AAISM - ADVANCED IN AI SECURITY MANAGEMENT CERTIFICATION PREP

Course Code: 840109

Master the principles of AI security governance, risk management, and technical controls to confidently lead secure and compliant AI initiatives.

Artificial Intelligence is transforming how organizations operate, but it also introduces new security challenges that require specialized expertise. The AAISM Certification Prep Course helps professionals build the advanced knowledge needed to manage AI security programs effectively. This course goes beyond theory, focusing on practical strategies for governance, risk management, and technical controls that align with global standards and regulatory requirements.

Participants will explore the full lifecycle of AI security—from developing governance frameworks and policies to assessing risks, implementing controls, and preparing for AI-specific incident response. The course also covers critical topics such as ethical AI use, privacy considerations, vendor risk management, and securing AI architectures. Real-world examples and best practices ensure learners can apply these concepts immediately within their organizations.

Whether your goal is to prepare for ISACA's AAISM certification or strengthen your organization's AI security posture, this course provides the tools and insights you need to lead confidently in this emerging field.

What You'll Learn

- Develop AI Governance Frameworks
- Create AI Security Policies and Procedures
- Manage AI Asset and Data Lifecycle
- Integrate AI into Incident Response and Business Continuity
- Perform AI Risk Assessments and Threat Analysis
- Secure AI Technologies and Architectures
- Monitor and Measure AI Security Effectiveness

Who Needs to Attend

This course is ideal for professionals who are responsible for securing AI systems or managing AI governance and risk, including:

- **Information Security Managers and Leaders**
  - Overseeing enterprise security programs and integrating AI into governance frameworks.
- **Risk and Compliance Professionals**

- Managing regulatory requirements, privacy considerations, and AI risk assessments.

- **AI Program Managers and Governance Specialists**
  - Developing strategies, policies, and procedures for responsible AI use.
- **Cybersecurity Architects and Engineers**
  - Designing secure AI architectures and implementing technical controls.
- **IT and Security Practitioners**
  - Seeking to expand their expertise into AI security management.

(Recommended for individuals preparing for ISACA's AAISM certification or those involved in AI security initiatives.)

Prerequisites

- For Taking This Course (recommended, not mandatory)
- Foundational knowledge of AI concepts (e.g., AI technologies, data lifecycle, basic machine learning principles).
- Background in information security, risk management, or governance frameworks.
- Experience in IT or security roles such as security analyst, risk manager, compliance officer, or IT governance professional.
- Basic understanding of regulatory and privacy requirements related to data protection and ethical technology use.
- For AAISM Certification

To earn the AAISM certification, candidates must hold either ISACA's CISM (Certified Information Security Manager) or ISC2 CISSP (Certified Information Systems Security Professional) prior to sitting for the exam.

AAISM - ADVANCED IN AI SECURITY MANAGEMENT CERTIFICATION PREP

Course Code: 840109

VIRTUAL CLASSROOM LIVE	$1,995 USD	2 Day

Virtual Classroom Live Outline

Domain 1. AI Governance and Program Management

- **Stakeholder Considerations, Industry Frameworks, and Regulatory Requirements**
  - Organizational Structure and Overall Governance
  - Roles and Responsibilities
  - Charter and Steering Committee
  - Identifying Stakeholder
  - Risk Appetite and Tolerance
  - Frameworks, Standards, and Regulations
  - Selecting appropriate Frameworks
  - Business and Use Cases for AI
  - Privacy Considerations
- **AI-related Strategies, Policies, and Procedures**
  - AI Strategy
  - Consumer v. Enterprise
  - Buy vs. Build
  - AI Policies
  - Responsible Use
  - Acceptable Use
  - AI Procedures
  - Implementation
  - Manuals
  - Ethic
- **AI Asset and Data Life Cycle Management**
  - AI Asset and Data Inventory
  - Inventory management
  - Model cards
  - Data handling, classification, discovery
  - Data Augmentation and Cleaning
  - Data Storage

- Data Protection
- Destruction

- **AI Security Program Development and Management**
  - Documented Program Plan
  - Security team, roles, responsibilities, and proficiencies
  - Alignment to existing info sec
  - Use of AI-enabled security tools in the program
  - Metrics and management
  - KRIs and KPIs for AI use with regard to the security
  - Management reporting
- **Business Continuity and Incident Response**
  - Incident detection
  - Notification
  - Incident classification
  - Criticality and severity
  - Resiliency
  - Business Continuity Plan
  - Red-button requirements for compliance
  - Incident response playbooks specifically for AI
  - Break glass policies/ go no go
  - Authority
  - RTO RPO – AI perspective
  - Disaster recovery
  - Testing

Domain 2. AI Risk Management

- **AI Risk Assessment, Thresholds, and Treatment**
  - Impact assessment
  - Conformity assessment
  - PIAs
  - Risk documentation
  - Acceptable levels of risk
  - Treatment plans
  - KRIs and KPIs for AI us
- **AI-related Strategies, Policies, and Procedures**
  - PEN test
  - Vulnerability tests
  - Red teaming
  - AI related vulnerabilities
  - Adversarial threats
  - Threat intelligence
  - AI-enabled threats/Attack chains
  - Anomalies
  - Threat landscape
  - Deep fakes
  - Insider threat

- AI agents
- **AI Vendor and Supply Chain Management**
  - Dependencies of software packages and libraries
  - Vendor due diligence and contracts
  - SLAs
  - Vendor usage
  - Accountability models
  - Provider vs. deployer
  - Third, fourth, and fifth parties
  - Ownership and intellectual property
  - Access controls
  - Liability
  - Vendor monitoring for risk and change

Domain 3. AI Technologies and Controls

- **AI Security Architecture and Design**
  - Change management
  - SDL
  - Secure by design
  - Securing infrastructure as code
  - Data flows
  - Approved base models
  - Interconnectivity and interaction with architecture
- **AI Life Cycle (e.g., model selection, training, and validation)**
  - Testing models interconnectivity
  - Linkages between models
  - Regression
  - Model testing
  - Progression
  - TEVV
  - Model accuracy testing and evaluation
- **Data Management Controls**
  - Data collection
  - Data control
  - Data Poisoning
  - BIAS
  - Accuracy
  - Data position requirements
  - Privacy, Ethical, Trust and Safety Controls
  - Explainability
- **Privacy controls – like right to be forgotten, data subject rights**
  - Consent
  - Transparency
  - Decision making
  - Fairness
  - Ethics

- Automated decision making
- Human in the loop
- Trust and safety - content moderation
- Potential harm
- Environmental impacts
- Data minimization and anonymization

- **Security Controls and Monitoring**
  - Security monitoring metrics
  - Selecting the right controls
  - Implementing controls
  - Self-assessment of controls (CSA)
  - Control life cycle
  - Continuous monitoring
  - KPIs and KRIs for security controls and monitoring
  - Technical controls
  - Threat controls mapping
  - Security awareness training

Jul 6 - 7, 2026 | 8:30 AM - 4:30 PM EDT

Sep 14 - 15, 2026 | 8:30 AM - 4:30 PM EDT

Nov 16 - 17, 2026 | 8:30 AM - 4:30 PM EST

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/24/2026 3:57:24 AM