ISACA

ISACA Advanced in AI Security Management.

Advanced in AI Security Management (AAISM)

Course Outline

ISACA Advanced in AI Security Management™ (AAISM) validates security management professionals' ability to demonstrate their expertise in AI. This credential builds upon existing security best practices to enhance expertise and adapt to the evolving AI-driven landscape, ensuring robust protection and a strategic edge.

Course Duration:
- 2 days
- Approximately 12 hours

Exam Duration:
- 90 questions
- Must be completed in 2 hours

Required Prerequisite:
- Must possess a CISM or CISSP to be eligible for certification.

CPE Requirements:
- A minimum of 10 hours of CPE/year in the AI domain.
- CPE can be applied to other certifications as well as part of the 20 annual /120 three year requirement.
- No additional three-year requirement.

Course Topics

1. AI Governance and Program Management

A. Stakeholder Considerations, Industry Frameworks, and Regulatory Requirements

- Organizational Structure and Overall Governance
- Roles and Responsibilities
- Charter and Steering Committee
- Identifying Stakeholders
- Risk Appetite and Tolerance
- Frameworks, Standards, and Regulations
- Selecting appropriate Frameworks
- Business and Use Cases for AI
- Privacy Considerations

B. AI-related Strategies, Policies, and Procedures

- AI Strategy
- Consumer v. Enterprise
- Buy vs. Build
- AI Policies
- Responsible Use
- Acceptable Use
- AI Procedures
- Implementation
- Manuals
- Ethics

C. 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

D. 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

E. 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

2. AI Risk Management

A. 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

B. 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

C. 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 changes

3. AI Technologies and Controls

A. 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

B. 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

C. Data Management Controls

- Data collection
- Data control
- Data Poisoning
- BIAS
- Accuracy
- Data position requirements

D. 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

E. Security Controls and Monitorin

- 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