Guide AAISM Torrent - Free Sample AAISM Questions

BONUS!!! Download part of ExamBoosts AAISM dumps for free: https://drive.google.com/open?id=1PLRfMf2rCKDJN0z7L74LZc1i5aI5pny8

Did you often feel helpless and confused during the preparation of the exam? Do you want to find an expert to help but feel bad about the expensive tutoring costs? Don't worry. AAISM learning materials can help you to solve all the problems. AAISM learning material always regards helping students to pass the exam as it is own mission. With AAISM learning materials, you only need to pay half the money to get the help of the most authoritative experts.

We have a special technical customer service staff to solve all kinds of consumers' problems on our AAISM exam questions. If you have questions when installing or using our AAISM practice engine, you can always contact our customer service staff via email or online consultation. They will solve your questions about AAISM Preparation materials with enthusiasm and professionalism, giving you a timely response whenever you contact them.

>> Guide AAISM Torrent <<

Free Sample AAISM Questions | Real AAISM Dumps

Considering many exam candidates are in a state of anguished mood to prepare for the AAISM exam, our company made three versions of AAISM real exam materials to offer help. All these variants due to our customer-oriented tenets. As a responsible company over ten years, we are trustworthy. In the competitive economy, this company cannot remain in the business for long. But we keep being the leading position in contrast. We are reactive to your concerns and also proactive to new trends happened in this 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 (Q114-Q119):

NEW QUESTION # 114
Which of the following MOST effectively minimizes the attack surface when securing AI agent components during their development and deployment?

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

Answer: C

Explanation:
The most effective strategy tominimize attack surfacesin 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 ofleast privilegeto 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 reviewsare important but insufficient against runtime exploitation.
Thus,compartmentalization with least privilege enforcementis the most effective technical safeguard.

NEW QUESTION # 115
Which of the following BEST reduces the risk of exposing sensitive data through the output of large language models (LLMs) in applications?

- A. Enforcing least privilege access
- B. Implementing data sanitization techniques
- C. Conducting adversarial testing
- D. Encrypting data in transit and at rest

Answer: B

Explanation:
AAISM materials make clear that the best safeguard against sensitive information being leaked through the outputs of LLMs is data sanitization. This involves filtering, redacting, or masking sensitive content before the model can use it, thereby preventing unintended disclosure in outputs. Encryption protects confidentiality in storage and transmission but does not stop output leaks. Adversarial testing helps identify vulnerabilities but does not prevent exposure by itself. Least privilege access restricts who can interact with the model but does not sanitize the content of its outputs. The control most directly tied to preventing leakage is implementing data sanitization techniques.
References:

AAISM Exam Content Outline - AI Technologies and Controls (Data Leakage Prevention) AI Security Management Study Guide - Sensitive Data Controls in Generative AI

NEW QUESTION # 116
An aerospace manufacturing company that prioritizes accuracy and security has decided to use generative AI to enhance operations. Which of the following large language model (LLM) adoption plans BEST aligns with the company's risk appetite?

- A. Developing a private LLM to automate non-critical functions
- B. Contracting LLM access from a reputable third-party provider
- C. Purchasing an LLM dataset on the open market
- D. Developing a public LLM to automate critical functions

Answer: A

Explanation:
AAISM recommends aligning AI adoption with organizational risk appetite by limiting blast radius, protecting sensitive data, and staging adoption in lower-risk domains first. Building a private LLM for non-critical functions preserves data control, enables tighter governance (access control, logging, evaluation), and confines any model errors away from safety- or mission-critical operations. A public LLM for critical functions (A) is misaligned with a high-assurance posture; buying open-market datasets (B) raises provenance and licensing risk; third-party access (C) can be appropriate but still introduces vendor/visibility limits and data residency concerns that may not meet aerospace security needs.
References: AI Security Management (AAISM) Body of Knowledge - Risk Appetite Mapping to AI Use Cases; Criticality Segmentation; Data Control & Deployment Models. AAISM Study Guide - Phased Adoption for High-Assurance Environments; Private vs. Hosted LLM Trade-offs; Governance, Evaluation, and Containment Patterns.

NEW QUESTION # 117
Which of the following is the MOST important factor to consider when selecting industry frameworks to align organizational AI governance with business objectives?

- A. Risk register
- B. Risk threshold
- C. Risk tolerance
- D. Risk appetite

Answer: D

Explanation:
According to AAISM governance principles, the risk appetite of the organization is the most important factor in selecting appropriate frameworks for AI governance. Risk appetite defines the level of risk an organization is willing to accept in pursuit of its objectives, ensuring frameworks are aligned with strategic goals. Risk tolerance and thresholds are operational measures derived from appetite, and the risk register is a documentation tool. The foundational consideration for framework alignment is the organization's risk appetite.
References:
AAISM Exam Content Outline - AI Governance and Program Management (Risk Appetite in Governance Alignment) AI Security Management Study Guide - Framework Selection and Business Strategy

NEW QUESTION # 118
An organization is deploying an automated AI cybersecurity system. Which of the following would be the MOST effective strategy to minimize human error and improve overall security?

- A. Implementing manual monitoring of potential alerts
- B. Conducting periodic penetration testing
- C. Utilizing machine learning (ML) algorithms to ensure responsible use
- D. Using historical data to train AI detection software

Answer: D

Explanation:

Training detection models on relevant, representative historical data improves signal quality, reduces false positives, and automates triage-directly lowering human workload and error rates (e.g., alert fatigue, missed correlations). Penetration testing is valuable but episodic and does not systematically reduce day-to-day operator error. "Ensure responsible use" is a governance aim, not a concrete method to cut human error in detection. Manual monitoring increases reliance on human judgment and is prone to inconsistency.
References: AI Security Management™ (AAISM) Body of Knowledge: Model Development & Evaluation Controls; Data Selection and Representativeness; Operationalization to Reduce Human Error. AAISM Study Guide: Tuning Detection Systems with Historical Corpora; Alert Quality, Precision/Recall, and SOC Workflow Integration.

NEW QUESTION # 119
.....

For candidates who are going to buy AAISM learning materials online, they may have the concern about the money safety. We apply international recognition third party for payment, therefore if you choose us, your safety of money and account can be guaranteed. Moreover, we have a professional team to compile and verify the AAISM Exam Torrent, therefore the quality can be guaranteed. We offer you free demo to have a try before buying, and you know the content of the complete version through the free demo. We have professional service staff for AAISM exam dumps, and if you have any questions, you can have a conversation with us.

Free Sample AAISM Questions: https://www.examboosts.com/ISACA/AAISM-practice-exam-dumps.html

P.S. Free & New AAISM dumps are available on Google Drive shared by ExamBoosts: https://drive.google.com/open?id=1PLRfMf2rCKDJN0z7L74LZc1i5aI5pny8