HOT AAISM Testking 100% Pass | The Best Exams ISACA Advanced in AI Security Management (AAISM) Exam Torrent Pass for sure

P.S. Free & New AAISM dumps are available on Google Drive shared by ITdumpsfree: https://drive.google.com/open?id=1xWtv-kUielCknbmzMVs97PaFILdYr3yM

Our ITdumpsfree is the most reliable backing for every AAISM candidate. All study materials required in AAISM exam are provided by Our ITdumpsfree. Once you purchased our AAISM exam dump, we will try our best to help you Pass AAISM Exam. Additionally, our excellent after sales service contains one-year free update service and the guarantee of dump cost full refund if you fail the exam with our dump.

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 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 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.

Your Investment with ITdumpsfree ISACA AAISM Exam Questions is Secured

If you intend to take the ISACA AAISM exam to open doors to high-paying jobs, you need an authentic ISACA AAISM practice exam material to get a passing score on the first attempt. Many people do not find a platform that is credible to purchase updated ISACA AAISM prep material. This leads to a waste of time and money, and ultimately failure in the AAISM exam.

ISACA Advanced in AI Security Management (AAISM) Exam Sample Questions (Q253-Q258):

NEW QUESTION # 253
A large corporation has received an influx of sophisticated credential-phishing emails and wants to leverage an AI solution to detect and quarantine these messages before they reach employees. Which of the following blue-team AI features is BEST suited to this task?

- A. Natural language processing (NLP)
- B. Large language model (LLM)
- C. Natural language generation (NLG)
- D. Retrieval-augmented generation (RAG)

Answer: A

Explanation:
For pre-delivery phishing detection and classification, the most appropriate capability is NLP- tokenization, feature extraction, semantic similarity, and supervised classifiers (e.g., transformer-based classifiers) tuned on phishing corpora and indicators. NLP models score messages and drive automated quarantine policies. An LLM (Option A) is a model type, not a specific blue-team feature; NLG (Option C) is for generation, not detection; RAG (Option D) augments responses with retrieved knowledge but does not by itself optimize classification and quarantine of phishing emails.
References:
AAISM Body of Knowledge: Defensive AI Use Cases; Text Classification Pipelines for Security Operations; Email Security and AI-Driven Triage.
AAISM Study Guide: NLP for Threat Detection; Model Evaluation for Precision/Recall in Security Classifiers; SOC Integration and Automated Containment.

NEW QUESTION # 254
A CISO has been tasked with providing key performance indicators (KPIs) on the organization's newly launched AI chatbot. Which of the following are the BEST metrics for the CISO to recommend?

- A. Customer effort score and user retention rate
- B. Error rate and bias detection
- C. Response time and throughput
- D. Explainability and F1 score

Answer: B

Explanation:
For executive security and governance reporting, AAISM prioritizes risk- and harm-oriented KPIs that reflect safety, reliability, and responsible behavior of AI systems. Error rate (safety/quality signal) and bias detection (fairness/compliance signal) provide leading indicators of model risk, potential user harm, and regulatory exposure-key interests for a CISO. Explainability and F1 (A) are model performance/interpretability metrics; customer effort/retention (B) are business CX metrics; response time/throughput (C) are operational SRE metrics. While valuable, they are secondary to risk-centric KPIs for CISO oversight.
References: AI Security Management™ (AAISM) Body of Knowledge - AI Risk Metrics and Assurance; Governance Dashboards for AI. AAISM Study Guide - Operationalizing AI Controls; Safety, Fairness, and Compliance Indicators for Executive Reporting.
O Error rate and bias detection

NEW QUESTION # 255
A global organization experienced multiple incidents of staff pasting confidential data into public chatbots.
Which action is MOST important to reduce short-term risk?

- A. Deliver role-based, scenario-driven AI security training mapped to job functions
- B. Publish an AI acceptable use policy and collect signatures
- C. Require employees to complete an annual generic phishing and deepfake module
- D. Block access to public LLMs at the network perimeter

Answer: A

Explanation:
AAISM states that the most effective short-term mitigation for unintentional data leakage into public AI tools is targeted, role-based AI security awareness, focused on:
* what data cannot be entered
* consequences of leakage
* real-world scenarios employees face
An acceptable-use policy (C) is necessary but insufficient alone. Blocking LLMs (D) may reduce access but does not change user behavior and may cause shadow AI usage. Generic phishing training (B) does not address AI misuse risks.
References: AAISM Study Guide - AI Security Awareness; Human-Centric Data Leakage Prevention.

NEW QUESTION # 256
During the deployment of a generative AI platform, a risk assessment highlighted threats such as data leakage and prompt manipulation. Which of the following is the BEST way to ensure appropriate control selection?

- A. Map identified AI threats to enterprise control catalogs and integrate AI-specific safeguards where gaps exist
- B. Apply AI-specific controls from external frameworks without customization and initiate monitoring to expedite compliance
- C. Postpone control selection until deployment and address risk through enhanced monitoring
- D. Rely primarily on vendor-provided security features and seek third-party certifications

Answer: A

Explanation:
AAISM requires that control selection be threat-led and context-specific, aligning AI threats to the organization's existing enterprise control catalogs (security, privacy, resilience) and augmenting them with AI- specific safeguards where coverage is insufficient. This ensures consistency with the risk appetite, removes duplication, and closes AI-unique gaps (e.g., prompt injection, data leakage from context windows, model misuse). Generic reliance on vendors or uncustomized external frameworks does not ensure fit-for-purpose coverage, and deferring control selection to post-deployment contradicts proactive risk treatment.
References: AI Security Management™ (AAISM) Body of Knowledge - Governance & Program Controls; Control Selection and Tailoring; Threat-to-Control Mapping for AI Systems; Risk Appetite & Control Assurance Alignment.

NEW QUESTION # 257
When evaluating a new AI tool for intrusion prevention, which of the following is the MOST important consideration to ensure the tool fits within the existing program architecture?

- A. Confirm tool capabilities align with the control objectives.
- B. Ensure automated response orchestration.
- C. Prioritize a tool that offers real-time anomaly detection.
- D. Select a tool that integrates with the existing SIEM.

Answer: A

Explanation:
The highest-priority fit criterion for introducing a new AI security capability is alignment to the organization' s established control objectives and program architectures. Control objectives encode what must be achieved (e.g., detection coverage, response timeliness, accountability, auditability) and are the basis for requirements traceability across governance, risk, and technical controls. Ensuring the tool's capabilities directly satisfy those objectives provides architectural fit, policy conformance, and measurable assurance. While integration (e.g., SIEM), detection features (e.g., real-time anomaly detection), and orchestration are important, they are secondary to proving the tool maps to-and can be verified against-the control objectives that define the program's intended

outcomes.
References:* AI Security Management™ (AAISM) Body of Knowledge: AI Governance and Program Management - Security program alignment, control objectives, and requirements traceability* AI Security Management™ Study Guide: Control objective mapping, architecture fit criteria, and solution selection governance

NEW QUESTION # 258
.....

Many of our users have told us that they are really busy. Students have to take a lot of professional classes and office workers have their own jobs. They can only learn our AAISM exam questions in some fragmented time. And our AAISM training guide can meet your requirements. For there are three versions of AAISM learning materials and are not limited by the device. They are the versions of PDF, Software and APP online.