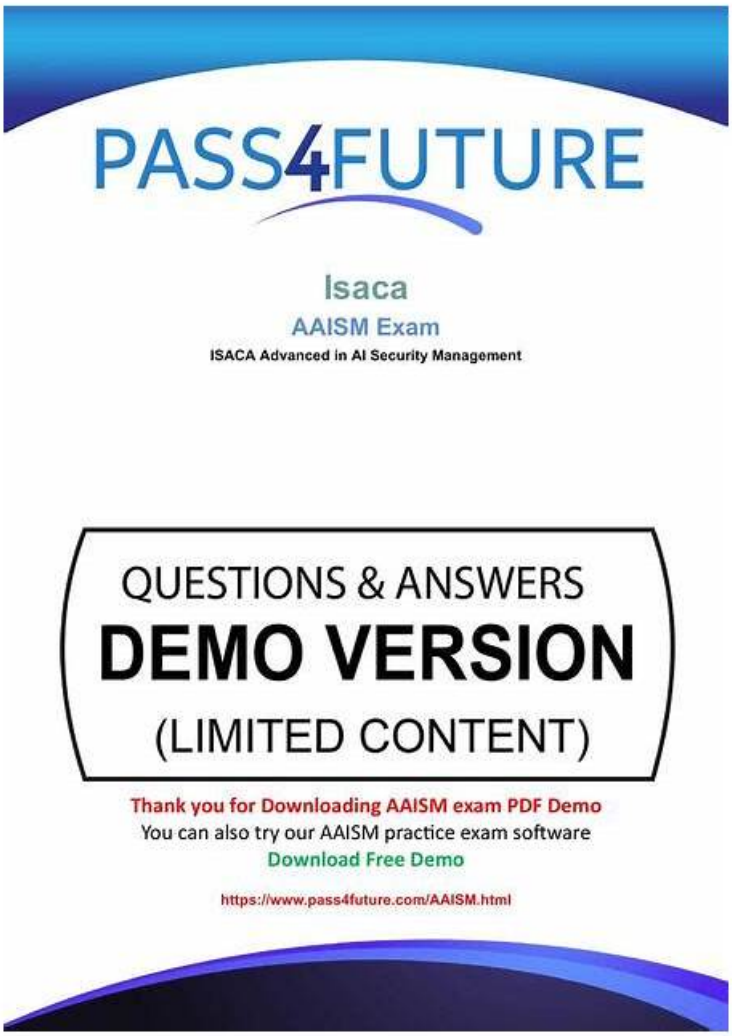
Updated and User Friendly Pass4sures AAISM Exam PDF Questions File



P.S. Free & New AAISM dumps are available on Google Drive shared by Pass4sures: https://drive.google.com/open?id=12_tM5WBa-0mJovOS61GHTN1tZgN0MvUR

The test software used in our products is a perfect match for Windows' AAISM learning material, which enables you to enjoy the best learning style on your computer. Our AAISM study materials also use the latest science and technology to meet the new requirements of authoritative research material network learning. Unlike the traditional way of learning, the great benefit of our AAISM Study Materials are that when the user finishes the exercise, he can get feedback in the fastest time.

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.

Professional Reliable AAISM Exam Camp to Obtain ISACA Certification

Since our company's establishment, we have devoted mass manpower, materials and financial resources into AAISM exam materials and until now, we have a bold idea that we will definitely introduce our study materials to the whole world and make all people that seek fortune and better opportunities have access to realize their life value. Our AAISM Practice Questions, therefore, is bound to help you pass though the exam and win a better future. We will also continuously keep a pioneering spirit and are willing to tackle any project that comes your way.

ISACA Advanced in AI Security Management (AAISM) Exam Sample Questions (Q220-Q225):

NEW QUESTION # 220
Which of the following controls would BEST help to prevent data poisoning in AI models?

- A. Regularly updating the foundational model
- B. Increasing the size of the training data set
- C. Establishing continuous monitoring
- D. Implementing a strict data validation mechanism

Answer: D

Explanation:
The most direct preventative control against data poisoning is robust data validation/ingestion gating: provenance checks, schema and constraint validation, anomaly/outlier screening, label consistency tests, and whitelist/blacklist source controls before data reaches training pipelines. Larger datasets (A) don't inherently prevent poisoning; monitoring (C) is detective; updating a foundation model (D) does not address tainted inputs entering the pipeline.
References: AI Security Management™ (AAISM) Body of Knowledge - Adversarial ML Threats and Training-Time Attacks; Secure Data Ingestion and Validation Controls. AAISM Study Guide - Poisoning Prevention: Provenance, Validation, and Sanitization Gates.

NEW QUESTION # 221
An organization is implementing AI agent development across engineering teams. What should AI-specific training focus on?

- A. Output moderation, hallucination handling, policy alignment
- B. Dataset bias, explainability, fairness
- C. Prompt injection, agent memory control, insecure tool execution
- D. API abuse, data leakage, third-party plug-in risk

Answer: C

Explanation:
AAISM states that AI agent security training should focus on the unique risks of agentic systems, which include:
* prompt injection
* memory control and context hijacking
* unsafe tool execution (agents triggering unauthorized actions)

These risks are specific to autonomous or semi-autonomous AI agents.
Bias, fairness (B) and output moderation (C) are important but not the most critical for agent security. API abuse and plug-in risk (D) matter but are secondary.
References: AAISM Study Guide - Agentic AI Security; Prompt Injection and Tool Execution Risks.

NEW QUESTION # 222
Secure aggregation enhances the security of federated learning systems by:

- A. Applying differential privacy techniques to mask sensitive information in training data
- B. Encrypting individual model updates during transmission to ensure only the server can access the data
- C. Processing client updates in isolation to reduce the risk of exposing sensitive information
- D. Ensuring individual client contributions remain confidential even if the server is compromised

Answer: D

Explanation:
Secure aggregation cryptographically aggregates client updates so that the server learns only the sum /aggregate, not any single client's update. Properly implemented, the server cannot recover individual contributions-even if compromised-thereby preserving client confidentiality. Option C (encryption in transit) is insufficient because decryption at the server reveals updates; Option A is procedural, not cryptographic; Option B (differential privacy) is a separate technique and not the defining property of secure aggregation.
References: AAISM Body of Knowledge: Privacy-Preserving ML-Federated Learning and Secure Aggregation; AAISM Study Guide: Threat Models for Aggregation Servers and Confidentiality Guarantees.

NEW QUESTION # 223
An organization concerned about the ethical and responsible use of a newly developed AI product should consider implementing:

- A. An accountability model
- B. Vendor monitoring
- C. Model cards
- D. Security by design

Answer: A

Explanation:
The AAISM framework highlights that organizations adopting AI must ensure accountability structures are in place to govern ethical and responsible use. An accountability model assigns clear responsibility for decisions, outputs, and risks related to AI systems. While model cards provide transparency about a model's design and performance, they are primarily documentation tools. Vendor monitoring focuses on third-party oversight, not internal accountability. Security by design improves resilience but does not by itself address ethical use. The governance approach that most directly supports responsible and ethical AI deployment is an accountability model.
References:
AAISM Study Guide - AI Governance and Program Management (Ethical AI and Accountability) ISACA AI Security Management - Responsible AI Practices

NEW QUESTION # 224
Which of the following methods provides the MOST effective protection against model inversion attacks?

- A. Implementing regularization output
- B. Using adversarial training
- C. Reducing the model's complexity
- D. Increasing the number of training iterations

Answer: A

Explanation:
AAISM classifies model inversion as a privacy leakage threat where adversaries infer sensitive attributes or training records from model outputs. The recommended technical risk treatments emphasize reducing overfitting and information leakage via regularization

and output-side constraints. Regularization (e.g., stronger penalties, output smoothing, confidence calibration, temperature limiting, and related techniques) reduces the model's tendency to memorize training data and curtails exploitable signal in outputs.
* A (adversarial training) targets perturbation robustness, not primary for inversion.
* B (reducing complexity) can help but is a coarse control with limited assurance versus explicit anti-leakage regularization.
* D (more iterations) typically increases overfitting and leakage risk.
AAISM further notes that privacy-preserving training and output minimization are preferred where feasible; among the listed options, regularization most directly addresses inversion risk.
References:* AI Security Management™ (AAISM) Body of Knowledge: Model Security-Privacy leakage threats (membership inference, inversion) and mitigation via regularization and output minimization.* AI Security Management™ Study Guide: Overfitting controls, calibration and confidence suppression as defenses against inference attacks.

NEW QUESTION # 225
.....

As candidates don't know what to expect on the ISACA Advanced in AI Security Management (AAISM) Exam exam, and they have to prepare for the unknown. In this case, candidates can take ISACA AAISM practice test to get help with their ISACA AAISM exam preparation. The real AAISM exam dumps by Pass4sures give them an idea of the ISACA Advanced in AI Security Management (AAISM) Exam AAISM Exam structure so that they can prepare accordingly. The ISACA AAISM PDF Questions and practice tests by Pass4sures play a big role in your ISACA AAISM exam success.