Ace Your Exam with ActualTestsQuiz ISACA AAISM Desktop Practice Test Software

The AAISM certification costs somewhere between 100$ and 1000$. Thus we save your amount by offering the best prep material with up to 1 year of free updates so that you pass the exam on the first attempt without having to retry, saving your time, effort, and money! ActualTestsQuiz offers the ISACA AAISM Dumps at a very cheap price.

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.

>> AAISM Test Dumps Demo <<

Latest Updated ISACA AAISM Test Dumps Demo: ISACA Advanced in AI Security Management (AAISM) Exam - Trustworthy AAISM Exam Content

To help you prepare for AAISM examination certification, we provide you with a sound knowledge and experience. The questions designed by ActualTestsQuiz can help you easily pass the exam. The ActualTestsQuiz ISACA AAISM practice including AAISM exam questions and answers, AAISM test, AAISM books, AAISM study guide.

ISACA Advanced in AI Security Management (AAISM) Exam Sample Questions (Q168-Q173):

NEW QUESTION # 168
Which of the following BEST describes an adversarial attack on an AI model?

- A. Attacking underlying hardware
- B. Providing inputs that mislead the model into incorrect predictions
- C. Conducting denial-of-service attacks on AI APIs
- D. Reverse-engineering the model using social engineering

Answer: B

Explanation:
AAISM defines adversarial attacks as manipulations of input data (text, image, audio, numeric values) designed to cause the model to produce incorrect or harmful predictions.
Hardware attacks (A) are infrastructure threats. Social engineering (C) targets people, not models. DoS attacks (D) affect availability, not model decision pathways.
References: AAISM Study Guide - Adversarial Threats; Input Manipulation.

NEW QUESTION # 169
A military contractor discovered that its large language model (LLM) is at high risk of being targeted by advanced persistent threat (APT) actors seeking to exploit the model to access confidential information.
Which of the following attacks is the HIGHEST priority to protect against?

- A. Unauthorized tuning
- B. Data poisoning
- C. Model inversion
- D. Model distillation

Answer: C

Explanation:
AAISM classifies model inversion as a privacy/information-leakage threat where adversaries infer or reconstruct sensitive training data or attributes from model outputs-directly jeopardizing confidential information targeted by APTs. While data poisoning, unauthorized tuning, and model distillation present material risks (integrity, governance/IP theft), the scenario's stated objective-accessing confidential information-most directly maps to inversion. Accordingly, AAISM prioritizes defenses such as output regularization, confidence suppression/calibration, overfitting controls, privacy-preserving techniques, and strict access/telemetry on inference interfaces.
References:* AI Security Management (AAISM) Body of Knowledge: Model Security-Inference-Time Threats (Inversion, Membership Inference) and Confidentiality Risks* AAISM Study Guide: Leakage Mitigations-Regularization, Output Minimization/Calibration, Access Controls & Monitoring on Model Interfaces

NEW QUESTION # 170
A post-incident investigation finds that an AI-powered anti-money laundering system inadvertently allowed suspicious transactions because certain risk signals were disabled to reduce false positives. Which of the following governance failures does this BEST demonstrate?

- A. Excessive reliance on external consultants for model design
- B. Lack of sufficient computing resources for the AI system
- C. Absence of metrics and dashboard for analysts
- D. Insufficient model validation and change control processes

Answer: D

Explanation:
AAISM requires formal model change governance: documented justification, risk assessment, validation /verification (V&V), approvals, and post-deployment monitoring when altering features, thresholds, or signals. Disabling risk indicators to reduce false positives without rigorous validation and controlled rollout reflects a failure in model validation and change control, which AAISM treats as a core safeguard against unintended harms and regulatory breaches.
References: AI Security Management (AAISM) Body of Knowledge - Model Risk Governance; Change Management & Approvals; Validation/Verification Requirements. AAISM Study Guide - Control Gates for Feature/Threshold Changes; Post-Change Monitoring and Backout Criteria.

NEW QUESTION # 171
A large language model (LLM) has been manipulated to provide advice that serves an attacker's objectives.
Which of the following attack types does this situation represent?

- A. Evasion attack
- B. Privilege escalation
- C. Model inversion
- D. Data poisoning

Answer: A

Explanation:
AAISM categorizes the manipulation of an LLM at inference time, where crafted inputs cause outputs to serve attacker objectives, as an evasion attack. Evasion attacks exploit weaknesses in the model's decision- making boundaries by altering queries to produce compromised or misleading outputs. Privilege escalation refers to unauthorized access rights, data poisoning targets the training phase, and model inversion reconstructs training data. In this case, manipulation of outputs to align with an attacker's goals reflects an evasion attack.
References:
AAISM Exam Content Outline - AI Risk Management (Adversarial Attack Types) AI Security Management Study Guide - Evasion and Manipulation Risks

NEW QUESTION # 172
Which of the following is the MOST effective action an organization can take to address data security risk when using generative AI features in an application?

- A. Establish guidelines and best practices with third parties for intellectual property ownership
- B. Rely on the AI provider's independent third-party audit reports for assurance
- C. Establish policies and awareness training for acceptable use of AI
- D. Require opt-out provisions for data usage in service agreements

Answer: D

Explanation:
AAISM directs organizations to manage third-party AI risks through contractual and technical controls that explicitly govern data use, retention, training/fine-tuning, isolation, and deletion. The most effective data- security action when consuming generative AI features is to require enforceable opt-out provisions that prohibit the provider from using the organization's data for training or secondary purposes and that mandate retention limits and secure deletion. Third-party audit reports (A) provide assurance but do not guarantee provider behavior for your specific data; awareness policies (B) are necessary but insufficient to control external processing; IP ownership guidelines (D) address legal rights, not data-security risk.
References: AI Security Management (AAISM) Body of Knowledge - Third-Party/Procurement Controls; Data Use & Retention Clauses; Training/Fine-tuning Opt-Out; Secure Deletion and Purpose Limitation.

NEW QUESTION # 173
.....

Our AAISM exam questions can assure you that you will pass the AAISM exam as well as getting the related certification under the guidance of our AAISM study materials as easy as pie. Firstly, the pass rate among our customers has reached as high as 98% to 100%, which marks the highest pass rate in the field. Secondly, you can get our AAISM Practice Test only in 5 to 10 minutes after

payment, which enables you to devote yourself to study as soon as possible.

Trustworthy AAISM Exam Content: https://www.actualtestsquiz.com/AAISM-test-torrent.html

- AAISM Latest Exam □ Demo AAISM Test □ Reliable AAISM Test Book □ Search for □ AAISM □ and easily obtain a free download on □ www.testkingpass.com □ □AAISM Latest Braindumps
- AAISM Online Tests □ AAISM Latest Braindumps □ AAISM Valid Study Guide □ Download ✔ AAISM □✔□ for free by simply entering ➽ www.pdfvce.com □ website □AAISM Accurate Study Material
- ISACA AAISM Questions To Complete Your Preparation [2026] □ Download ➥ AAISM □ for free by simply searching on " www.practicevce.com " □Exams AAISM Torrent
- AAISM Valid Study Guide □ Actual AAISM Test □ New AAISM Test Test □ Open □ www.pdfvce.com □ enter ➡ AAISM □□□ and obtain a free download □AAISM Online Tests
- Free PDF Quiz Efficient AAISM - ISACA Advanced in AI Security Management (AAISM) Exam Test Dumps Demo □ Search on 《 www.prepawayete.com 》 for ⇛ AAISM ⇚ to obtain exam materials for free download □New AAISM Test Test
- AAISM Exam Overview □ AAISM Exam Overview □ New AAISM Test Test ❣ Copy URL 【 www.pdfvce.com 】 open and search for ☀ AAISM □☀□ to download for free □Test AAISM Testking
- AAISM Latest Exam Registration □ Accurate AAISM Study Material □ Actual AAISM Test □ Immediately open 「 www.dumpsquestion.com 」 and search for ➠ AAISM □ to obtain a free download □AAISM Exam Overview
- Accurate AAISM Study Material □ AAISM Exam Sims □ Valid Dumps AAISM Pdf □ Open { www.pdfvce.com } enter ✔ AAISM □✔□ and obtain a free download □AAISM Accurate Test
- Valid Dumps AAISM Pdf □ AAISM Valid Study Guide □ AAISM Latest Exam □ Search for （ AAISM ） and obtain a free download on [www.dumpsquestion.com] □AAISM Latest Braindumps
- AAISM Online Tests □ Reliable AAISM Test Book □ Exams AAISM Torrent □ Copy URL ➡ www.pdfvce.com □□□ open and search for □ AAISM □ to download for free □AAISM PDF Question
- AAISM Valid Study Guide □ Exams AAISM Torrent □ AAISM Valuable Feedback ☢ Search for □ AAISM □ and download it for free on ▸ www.easy4engine.com ◂ website □Exams AAISM Torrent
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes