 — มาตรฐานและกรอบสากล

- ISO/IEC 42001 — Artificial Intelligence Management System
- ISO/IEC 38507 — Governance Implications of the Use of AI by Organizations
- ISO/IEC 23894 — Artificial Intelligence Risk Management
- ISO/IEC 42005 — AI System Impact Assessment
- NIST AI Risk Management Framework: Govern, Map, Measure และ Manage
- ความสัมพันธ์ระหว่าง Governance, Management, Risk และ Technical Controls
- แต่ละมาตรฐานตอบโจทย์ใครและใช้ในระดับใดขององค์กร
- แนวทางเลือกจุดเริ่มต้นสำหรับองค์กรที่ยังไม่มี AI Governance

ส่วนที่ 2 — บริบทประเทศไทย

- ภาพรวมแนวทาง AI Governance และหลักจริยธรรม AI ของ ETDA
- หลักจริยธรรม AI ของประเทศไทย
- แนวทางการกำกับดูแลแบบ Risk-based Approach
- สถานะและทิศทางการกำกับดูแล AI ในประเทศไทย โดยแยกกฎหมายที่มีผลบังคับ ร่างกฎหมาย และ Soft Law
- ความเชื่อมโยงกับ PDPA, Cybersecurity และ Sector Regulation
- ภาพรวมความเชื่อมโยงระหว่างแนวทางประเทศไทยกับ ISO, NIST และการกำกับดูแลแบบ Risk-based

Workshop: Standards Comparison and Initial Alignment

- ผู้เรียนจับคู่มาตรฐานและกรอบกำกับดูแลกับ AI Use Case ขององค์กร พร้อมจัดทำ Standards Alignment Worksheet เบื้องต้น

Module 2: Governance Challenges for Enterprise AI

- ความแตกต่างระหว่าง Traditional AI, Generative AI และ Agentic AI
- AI ที่ให้คำแนะนำกับ AI ที่สามารถดำเนินการมีความเสี่ยงต่างกันอย่างไร
- ความเสี่ยงเมื่อ AI เข้าถึงข้อมูลภายในองค์กร
- ความเสี่ยงเมื่อ AI เชื่อมต่อ API, Database, Cloud และระบบ IT
- การแยก Model, Application Harness, Data/Knowledge และ Integration/MCP เพื่อระบุขอบเขตความรับผิดชอบ
- Application Harness as a Governance Control Layer: ครอบคลุม Policy Enforcement, Access Control, Human Approval, Logging และ Evaluation
- ความเสี่ยงจาก Tool Calling และ Model Context Protocol
- Hallucination และการใช้ผลลัพธ์ที่ไม่มีหลักฐานรองรับ
- Data Leakage และการเปิดเผยข้อมูลผ่าน Prompt หรือ Tool
- Prompt Injection และคำสั่งที่ไม่พึงประสงค์
- Excessive Agency และการให้อำนาจ AI มากเกินความจำเป็น
- Third-party Model และ Vendor Risk
- Shadow AI และการใช้เครื่องมือ AI โดยไม่ได้รับอนุมัติ
- ความแตกต่างระหว่าง Prototype, Pilot และ Production AI
- ความสำคัญของ Logging, Traceability และ Evidence
- ความเสี่ยงจากการตรวจเพียง Final Outcome โดยไม่ตรวจสอบกระบวนการทำงาน

กรณีศึกษาและกิจกรรม

- AI Service Desk จำแนกและดำเนินการกับ Ticket
- AI ช่วยวิเคราะห์ Cybersecurity Incident
- AI Agent เชื่อมต่อ Database และระบบองค์กร
- AI ช่วย Network Operations และ Infrastructure Troubleshooting

กิจกรรมกลุ่ม: เลือก Enterprise AI Use Case และระบุประเด็นกำกับดูแลที่ต้องพิจารณาเพื่อนำขึ้น Production

สรุปวันที่ 1

- ทบทวนความสัมพันธ์ระหว่างมาตรฐานสากล บริบทประเทศไทย และความเสี่ยงของ Enterprise AI
- เตรียม AI Use Case สำหรับนำไปประเมินความเสี่ยงในวันที่ 2

วันที่ 2: AI Risk Assessment and Policy Design

Module 3: AI Use Case Inventory, Risk Classification and Impact Assessment

- เหตุผลที่องค์กรต้องมี AI Use Case Inventory
- ข้อมูลขั้นต่ำที่ควรบันทึกสำหรับ AI แต่ละระบบ
- การระบุ Business Owner, System Owner, Model Provider และผู้รับผิดชอบความเสี่ยง
- วัตถุประสงค์ ขอบเขต ผู้ใช้งาน และผู้ได้รับผลกระทบ
- ประเภทข้อมูลและระดับความอ่อนไหว
- ระบบภายนอกและเครื่องมือที่ AI สามารถเข้าถึง
- ระดับ Autonomy ของ AI
- ความสามารถในการเปลี่ยนแปลงข้อมูลหรือระบบจริง
- ความรุนแรงและโอกาสเกิดความเสียหาย
- Human Oversight และจุดอ่อน
- การจำแนกระดับ Low, Medium และ High Risk
- หลักการทำ AI System Impact Assessment

คำถามหลักสำหรับประเมินความเสี่ยง

- AI เกี่ยวข้องกับระบบหรือบริการสำคัญหรือไม่
- AI ใช้ข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวหรือไม่
- AI มีผลต่อสิทธิ โอกาส หรือการตัดสินใจเกี่ยวกับบุคคลหรือไม่
- AI สามารถเรียก Tool หรือดำเนินการกับระบบจริงหรือไม่
- หาก AI ผิดพลาด ผลกระทบสามารถย้อนกลับได้หรือไม่
- มีมนุษย์ตรวจสอบก่อนหรือหลังการดำเนินการหรือไม่

- สามารถตรวจสอบ Input, Output, Tool Call และ Tool Result ย้อนหลังได้หรือไม่

Workshop: AI Risk Classification and Impact Assessment

- ผู้เรียนเลือก AI Use Case จำนวน 1 กรณี จัดทำข้อมูลใน AI Use Case Inventory และทดลองประเมินความเสี่ยงและผลกระทบเบื้องต้น

Module 4: Designing an Enterprise AI Governance Policy

องค์ประกอบของนโยบาย

- Purpose and Objectives
- Scope and Applicability
- Definitions
- Governance Principles
- Roles and Responsibilities
- AI Use Case Registration and Classification
- Risk and Impact Assessment
- Data, Model and Tool Governance
- Human Oversight and Approval
- Security and Access Control
- Testing, Evaluation and Acceptance Criteria
- Monitoring, Evidence and Incident Handling
- Third-party and Procurement Requirements
- Review and Continuous Improvement

Policy Design Workshop

- กำหนดขอบเขตและวัตถุประสงค์ของนโยบาย
- จัดทำโครงสร้างนโยบายสำหรับองค์กร
- กำหนดผู้รับผิดชอบในแต่ละส่วนของนโยบาย
- กำหนดผู้มีอำนาจอนุมัติ AI Use Case
- กำหนดข้อยกเว้นและกระบวนการขออนุมัติ
- ร่าง AI Governance Vision Statement

Final Workshop: Enterprise AI Governance Starter Draft

ผู้เรียนรวบรวมผลลัพธ์จาก Workshop ตลอด 2 วันเป็น Starter Draft จาก AI Use Case จำนวน 1 กรณี ประกอบด้วย

- Standards Alignment Worksheet
- AI Use Case Inventory
- AI Risk Screening and Impact Assessment Starter Draft
- AI Governance Policy Outline (Starter Draft)
- AI Governance Vision Statement
- Roles and Responsibilities

แต่ละกลุ่มนำเสนอ Enterprise AI Governance Starter Draft พร้อมรับข้อเสนอแนะจากวิทยากร

สิ่งที่ผู้เรียนจะได้รับ

- Template สำหรับจัดทำ AI Use Case Inventory
- AI Risk Classification Worksheet
- AI System Impact Assessment Template
- AI Governance Policy Outline (Starter Draft)
- Roles and Responsibilities Matrix
- Enterprise AI Governance Starter Draft

จุดเด่นของหลักสูตร

- ออกแบบสำหรับผู้บริหารและผู้รับผิดชอบระบบ IT โดยเฉพาะ
- ครอบคลุมทั้ง Generative AI และ Agentic AI
- เชื่อมโยง Governance เข้ากับระบบ IT, Cybersecurity และ IT Service Management

- เน้นการจำแนกความเสี่ยง หลักฐาน และการกำกับ AI ที่เชื่อมต่อบริษัทจริง
- มี Workshop ต่อเนื่องตลอด 2 วัน
- ผู้เรียนได้รับชุดเอกสารตั้งต้นที่นำกลับไปปรับใช้ในองค์กรได้

รูปแบบการเรียนรู้

- Lecture พร้อมตัวอย่างจากระบบ IT และการใช้ AI ในองค์กร
- Guided Workshop แบบเป็นขั้นตอน
- Group Exercise และการแลกเปลี่ยนประสบการณ์
- AI Use Case Risk Assessment
- Policy Drafting Workshop
- Template และ Worksheet สำหรับนำกลับไปใช้งานต่อ

หลักสูตรนี้เหมาะกับ

- CIO, CTO, CISO, CDO และผู้บริหารด้านเทคโนโลยี
- IT Director, IT Manager และ Digital Transformation Leader
- ผู้รับผิดชอบ IT Governance, Enterprise Architecture และ Technology Risk
- ผู้รับผิดชอบ Cybersecurity, Data Governance, Compliance และ Internal Audit
- Project Manager และ Product Owner ที่ดูแลโครงการ AI
- ผู้ดูแล IT Service Management และ IT Operations
- AI Developer, Solution Architect และ Technology Consultant
- บุคลากรภาครัฐที่รับผิดชอบนโยบายหรือโครงการ AI

ผู้เข้าอบรมไม่จำเป็นต้องมีทักษะด้านการเขียนโปรแกรม

สิ่งที่ต้องเตรียมก่อนเข้าเรียน

- Notebook สำหรับทำ Workshop
- ตัวอย่าง AI Use Case หรือแผนการนำ AI มาใช้ในองค์กร หากมี
- ข้อมูลเบื้องต้นเกี่ยวกับ Workflow, Stakeholder และระบบที่ AI อาจเชื่อมต่อ