AI Governance: Principles to Practice (NIST AI RMF with ISO/IEC 38507 Focus)

Duration 2 Days

COURSE DESCRIPTION

This fast-paced course explores AI governance principles, security considerations for AI usage, and concludes with a session on ISO/IEC 38507 AI governance standards. Participants will gain knowledge of foundational AI concepts, risk management practices, hands-on AI use cases, and structured governance frameworks to responsibly implement AI within organizations.

COURSE OBJECTIVE

By the end of this course, participants will be able to:

- Understand AI governance principles, ethical foundations, and associated risks.
- Align AI projects with organizational goals responsibly and securely.
- Identify and mitigate major AI security risks.
- Apply secure and responsible practices when interacting with AI tools such as ChatGPT, Gemini, and Claude.ai.
- Understand and apply ISO/IEC 38507 guidance for AI governance, accountability, and compliance oversight.
- Develop foundational AI governance policies and organizational frameworks.

COURSE OUTLINE

Day 1: AI Governance Fundamentals and Secure AI Practices

Time	Topics
9.00–10.30	Introduction to AI Governance and Generative AI ▪ Key Principles (Transparency, Accountability, Ethics) ▪ Roadmap to AI Governance
10.45–12.00	AI Technologies and Business Applications ▪ Use Cases and Risk Awareness ▪ Stakeholder Engagement
13.00–14.30	AI Governance Frameworks ▪ Overview of NIST AI RMF and ISO AI Standards ▪ AI Risk Control Planning
14.45–16.00	Group Hands-on Activity ▪ Define AI business use case and governance roadmap ▪ Risk identification and stakeholder analysis

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

Day 2: Secure AI Usage and ISO/IEC 38507 Governance

Time	Topics
9.00–10.30	Secure AI Fundamentals ▪ Basics of AI Models (ChatGPT, Gemini, Claude.ai) ▪ Security and Privacy Considerations
10.45–12.00	Identifying and Mitigating AI Security Risks ▪ Top Threats (Data leakage, Unauthorized Access, Adversarial Attacks) ▪ Best Secure AI Practices
13.00–14.30	ISO/IEC 38507: Governance of AI ▪ Governance Implications and Accountability Principles
14.45–16.00	Building Governance Oversight ▪ Draft Governance Policies ▪ Ethical and Compliance Considerations ▪ Closing Q&A and Best Practices

TEACHING AND LEARNING METHODS

- **Lectures:** Key concept delivery with examples.
- **Case Studies:** Practical cases highlighting AI governance and security incidents.
- **Group Exercises:** Define AI use cases, stakeholder risks, and draft governance policies.
- **Interactive Discussions:** Application of standards and ethical analysis of real-world AI governance issues.

RECOMMENDED MATERIALS

- Provided extracts from ISO/IEC 38507:2022 (in-class use).
- Selected extracts from NIST AI RMF 1.0 (overview provided in class).
- ISACA AI Governance and Assurance frameworks (for optional deeper reading)

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th