

Prepare With ISACA AAISM Exam Questions [2025] A Genuine Information For You



2025 Latest TestKingFree AAISM PDF Dumps and AAISM Exam Engine Free Share: <https://drive.google.com/open?id=1zdvw55RxqBa59O7LuU3Dmwwg2-8sHwSYI>

Candidates who become ISACA AAISM certified demonstrate their worth in the ISACA field. The ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) certification is proof of their competence and skills. This is a highly sought-after skill in large ISACA companies and makes a career easier for the candidate. To become certified, you must pass the ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) certification exam. For this task, you need high-quality and accurate ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) exam dumps. We have seen that candidates who study with outdated ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) practice material don't get success and lose their resources.

Up to now our AAISM practice materials consist of three versions, all those three basic types are favorites for supporters according to their preference and inclinations. On your way moving towards success, our AAISM preparation materials will always serve great support. As long as you have any questions on our AAISM Exam Questions, you can just contact our services, they can give you according suggestion on the first time and ensure that you can pass the AAISM exam for the best way.

>> AAISM Updated Test Cram <<

ISACA AAISM Online Tests | AAISM Valid Study Questions

Overall, AAISM is committed to helping candidates achieve success in the ISACA AAISM exam. Their goal is to save students time and money, and they guarantee that candidates who use their product will pass the AAISM Exam on their first try. With the right study material and support team, passing the exam at the first attempt is an achievable goal.

ISACA AAISM Exam Syllabus Topics:

Topic	Details

Topic 1	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.
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 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.

ISACA Advanced in AI Security Management (AAISM) Exam Sample Questions (Q47-Q52):

NEW QUESTION # 47

Which of the following controls BEST mitigates the inherent limitations of generative AI models?

- A. Reverse engineering the models
- **B. Ensuring human oversight**
- C. Adopting AI-specific regulations
- D. Classifying and labeling AI systems

Answer: B

Explanation:

The AAISM governance framework emphasizes that the inherent limitations of generative AI—including hallucinations, bias, and unpredictability—are best mitigated by human oversight. Human-in-the-loop review ensures that outputs are validated before being used in sensitive or high-risk contexts. Regulatory adoption, system classification, and reverse engineering all play supporting roles but do not directly safeguard against the model's inherent unpredictability. Governance best practices highlight human oversight as the critical safeguard.

References:

AAISM Exam Content Outline - AI Governance and Program Management (Human Oversight and Accountability) AI Security Management Study Guide - Mitigating Generative AI Limitations

NEW QUESTION # 48

Which of the following controls BEST mitigates the risk of data poisoning?

- A. Digital watermarking
- **B. Data validation**
- C. Data set restoration
- D. Intrusion detection

Answer: B

Explanation:

The AAISM technical controls framework emphasizes data validation as the primary safeguard against data poisoning attacks. Poisoning occurs when attackers insert malicious or corrupted data into training sets.

Validation techniques verify the quality, authenticity, and consistency of input data before training, preventing compromised samples from corrupting the model. Restoration helps after compromise, watermarking protects ownership, and intrusion detection monitors networks rather than data quality. The most effective preventive measure is data validation.

References:

AAISM Study Guide - AI Technologies and Controls (Data Poisoning Mitigation) ISACA AI Security Management - Data Validation and Quality Controls

NEW QUESTION # 49

Which of the following is MOST important to consider when validating a third-party AI tool?

- A. Right to audit
- B. Industry analysis and certifications
- C. Roundtable testing
- D. Terms and conditions

Answer: A

Explanation:

The AAISM framework specifies that when adopting third-party AI tools, the right to audit is the most critical contractual and governance safeguard. This ensures that the organization can independently verify compliance with security, privacy, and ethical requirements throughout the lifecycle of the tool. Terms and conditions provide general usage guidance but often limit liability rather than ensuring transparency. Industry certifications may indicate good practice but do not substitute for direct verification. Roundtable testing is useful for evaluation but lacks enforceability. Only the contractual right to audit provides formal assurance that the tool operates in accordance with organizational policies and external regulations.

References:

AAISM Exam Content Outline - AI Governance and Program Management (Third-Party Governance) AI Security Management Study Guide - Vendor Oversight and Audit Rights

NEW QUESTION # 50

Which of the following is the BEST reason to immediately disable an AI system?

- A. Insufficient model training
- B. Excessive model drift
- C. Overly detailed model outputs
- D. Slow model performance

Answer: B

Explanation:

According to AAISM lifecycle management guidance, the best justification for disabling an AI system immediately is the detection of excessive model drift. Drift results in outputs that are no longer reliable, accurate, or aligned with intended purpose, creating significant risks. Performance slowness and overly detailed outputs are operational inefficiencies but not critical shutdown triggers. Insufficient training should be addressed before deployment rather than after. The trigger for immediate deactivation in production is excessive drift compromising reliability.

References:

AAISM Exam Content Outline - AI Governance and Program Management (Model Drift Management) AI Security Management Study Guide - Disabling AI Systems

NEW QUESTION # 51

Which of the following MOST effectively minimizes the attack surface when securing AI agent components during their development and deployment?

- A. Implement compartmentalization with least privilege enforcement.
- B. Consolidate event logs for correlation and centralized analysis.
- C. Deploy pre-trained models directly into production.
- D. Schedule periodic manual code reviews.

Answer: A

Explanation:

The most effective strategy to minimize attack surfaces in AI agent security is to apply compartmentalization and least privilege enforcement.

AAISM control frameworks emphasize:

- * Isolation of components (e.g., training, inference, data pipelines) to limit lateral movement.
- * Principle of least privilege to restrict access only to what is required for function.
- * Hardening AI pipelines through segmentation rather than relying solely on manual reviews or monitoring.

Pre-trained models and log centralization are useful but do not directly reduce the attack surface. Manual code reviews are important but insufficient against runtime exploitation. Thus, compartmentalization with least privilege enforcement is the most effective technical safeguard.

NEW QUESTION # 52

• • • • •

Do you want to pass the ISACA AAISM exam better and faster? Then please select the TestKingFree. It can help you achieve your dreams. TestKingFree is a website that provide accurate exam materials for people who want to participate in the IT certification. TestKingFree can help a lot of IT professionals to enhance their career blueprint. Our strength will make you incredible. You can try a part of the questions and answers about ISACA AAISM Exam to test our reliability.

AAISM Online Tests: <https://www.testkingfree.com/ISACA/AAISM-practice-exam-dumps.html>

- [illegible]

2025 Latest TestKingFree AAISM PDF Dumps and AAISM Exam Engine Free Share: <https://drive.google.com/open?id=1zdvw55RxqBa59O7LuU3Dmwig2-8sHwSYI>