AAISM Study Materials & AAISM Exam Preparatory & AAISM Test Prep

BTW, DOWNLOAD part of Getcertkey AAISM dumps from Cloud Storage: https://drive.google.com/open?id=1A82lILLPjj-KaZ2g8jCf8OJbcIa88Rpd

We have professional technicians examine the website every day, therefore if you buy AAISM exam cram from us, you can enjoy a clean and safe online shopping environment. What's more, we offer you free demo to have a try before buying AAISM exam torrent, you can know what the complete version is like through free demo. AAISM Exam Materials cover most of knowledge points for the exam, and you can improve your ability in the process of learning as well as pass the exam successfully if you choose us. We offer you free update for 365 days for AAISM exam materials after purchasing.

Are you planning to attempt the ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) exam of the AAISM certification? The first hurdle you face while preparing for the ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) exam is not finding the trusted brand of accurate and updated AAISM exam questions. If you don't want to face this issue then you are at the trusted Getcertkey is offering actual and Latest AAISM Exam Questions that ensure your success in the ISACA Advanced in AI Security Management (AAISM) Exam (AAISM) certification exam on your maiden attempt.

>> Flexible AAISM Testing Engine <<

Reliable ISACA AAISM Test Questions, Latest AAISM Test Guide

During the process of using our AAISM study materials, you focus yourself on the exam bank within the given time, and we will refer to the real exam time to set your AAISM practice time, which will make you feel the actual exam environment and build up confidence. Not only that you can get to know the real questins and answers of the AAISM Exam, but also you can adjust yourself to the real pace of the AAISM exam.

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 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 3	• 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.

ISACA Advanced in AI Security Management (AAISM) Exam Sample Questions (Q189-Q194):

NEW QUESTION # 189
Implementing which of the following would MOST effectively address bias in generative AI models?

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

Answer: D

Explanation:
AAISM identifies fairness constraints (e.g., constrained optimization, debiasing objectives, conditional generation controls, and post-processing calibrations) as the most direct, measurable method to mitigate disparate outcomes in generative systems. While data augmentation can help with coverage, and adversarial training improves robustness, fairness constraints explicitly target distributional fairness and outcome equity in generated content, aligning with governance and compliance goals.
References: AI Security Management (AAISM) Body of Knowledge - Fairness & Bias Management in Generative AI; Metrics, Constraints, and Remediation. AAISM Study Guide - Fairness Objectives, Post-hoc Debiasing, and Evaluation Protocols.

NEW QUESTION # 190
Which of the following is the MAIN objective of the operational phase of AI life cycle management?

- A. Align the model to business needs
- B. Optimize the model's algorithms
- C. Monitor model performance
- D. Obtain end-user feedback on the model

Answer: C

Explanation:
In the operational phase, AAISM emphasizes continuous monitoring of models for performance, stability, robustness, drift, data quality, security events, and policy compliance. This includes telemetry, thresholds, alerts, incident response for AI failures, and evidence collection for audits. Alignment to business needs is established earlier in planning/governance; algorithmic optimization and feedback collection are supporting activities, but the primary operational objective is live monitoring and assurance to keep risk within tolerance.
References:* AI Security Management™ (AAISM) Body of Knowledge: AI Life Cycle-Operate/Monitor; Ongoing Performance & Drift Monitoring; AI Incident Management* AAISM Study Guide: Operational Controls, Metrics & SLAs/SLOs; Evidence & Audit Readiness in Production

NEW QUESTION # 191

A programmer suspects an AI system is inferring sensitive user information. What is the BEST action?

- A. Conduct a code review
- B. Alert the CIO
- C. Suggest fine-tuning
- D. Inform the governance panel

Answer: D

Explanation:
AAISM directs that potential privacy, ethical, or compliance risks must be escalated to the AI Governance Panel, the body responsible for oversight, risk approval, and corrective action.
Fine-tuning (B) is premature and may worsen risk. Code review (C) does not address model-level inference issues. Escalating directly to the CIO (D) bypasses the required governance process.
References: AAISM Study Guide - AI Governance Committees; Escalation Procedures.

NEW QUESTION # 192
An organization is planning to commission a third-party AI system to make decisions using sensitive data.
Which of the following metrics is MOST important for the organization to consider?

- A. Accessibility rating
- B. Accuracy thresholds
- C. Model response time
- D. Service availability

Answer: B

Explanation:
When AI systems make consequential decisions over sensitive data, AAISM requires explicit performance thresholds tied to decision quality-i.e., accuracy (and related error/false-rate limits) aligned to business risk appetite and regulatory expectations. Availability and latency are important service metrics, but decision integrity and error bounds are primary risk drivers in sensitive contexts. Establishing, monitoring, and enforcing minimum accuracy thresholds (with subgroup performance checks) is essential to reduce harm, ensure fairness/compliance, and support auditability.
References:* AI Security Management™ (AAISM) Body of Knowledge: Risk-aligned performance metrics; decision quality thresholds; harm and error-rate governance in sensitive processing.* AI Security Management™ Study Guide: Metric selection for high-risk AI; accuracy, false positive/negative limits, and acceptance criteria tied to business controls.

NEW QUESTION # 193
A retail organization implements an AI-driven recommendation system that utilizes customer purchase history. Which of the following is the BEST way for the organization to ensure privacy and comply with regulatory standards?

- A. Conducting quarterly retraining of the AI model to maintain the accuracy of recommendations
- B. Maintaining a register of legal and regulatory requirements for privacy
- C. Storing customer data indefinitely to ensure the AI model has a complete history
- D. Establishing a governance committee to oversee AI privacy practices

Answer: B

Explanation:
According to the AI Security Management™ (AAISM) study framework, compliance with privacy and regulatory standards must begin with a formalized process of identifying, documenting, and maintaining applicable obligations. The guidance explicitly notes that organizations should maintain a comprehensive register of legal and regulatory requirements to ensure accountability and alignment with privacy laws. This register serves as the foundation for all governance, risk, and control practices surrounding AI systems that handle personal data.
Maintaining such a register ensures that the recommendation system operates under the principles of privacy by design and privacy by default. It allows decision-makers and auditors to trace every AI data processing activity back to relevant compliance obligations, thereby demonstrating adherence to laws such as GDPR, CCPA, or other jurisdictional mandates.
Other measures listed in the options contribute to good practice but do not achieve the same direct compliance outcome. Retraining models improves technical accuracy but does not address legal obligations. Oversight committees are valuable but require the

documented register as a baseline to oversee effectively. Indefinite storage of customer data contradicts regulatory requirements, particularly the principle of data minimization and storage limitation.
AAISM Domain Alignment:
This requirement falls under Domain 1 - AI Governance and Program Management, which emphasizes organizational accountability, policy creation, and maintaining compliance documentation as part of a structured governance program.
References from AAISM and ISACA materials:
AAISM Exam Content Outline - Domain 1: AI Governance and Program Management AI Security Management Study Guide - Privacy and Regulatory Compliance Controls ISACA AI Governance Guidance - Maintaining Registers of Applicable Legal Requirements

NEW QUESTION # 194
......

If you have Getcertkey's ISACA AAISM exam training materials, we will provide you with one-year free update. This means that you can always get the latest exam information. As long as the Exam Objectives have changed, or our learning material changes, we will update for you in the first time. We know your needs, and we will help you gain confidence to pass the ISACA AAISM Exam. You can be confident to take the exam and pass the exam.