ISACA AAISM CERTIFICATION

ISACA AI Security Management Certification Questions & Answers

Exam Summary – Syllabus –Questions

AAISM
ISACA Advanced in AI Security Management (AAISM)
90 Questions Exam – 450 / 800 Cut Score – Duration of 150 minutes

Table of Contents:

Know Your AAISM Certification Well:

The AAISM is best suitable for candidates who want to gain knowledge in the ISACA Emerging Technology. Before you start your AAISM preparation you may struggle to get all the crucial AI Security Management materials like AAISM syllabus, sample questions, study guide.

But don't worry the AAISM PDF is here to help you prepare in a stress-free manner. The PDF is a combination of all your queries like-

- What is in the AAISM syllabus?
- How many questions are there in the AAISM exam?
- Which Practice test would help me to pass the AAISM exam at the first attempt?

Passing the AAISM exam makes you ISACA Advanced in AI Security Management (AAISM). Having the AI Security Management certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISACA AAISM AI Security Management Certification Details:

Exam Name	ISACA Advanced in AI Security Management (AAISM)
Exam Code	AAISM
Exam Price	ISACA Member: US $459 (USD) ISACA Nonmember: US $599 (USD)
Duration	150 mins
Number of Questions	90
Passing Score	450 / 800
Books / Training	**AAISM Online Review Course**
Schedule Exam	**Exam Registration**
Sample Questions	**ISACA AAISM Sample Questions**
Practice Exam	**ISACA AAISM Certification Practice Exam**

AAISM Syllabus:

Topic	Details	Weights
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	31%
AI Risk and Opportunity Management	- AI Risk Assessment, Thresholds, and Treatment - AI Threat and Vulnerability Management - AI Vendor and Supply Chain Management	31%
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	38%

ISACA AAISM Sample Questions:

Question: 1

When designing an AI security architecture, what is the PRIMARY purpose of using adversarial training?

a) To make AI models more resilient to potential attacks
b) To improve the fairness of AI model decisions
c) To reduce the computational cost of resisting attacks
d) To enhance AI model performance on standard datasets

Answer: a

Question: 2

Which of the following data management techniques BEST improves an AI model's performance by enhancing training data quality?

a) Data classification
b) Data access
c) Data scrubbing
d) Data encoding

Answer: c

Question: 3

What is the role of an AI governance committee within an organization?

a) To prioritize AI vendors over other business operations
b) To oversee AI implementation and ensure alignment with ethical guidelines
c) To solely focus on marketing AI products
d) To ensure AI models are proprietary and not shared with stakeholders

Answer: b

Question: 4

Which of the following is the BEST method to uncover known vulnerabilities in an AI-based web application that has been recently deployed?

a) Dynamic application security testing (DAST)
b) Static application security testing (SAST)
c) Runtime application self-protection (RASP)
d) Interactive application security testing (IAST)

Answer: a

Question: 5

When an AI impact assessment reveals biased training data, what is the MOST effective method to ensure regulatory compliance?

a) Keep the original dataset when the model's accuracy is high.
b) Rely on model transparency to validate decision making
c) Use diverse and representative datasets to monitor the bias.
d) Focus on ethical guidelines to validate model performance.

Answer: c

Question: 6

A hospital adopts an AI solution from an external vendor to help diagnose rare diseases. Which of the following BEST demonstrates the verification of security requirements for this technology?

a) Require contractual clauses stipulating periodic information security reviews.
b) Preview contractual clauses of mandatory security AI software update.
c) Perform regular in-depth vulnerability scans on the AI system.
d) Integrate requirements for sensitive data aligned with healthcare regulations.

Answer: d

Question: 7

Which of the following is the MOST effective approach to mitigate privacy concerns when an organization collects personal data through a third-party AI application?

a) Have the vendor sign a nondisclosure agreement.
b) Obtain data subject consent on the end user interface.
c) Apply encryption to safeguard personnel data.
d) Conduct a review of applicable data protection regulations.

Answer: b

Question: 8

Within which stage of the AI development life cycle should effective feature engineering be conducted?

a) Development
b) Testing
c) Design
d) Define

Answer: a

Question: 9

What is the MOST effective metric for monitoring AI solutions provided by AI vendors?

a) Wait for supplier reports before investigating.
b) Use real-time tools to track AI anomalies.
c) Prioritize endpoint logs over centralized platforms.
d) Track model input with key performance indicators.

Answer: b

Question: 10

The MOST effective AI-driven capability to ensure real-time business continuity is:

a) Predicting potential disruptions without taking preventive action
b) Sending alerts while waiting for manual intervention
c) Keeping logs of incidents for future analysis
d) Automating system failover to backup servers

Answer: d

Study Guide to Crack ISACA AI Security Management AAISM Exam:

- Getting details of the AAISM syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the AAISM exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISACA provided training for AAISM exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the AAISM sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on AAISM practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for AAISM Certification

Make EduSum.com your best friend during your ISACA Advanced in AI Security Management exam preparation. We provide authentic practice tests for the AAISM exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual AAISM exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the AAISM exam.

Start Online practice of AAISM Exam by visiting URL
https://www.edusum.com/isaca/aaism-isaca-advanced-ai-security-management