AAISM - Advanced in AI Security Management Certification Prep

Durée: 365 Jours **Réf de cours: AAISM** **Version: 1.0** **Méthodes d'apprentissage: E-learning**

Résumé:

Build the expertise to lead secure, ethical, and resilient AI initiatives in today's 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 organization's security posture in response. 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.

Throughout the course, learners will dive into three core domains:
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 Controlsincluding 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
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 compliance—ensuring participants are well-prepared to advise stakeholders and lead secure AI initiatives.

Learners will have access to the course for one year from date of purchase and will earn 11 CPE upon completion. This course has a seat time of approximately 11 hours and is accessed via the Learning Access tab of your MyISACA dashboard.
This course uses dynamic modules, with integrated videos, text, and interactive elements to ensure a thorough grasp of all three AAISM domains.
As you navigate through the course, you'll engage with a variety of educational tools and can use our structured study plan to guide your preparation to make sure you are ready for exam day.
The course content is equipped with adjustable settings for volume, speed, and quality, accommodating different learning preferences and ensuring optimal clarity. Features like closed captions and a transcript panel are also available to enhance your learning experience.

Public visé:

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

Objectifs pédagogiques:

- **After completing this course you should have a good understanding of:**
- 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.

Pré-requis:

Attendees should meet the following prerequisites:

- Candidates must hold an active CISM or CISSP certification.

Test et certification

Recommended as preparation for the following exam:

- **AAISM** - ISACA - Advanced in AI Security Management

- Participants should have a foundational understanding of AI systems.
- CISM - CISM® : Préparation à la certification Certified Information Security Manager®
- CISSP - Certified Information Systems Security Professional Certification Preparation

Contenu:

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