# Advanced in AI Security Management

Course Duration: 2 Days
Exam Reference: AAISM

## Course Overview

With the significant potential of artificial intelligence comes new threats and vulnerabilities. ISACA Advanced in AI Security Management™ (AAISM™) is the first and only AI-centric security management certification designed to help experienced IT professionals reinforce the enterprise's security posture and protect against AI-specific threats. You'll be able to manage the evolving security risk related to AI, implement policy, and ensure its responsible and effective use across the organization.

## Prerequisites

Before attending this accelerated course, you should have:

- An active CISM or CISSP certification;
- Proven experience in security or advisory roles;
- Some expertise in assessing, implementing, and maintaining AI systems.

## Course Objectives

The first and only credential of its kind, AAISM is designed to equip technology and information security leaders with the specialized skills needed to manage the evolving security risk related to AI, implement policy, and ensure its responsible and effective use across the organization. The learner will be able to:

- Design and implement AI governance models, establish roles and responsibilities, interpret and apply AI regulations, and align AI initiatives with business objectives.
- Identify and mitigate AI-related risks, address AI-specific vulnerabilities, and conduct AI asset and data inventory.
- Implement technical and procedural controls to protect AI models and data, embed AI in security architectures, ensure data privacy, and address ethical and safety issues.


APPLIED TECHNOLOGY ACADEMY

**Contact Us**

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

**Connect With Us**

# Advanced in AI Security Management

## Course Outline

Module 1: AI Governance and Program Management

This module demonstrates your ability to advise stakeholders on implementing AI security solutions through appropriate and effective policy, data governance, program management and incident response.

- Stakeholder Considerations, Industry Frameworks, and Regulatory Requirements
- AI-Related Strategies, Policies, and Procedures
- AI Asset and Data Life Cycle Management
- AI Security Program Development and Management
- Business Continuity and Incident Response

Module 2: AI Risk Management

This module confirms your skill at assessing and managing risks, threats, vulnerabilities and supply chain issues related to the enterprise-wide adoption of AI.

- AI Risk Assessment, Thresholds, and Treatment
- AI Threat and Vulnerability Management
- AI Vendor and Supply Chain Management

Module 3: AI Security Controls and Architecture

This module focuses on optimizing AI security and highlights your knowledge of security technologies, techniques and controls tailored to AI systems.

- AI Security Architecture and Design
- AI-Related Strategies, Policies, and Procedures
- Data Management Controls
- Privacy, Ethical, Trust and Safety Controls
- Security Controls and Monitoring