ISACA Advanced in AI Security Management (AAISM)

Duration: 2 Days **Course Code: AAISM** **Version: 1.0**

Overview:

Build the expertise to lead secure, ethical, and resilient AI initiatives in todays evolving threat landscape.
The ISACA Advanced in AI Security Management certification is designed for experienced security professionals who are ready to lead in the evolving landscape of AI-driven enterprise environments. This course equips learners with the knowledge and tools to manage AI-specific risks, implement effective governance frameworks, and ensure the secure and ethical use of AI technologies across the organization. Participants will explore how AI is reshaping the threat landscape and gain practical strategies to reinforce their organizations security posture in response.
Throughout the course, learners will dive into three core domains: AI Governance and Program Management, AI Risk Management, and AI Technologies and Controls. These areas cover everything from designing AI governance models and aligning them with business objectives, to identifying AI-specific vulnerabilities, managing third-party risks, and embedding AI into secure architectures. The course also addresses critical topics such as data privacy, ethical AI use, and regulatory complianceensuring participants are well-prepared to advise stakeholders and lead secure AI initiatives.
Whether you're a CISM or CISSP holder looking to expand your expertise, or a security leader navigating the complexities of AI integration, this course offers a forward-looking credential that validates your ability to manage AI-related security challenges with confidence and clarity.

Target Audience:

- ACTIVE CISM OR CISSP HOLDERS
- PROVEN EXPERIENCE IN SECURITY OR ADVISORY ROLES
- SOME EXPERTISE ASSESSING, IMPLEMENTING AND MAINTAINING AI SYSTEMS

Objectives:

- AI Governance and Program Management including 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 business continuity and incident response.
- AI Risk Management including AI risk assessment, thresholds, and treatment; AI-related strategies, policies, and procedures; AI vendor and supply chain management.
- AI Technologies and Controls including AI security architecture and design; AI life cycle (model selection, training, and validation); data management controls; privacy, ethical, trust and safety controls; security controls and monitoring.

Prerequisites:

- Candidates must hold an active CISM or CISSP certification.
- Participants should have a foundational understanding of AI systems.
- CISM - ISACA CISM®, Certified Information Security Manager® incl QAE
- CISSP - Certified Information Systems Security Professional

Testing and Certification

-

Content:

1. AI Governance and Program Management

- 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

2. AI Risk Management

- AI Risk Assessment, Thresholds, and Treatment
- AI-related Strategies, Policies, and Procedures
- AI Vendor and Supply Chain Management

3. AI Technologies and Controls

- AI Security Architecture and Design
- AI Life Cycle (e.g., model selection, training, and validation)
- Data Management Controls
- Privacy, Ethical, Trust and Safety Controls
- Security Controls and Monitoring

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar