ISACA's Advanced in AI Security Management (AAISM)

Course Duration : 40 Hours **Course code : AAISM**

1. Course Overview

ISACA's Advanced in AI Security Management (AAISM) course is designed for professionals responsible for securing artificial intelligence systems and managing AI-related security risks. This course focuses on protecting AI models, data pipelines, and AI-enabled applications from emerging threats while ensuring governance, compliance, and ethical use. Learners gain advanced knowledge of AI security architecture, risk management, and controls required to safeguard AI-driven environments.

2. What you'll learn?

- AI security fundamentals and threat landscape
- Securing AI models, data, and pipelines
- AI governance, risk, and compliance frameworks
- Managing adversarial attacks and model manipulation
- Privacy, ethics, and regulatory considerations in AI
- Continuous monitoring and improvement of AI security

3. Target Audience

- Information Security and Cybersecurity Managers
- AI and Machine Learning Security Professionals
- Risk, Governance, and Compliance Professionals
- Security Architects and Technology Consultants
- Professionals managing AI-enabled systems

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

4. Pre-Requisites

- Basic understanding of AI and machine learning concepts
- Experience in cybersecurity, risk management, or governance is recommended
- Familiarity with information security frameworks is beneficial

5. Course Content (Modules)

Module 1: AI Security Foundations

- AI systems overview and security challenges

Module 2: AI Governance and Risk Management

AI governance models and policies

- Risk identification and assessment for AI systems

Module 3: Securing AI Data and Models

- Data protection and integrity controls
- Model security and adversarial defense techniques

Module 4: AI Security Operations and Incident Management

- Monitoring AI systems
- Incident response for AI-related security events

Module 5: Compliance, Ethics, and Continuous Improvement

- Regulatory requirements and ethical AI
- Continuous monitoring and security optimization