AAISM Exam Blueprint - Training AAISM Solutions

DOWNLOAD the newest Actualtests4sure AAISM PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1aZoa-5M7zOKEgS68X90AWkg2DXgGaQ0x

With the ever-increasing competition, people take ISACA AAISMcertification to exhibit their experience, skills, and abilities in a better way. Having ISACA Advanced in AI Security Management (AAISM) Exam AAISM certificate shows that you have better exposure than others. So, AAISM Certification also gives you an advantage in the industry when employers seek candidates for job opportunities. However, preparing for the ISACA AAISM exam can be a difficult and time-consuming process.

ISACA AAISM Exam Syllabus Topics:

Topic	Details
Topic 1	• AI Governance and Program Management: This section of the exam measures the abilities of AI Security Governance Professionals and focuses on advising stakeholders in implementing AI security through governance frameworks, policy creation, data lifecycle management, program development, and incident response protocols.
Topic 2	• AI Risk Management: This section of the exam measures the skills of AI Risk Managers and covers assessing enterprise threats, vulnerabilities, and supply chain risk associated with AI adoption, including risk treatment plans and vendor oversight.
Topic 3	• AI Technologies and Controls: This section of the exam measures the expertise of AI Security Architects and assesses knowledge in designing secure AI architecture and controls. It addresses privacy, ethical, and trust concerns, data management controls, monitoring mechanisms, and security control implementation tailored to AI systems.

>> AAISM Exam Blueprint <<

Training AAISM Solutions - AAISM Latest Dump

Ready to take the next level in your ISACA career? Pass the ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) exam with our updated AAISM exam dumps. Too often, candidates struggle to find credible study materials and end up wasting resources on outdated material. But with our platform, you can access real ISACA AAISM Practice Questions in three formats - PDF, web-based practice exams, and desktop practice test software. Whether you prefer to study on your smart device or offline on your computer, we have the tools you need to succeed.

ISACA Advanced in AI Security Management (AAISM) Exam Sample Questions (Q73-Q78):

NEW QUESTION # 73
Which of the following controls BEST mitigates the risk of bias in AI models?

- A. Diverse data sourcing strategies
- B. Cryptographic hash functions
- C. Robust access control techniques
- D. Regular data reconciliation

Answer: A

Explanation:
Bias in AI models primarily stems from limitations or imbalances in training data. The AAISM study materials emphasize that the most effective way to mitigate this risk is through diverse data sourcing strategies that ensure coverage across demographics, scenarios, and contexts. Access controls protect data security, not fairness. Data reconciliation ensures accuracy but does not address representational imbalance.
Cryptographic hashing preserves integrity but has no impact on bias mitigation. To reduce systemic unfairness, the critical control is sourcing diverse and representative data.
References:
AAISM Exam Content Outline - AI Technologies and Controls (Bias and Fairness Management) AI Security Management Study Guide - Data Governance and Bias Reduction Strategies

NEW QUESTION # 74
Which phase of the AI data life cycle presents the GREATEST inherent risk?

- A. Preparation
- B. Monitoring
- C. Training
- D. Maintenance

Answer: C

Explanation:
AAISM identifies training as the phase with the highest inherent risk because this is where:
* data poisoning can occur
* sensitive data may be exposed
* bias can be introduced
* model inversion risks originate
* security and privacy vulnerabilities are embedded
Preparation (C) carries risk but is less critical. Maintenance (B) and monitoring (A) involve operational safeguards, not foundational risk creation.
References: AAISM Study Guide - AI Data Life Cycle Risks; High-Risk Model Training Phase.

NEW QUESTION # 75
A large pharmaceutical company using a new AI solution to develop treatment regimens is concerned about potential hallucinations with the introduction of real-world data. Which of the following is MOST likely to reduce this risk?

- A. Human-in-the-loop
- B. AI impact analysis
- C. Data asset validation

- D. Penetration testing

Answer: A

Explanation:
AAISM materials identify human-in-the-loop governance as the most effective safeguard against risks such as hallucinations in AI systems used in high-stakes domains like healthcare. By ensuring that human experts validate outputs before they influence patient treatment decisions, organizations preserve accountability, safety, and accuracy. Penetration testing is a cybersecurity measure, not relevant to hallucination risk. AI impact analysis helps evaluate systemic effects but does not directly prevent faulty outputs. Data validation improves input quality but cannot fully prevent generative hallucinations. The key safeguard is human-in-the- loop oversight.
References:
AAISM Study Guide - AI Governance and Program Management (Human Oversight in High-Risk AI) ISACA AI Security Management - Mitigating Hallucinations in Generative AI

NEW QUESTION # 76
An organization plans to use AI to analyze the shopping patterns of its customers to predict interests and send targeted, customized marketing emails. Which of the following should be done FIRST?

- A. Obtain customer consent
- B. Update the terms of service
- C. Verify customer email addresses
- D. Train the marketing department

Answer: A

Explanation:
The first action, before any processing of personal data for AI-driven profiling and targeted communications, is to establish a lawful basis for processing. Under AAISM-aligned privacy governance, explicit and informed consent is prioritized for new or sensitive uses such as interest profiling and targeted marketing. Consent ensures purpose limitation, transparency, and user control prior to model ingestion and campaign activation.
Training teams, updating terms of service, or verifying contact details are important, but they do not provide legal authority to process data; therefore, they follow after consent is obtained.
References: AI Security Management™ (AAISM) Body of Knowledge - Privacy Governance and Lawful Basis; Purpose Limitation and Transparency; Consent Management in AI-enabled Marketing. AAISM Study Guide - Data Protection Controls for AI Profiling; Consent Capture and Record-Keeping.

NEW QUESTION # 77
Which of the following MOST effectively addresses bias in generative AI models?

- A. Data augmentation
- B. Data minimization
- C. Adversarial training
- D. Fairness constraints

Answer: D

Explanation:
AAISM identifies fairness constraints as a direct mechanism to mitigate and control model bias by embedding fairness requirements into optimization objectives during training.
Data augmentation (B) helps but is not a primary anti-bias control. Adversarial training (C) focuses on robustness, not fairness. Minimization (A) reduces data, often making bias worse.
References: AAISM Study Guide - Fairness, Bias Mitigation Techniques, Ethical AI Controls.

NEW QUESTION # 78
.....

Once you start to become diligent and persistent, you will be filled with enthusiasms. Nothing can defeat you as long as you are

optimistic. We sincerely hope that our AAISM study materials can become your new purpose. Our AAISM Exam Questions can teach you much practical knowledge, which is beneficial to your career development. And with the AAISM certification, you are bound to have a bighter future.

Training AAISM Solutions: https://www.actualtests4sure.com/AAISM-test-questions.html