Advanced in AI Security Management (AAISM) Training

Duration: **2 Day**

BILGINC IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

The **Advanced in AI Security Management (AAISM)** course is an expert-level cybersecurity training program focused on securing, governing, and managing enterprise AI systems. Developed by ISACA, this certification equips professionals with the skills needed to ensure safe, ethical, and compliant AI adoption.

This accelerated training provides a comprehensive understanding of:

- AI governance frameworks
- AI risk management strategies
- Secure and ethical AI operations
- Enterprise-level AI security controls

The course aligns with globally recognized ISACA standards.

Why Choose AAISM?

- Specialize in AI security management
- Reduce enterprise AI risks
- Gain globally recognized certification
- Advance your cybersecurity career

Prerequisites

Participants are recommended to have:

- ISACA CISM or ISC2 CISSP certification
- Experience in security roles
- Basic knowledge of AI systems

Who Should Attend

This course is ideal for:

- Information security managers and consultants
- Governance, risk, and compliance professionals
- Cybersecurity leaders
- Organizations implementing AI security frameworks

Advanced in AI Security Management (AAISM) Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

What You Will Learn

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

- Manage AI governance frameworks
- Conduct AI risk assessments
- Evaluate AI technologies securely
- Define KPIs and KRIs for AI oversight
- Design AI security programs

Outline

Domain 1. AI governance and program management

- Stakeholder considerations, frameworks, and regulatory requirements
- Organisational structure, roles, and governance models
- Defining charters and establishing AI steering committees
- Risk appetite, tolerance, and framework alignment
- Selecting and applying appropriate AI governance frameworks
- Developing AI business use cases and managing privacy implications
- Establishing AI strategies, policies, and procedures
- Responsible and acceptable use of AI systems
- Managing AI assets and data lifecycles
- Creating AI asset inventories and data management protocols
- Model documentation, classification, and storage practices
- Implementing AI data protection and destruction measures
- Building an AI security management program
- Establishing documented plans, team roles, and proficiency standards
- Integrating AI-enabled security tools and performance metrics
- Developing KRIs and KPIs to measure AI security effectiveness
- Managing business continuity and incident response for AI
- Implementing AI-specific detection, notification, and escalation processes
- Designing AI response playbooks and red-button protocols
- Defining recovery objectives (RTO and RPO) from an AI perspective

Domain 2. AI risk management

- Conducting AI risk assessments and defining acceptable risk thresholds
- Performing impact, conformity, and privacy impact assessments (PIAs)
- Developing treatment plans and documenting AI-specific risk responses
- Implementing AI-focused penetration testing, vulnerability testing, and red teaming
- Managing adversarial and insider threats within AI ecosystems
- Identifying AI-enabled threats, deepfakes, and synthetic data misuse
- Applying threat intelligence to AI-based attack chains and anomaly detection
- Managing AI vendor and supply chain risk
- Conducting due diligence and defining accountability between provider and deployer
- Managing dependencies in AI software packages and libraries
- Establishing SLAs, ownership, and IP considerations for AI systems
- Implementing access control, liability, and vendor monitoring processes

Advanced in AI Security Management (AAISM) Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Domain 3. AI technologies and controls

- Designing AI security architecture aligned with secure-by-design principles
- Managing AI change control and secure development lifecycles (SDL)
- Securing infrastructure-as-code and model interconnectivity
- Managing AI model lifecycles, including selection, training, validation, and regression testing
- Implementing technical evaluation, verification, and validation (TEVV) of AI models
- Applying data management controls to mitigate data poisoning, bias, and accuracy issues
- Managing privacy, ethical, trust, and safety controls within AI systems
- Ensuring explainability, consent, transparency, and fairness in AI decision-making
- Maintaining human oversight (human-in-the-loop) in automated processes
- Applying trust and safety measures such as content moderation and harm prevention
- Monitoring environmental impact and ensuring data minimisation and anonymisation
- Designing and implementing AI security controls and continuous monitoring processes
- Mapping AI security threats to controls and metrics
- Implementing control life cycles and self-assessments (CSA)
- Delivering AI security awareness training to drive organisational readiness