Risk Management for Information Security

Duration: 1 Day

COURSE DESCRIPTION

This one-day intensive course is tailored to equip professionals with a robust understanding of Information Security Risk Management principles, based on the ISO 27005 standard. Participants will delve into the essential elements of managing information security risks effectively, including risk assessment methodologies, context establishment, and risk treatment strategies. This course is ideal for enhancing compliance and reinforcing an organization's security posture by aligning with international standards.

COURSE OBJECTIVES

- **In-depth Insights:** Gain a comprehensive understanding of the Information Security Risk Management process tailored to the ISO 27005 framework.
- **Hands-on Skills:** Acquire practical skills in identifying, analyzing, and managing information security risks to safeguard organizational assets.
- **Enhanced Compliance:** Implement risk management practices that improve compliance with international standards, thereby boosting your organization's security mechanisms.
- **Career Development:** Position yourself for career growth in various roles related to information security, risk management, and compliance.

COURSE OUTLINE

Morning Session:

- **Introduction and Overview of the Framework:**
  - Introduction to Information Security Risk Management
  - Understanding the core concepts and process outline as per ISO 27005
- **Context Establishment and Risk Assessment:**
  - Setting up the context for risk management: Scope, criteria, and organizational structure
  - Detailed walkthrough of risk identification processes including assets, threats, controls, vulnerabilities, and potential impacts

Afternoon Session:

- **Risk Analysis and Evaluation:**
  - Analyzing risks through various methodologies to assess potential consequences and the likelihood of incidents
  - Evaluating risks to determine their acceptability and impact on organizational objectives
- **Risk Treatment and Communication:**
  - Exploring different risk treatment options: Modification, retention, avoidance, and sharing
  - Strategies for effective risk communication and the importance of stakeholder engagement in the risk management process
- **Monitoring, Review, and Continual Improvement:**
  - Techniques for ongoing monitoring and review of the risk management framework
  - Discussion on continual improvement practices to adapt and evolve the risk management strategy

Practical Application and Case Studies:

- Participants will engage in interactive sessions that apply the concepts learned to real-world scenarios through case studies and group discussions.

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

This course ensures a comprehensive understanding of Information Security Risk Management, encouraging participants to implement and manage an effective risk management strategy within their organizations.

WHO SHOULD ATTEND

- Information Security Managers and Analysts
- Risk Management Professionals
- IT Managers and Consultants
- Compliance Officers and Assurance Staff
- Personnel involved in the security management processes within organizations

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