Isaca

Exam Questions AAISM

ISACA Advanced in AI Security Management (AAISM) Exam

NEW QUESTION 1
Which of the following is the BEST mitigation control for membership inference attacks on AI systems?

A. Model ensemble techniques
B. AI threat modeling
C. Differential privacy
D. Cybersecurity-oriented red teaming

Answer: C

NEW QUESTION 2
Which attack type is MOST likely to cause model drift?

A. Model stealing
B. Perfect knowledge
C. Data poisoning
D. Membership inference

Answer: C

NEW QUESTION 3
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. Select a tool that integrates with the existing SIEM.
C. Prioritize a tool that offers real-time anomaly detection.
D. Ensure automated response orchestration.

Answer: A

NEW QUESTION 4
A SaaS-based LLM system has risks including prompt injection, data poisoning, and model exfiltration. What is the BEST way to ensure consistent risk treatment?

A. Apply control baselines from a recognized industry standard
B. Implement an AI threat control matrix mapping threats to controls and assurance
C. Focus on post-deployment red teaming
D. Rely on vendor audit reports and SLAs

Answer: B

NEW QUESTION 5
The PRIMARY goal of data poisoning attacks is to:

A. compromise the confidentiality of output data from the model
B. compromise the confidentiality of model input data
C. manipulate the behavior of the model during development
D. undermine the integrity of the AI system??s outputs

Answer: D

NEW QUESTION 6
An organization is updating its vendor arrangements to facilitate the safe adoption of AI technologies. Which of the following would be the PRIMARY challenge in delivering this initiative?

A. Failure to adequately assess AI risk
B. Inability to sufficiently identify shadow AI within the organization
C. Unwillingness of large AI companies to accept updated terms
D. Insufficient legal team experience with AI

Answer: C

NEW QUESTION 7
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. Require employees to complete an annual generic phishing and deepfake module
C. Publish an AI acceptable use policy and collect signatures
D. Block access to public LLMs at the network perimeter

Answer: A

NEW QUESTION 8
Which of the following strategies is the MOST effective way to protect against AI data poisoning?

A. Ensuring the model is trained on diverse data sources
B. Increasing model complexity
C. Using robust data validation techniques and anomaly detection
D. Incorporating more features and data into model training

Answer: C

NEW QUESTION 9
Which of the following would BEST help mitigate vulnerabilities associated with hidden triggers in generative AI models?

A. Regularly retraining the model using a diverse data set
B. Applying differential privacy and masking sensitive patterns in the training data
C. Incorporating adversarial training to expose and neutralize potential triggers
D. Monitoring model outputs and suspicious patterns to detect trigger activations

Answer: C

NEW QUESTION 10
An organization is facing a deepfake attack intended to manipulate stock prices. The organization??s crisis communication plan has been activated. Which of the following is MOST important to include in the initial response?

A. Conduct employee awareness training on recognizing deepfake videos and audio
B. Provide clarifying information in a pre-approved public statement
C. Conduct a detailed forensic analysis to identify the source of the deepfake
D. Engage with brand monitoring services to track social media activity

Answer: B

NEW QUESTION 10
Which of the following is the BEST reason to immediately disable an AI system?

A. Excessive model drift
B. Slow model performance
C. Overly detailed model outputs
D. Insufficient model training

Answer: A

NEW QUESTION 11
What is the PRIMARY purpose of a dedicated AI management system policy?

A. Minimizing environmental impact
B. Optimizing AI model accuracy
C. Complying with external regulations
D. Providing a framework to set AI objectives

Answer: D

NEW QUESTION 16
Which of the following is the MOST important consideration for an organization that has decided to adopt AI to leverage its competitive advantage?

A. Develop a comprehensive strategic roadmap for AI integration
B. Develop a comprehensive risk management process to address AI-related issues
C. Develop internal training programs on AI governance, risk, and compliance (GRC)
D. Develop a business case for the procurement of AI monitoring tools

Answer: A

NEW QUESTION 20
For a life insurance company deploying AI for fraud detection, which factor is MOST critical?

A. Robustness
B. Accuracy
C. Explainability
D. Adaptability

Answer: A

NEW QUESTION 25
Which of the following approaches BEST helps reduce model bias?

A. Ensuring diversity in training data sources

B. Utilizing a more complex architecture
C. Decreasing frequency of model updates
D. Increasing the number of labels per instance

Answer: A

NEW QUESTION 29
An organization is adopting an agentic AI solution from an external vendor to support internal IT operations. Which of the following provides the MOST reliable and independently verifiable evidence of implemented security controls?

A. Industry benchmarking peer review
B. Third-party audit reports
C. Internal red-team testing reports
D. General AI security whitepapers

Answer: B

NEW QUESTION 31
An organization is adopting an agentic AI solution from an external vendor to support its internal IT operations. To evaluate the security posture of this system, which of the following provides the MOST reliable and independently verifiable evidence of implemented security controls?

A. Internal red team testing reports
B. Industry benchmarking peer review
C. General AI security whitepapers
D. Third-party audit reports

Answer: D

NEW QUESTION 35
An organization is evaluating a SaaS-based HR system that uses AI for resume vetting. Which control is MOST important?

A. Inclusion of diverse and representative training data
B. Availability of backups
C. Vendor conformity assessments
D. Encryption and isolation of customer data

Answer: A

NEW QUESTION 36
In the context of generative AI, which of the following would be the MOST likely goal of penetration testing during a red-teaming exercise?

A. Generate outputs that are unexpected using adversarial inputs
B. Stress test the model??s decision-making process
C. Degrade the model??s performance for existing use cases
D. Replace the model??s outputs with entirely random content

Answer: A

NEW QUESTION 39
Which of the following AI-driven systems should have the MOST stringent recovery time objective (RTO)?

A. Health support system
B. Credit risk modeling system
C. Car navigation system
D. Industrial control system

Answer: D

NEW QUESTION 41
When documenting information about machine learning (ML) models, which of the following artifacts BEST helps enhance stakeholder trust?

A. Hyperparameters
B. Data quality controls
C. Model card
D. Model prototyping

Answer: C

NEW QUESTION 46
Which of the following strategies is the MOST effective way to protect against AI data poisoning?

A. Increasing model complexity to better handle data variations
B. Ensuring the model is trained on diverse data sources
C. Incorporating more features and data into model training
D. Using robust data validation techniques and anomaly detection

Answer: D

NEW QUESTION 48
Which of the following is the BEST way to reduce the risk of misuse of an AI agent that has access to critical data and systems?

A. Validate agent compliance with output restrictions
B. Allow users to configure the agent for productivity
C. Prohibit users from manipulating agent behavior
D. Limit human review of AI decisions

Answer: A

NEW QUESTION 51
When integrating AI for innovation, which of the following can BEST help an organization manage security risk?

A. Re-evaluating the risk appetite
B. Seeking third-party advice
C. Evaluating compliance requirements
D. Adopting a phased approach

Answer: D

NEW QUESTION 54
What BEST ensures a proper business continuity plan (BCP) for an AI solution?

A. Enhancing monitoring for model failure
B. Testing AI infrastructure failover mechanisms
C. Implementing access controls
D. Increasing backup restoration detail

Answer: B

NEW QUESTION 55
When preparing for an AI incident, which of the following should be done FIRST?

A. Implement a communication channel to report AI incidents
B. Establish a cross-functional incident response team with AI knowledge
C. Establish recovery processes for AI system models and data sets
D. Create containment and eradication procedures for AI-related incidents

Answer: B

NEW QUESTION 57
A financial organization is concerned about AI data poisoning. Which control BEST mitigates this risk?

A. Implementing a break-glass policy
B. Transparency with customers about data sources
C. Using training data from multiple sources
D. Delivering AI-specific security awareness training

Answer: C

NEW QUESTION 62
When robust input controls are not practical on a large language model (LLM) to prevent prompt injection attacks from external threats, which of the following would be the BEST compensating control to address the risk?

A. Review and annotate the AI system's outputs
B. Implement identity and access management (IAM)
C. Conduct human reviews of the AI system's inputs
D. Fine-tune the system to validate the AI system's inputs

Answer: A

NEW QUESTION 65
A CISO must provide KPIs for the organization??s newly deployed AI chatbot. Which metrics are BEST?

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

Answer: B

NEW QUESTION 68

Which of the following BEST ensures AI components are validated as part of disaster recovery testing?

A. Disconnecting primary model training clusters to test retraining workflow during extended outages
B. Simulating denial of service (DoS) attacks against AI APIs to evaluate detection capabilities
C. Running simulated data loss scenarios by erasing test records from the AI system??s feature store
D. Monitoring model performance metrics during failover and recovery to assess system stability

Answer: D

NEW QUESTION 69
Personal data used to train AI systems can BEST be protected by:

A. Erasing personal data after training
B. Ensuring the quality of personal data
C. Anonymizing personal data
D. Hashing personal data

Answer: C

NEW QUESTION 71
Which of the following metrics BEST evaluates the ability of a model to correctly identify all true positive instances?

A. F1 score
B. Recall
C. Precision
D. Specificity

Answer: B

NEW QUESTION 74
Which of the following is the BEST way to ensure role clarity and staff effectiveness when implementing AI-assisted security monitoring tools?

A. Defer implementation until the security team can be expanded with data scientists.
B. Update the security program to include cross-functional AI-specific responsibilities.
C. Transition responsibilities for AI tools to external consultants for improved scalability.
D. Increase training budgets for business staff to obtain vendor-neutral AI certifications.

Answer: B

NEW QUESTION 77
Which of the following MOST effectively minimizes the attack surface when securing AI agent components during their development and deployment?

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

Answer: D

NEW QUESTION 78
A school district contracts a third-party provider for AI-based curriculum recommendations. Which of the following is the BEST way to ensure the vendor uses AI responsibly?

A. Confirming the AI solution supports single sign-on (SSO)
B. Verifying the vendor has updated terms of service
C. Requiring the vendor to provide the model card
D. Ensuring the vendor offers 24/7 technical support

Answer: C

NEW QUESTION 82
An AI application development team has been given access to user information and now must format it to be readable by the AI model. During which phase of the data life cycle would this MOST likely occur?

A. Data minimization
B. Data preparation
C. Data collection
D. Data normalization

Answer: B

NEW QUESTION 85
Which AI data management technique involves creating validation and test data?

A. Learning

B. Splitting
C. Training
D. Annotating

Answer: B

NEW QUESTION 88
Which of the following would BEST help an organization align its AI initiatives with business objectives?

A. Complying with applicable AI-related regulations
B. Ensuring ethical use of AI technologies in projects
C. Establishing an AI governance committee
D. Protecting enterprise information used by AI projects

Answer: C

NEW QUESTION 92
Which of the following is MOST important to monitor in order to ensure the effectiveness of an organization??s AI vendor management program?

A. Vendor compliance with AI-related requirements
B. Vendor reviews of external AI threat reports
C. Vendor results in compliance training programs
D. Vendor participation in industry AI research

Answer: A

NEW QUESTION 95
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 IP ownership guidelines with third parties
B. Require opt-out provisions for data usage
C. Establish policies and awareness training for acceptable AI use
D. Rely on the AI provider??s independent audit reports

Answer: C

NEW QUESTION 96
Which of the following is the PRIMARY purpose of a dedicated AI system policy?

A. Ensuring environmental impact is minimized
B. Optimizing AI accuracy
C. Providing a framework to set AI objectives
D. Complying with external regulations

Answer: C

NEW QUESTION 99
Secure aggregation enhances federated learning security by:

A. Encrypting individual model updates so only the server can access them
B. Applying differential privacy to training data
C. Ensuring client contributions remain confidential even if the server is compromised
D. Processing client updates in isolation

Answer: C

NEW QUESTION 104
Which of the following is the MAIN objective of the operational phase of AI life cycle management?

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

Answer: C

NEW QUESTION 109
Which area of intellectual property law presents the GREATEST challenge in determining copyright protection for AI-generated content?

A. Enforcing trademark rights associated with AI systems
B. Determining the rightful ownership of AI-generated creations
C. Protecting trade secrets in AI technologies
D. Establishing licensing frameworks for AI-generated works

Answer: B

NEW QUESTION 114
Which of the following should be the PRIMARY consideration for an organization concerned about liabilities associated with unforeseen behavior from agentic AI systems?

A. Model dependencies
B. Approved base models
C. Accountability model
D. Acceptable risk level

Answer: C

NEW QUESTION 119
An organization is reviewing an AI application to determine whether it is still needed. Engineers have been asked to analyze the number of incorrect predictions against the total number of predictions made. Which of the following is this an example of?

A. Control self-assessment (CSA)
B. Model validation
C. Key performance indicator (KPI)
D. Explainable decision-making

Answer: C

NEW QUESTION 121
An organization uses an AI tool to scan social media for product reviews. Fraudulent social media accounts begin posting negative reviews attacking the organization's product. Which type of AI attack is MOST likely to have occurred?

A. Model inversion
B. Deepfake
C. Availability attack
D. Data poisoning

Answer: C

NEW QUESTION 122
An AI research team is developing a natural language processing model that relies on several open-source libraries. Which of the following is the team??s BEST course of action to ensure the integrity of the software packages used?

A. Maintain a list of frequently used libraries to ensure consistent application in projects
B. Scan the packages and libraries for malware prior to installation
C. Use the latest version of all libraries from public repositories
D. Retrain the model regularly to handle package and library updates

Answer: B

NEW QUESTION 123
Which of the following is the MOST effective way to prevent a model inversion attack?

A. Monitor model output for anomalies
B. Utilize data pseudonymization
C. Implement differential privacy during model training
D. Ensure data minimization

Answer: C

NEW QUESTION 125
An aerospace manufacturer prioritizing accuracy and security wants to use generative AI. Which LLM adoption plan BEST aligns with its risk appetite?

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

Answer: A

NEW QUESTION 130
Which of the following BEST describes the role of risk documentation in an AI governance program?

A. Providing a record of past AI-related incidents for audits
B. Outlining the acceptable levels of risk for AI-related initiatives
C. Offering detailed analyses of technical risk and vulnerabilities
D. Demonstrating governance, risk, and compliance (GRC) for external stakeholders

Answer: B

NEW QUESTION 134
An organization using an AI model for financial forecasting identifies inaccuracies caused by missing data. Which of the following is the MOST effective data cleaning technique to improve model performance?

A. Increasing the frequency of model retraining with the existing data set
B. Applying statistical methods to address missing data and reduce bias
C. Deleting outlier data points to prevent unusual values impacting the model
D. Tuning model hyperparameters to increase performance and accuracy

Answer: B

NEW QUESTION 136
Cybersecurity teams should FIRST be embedded in the:

A. Model testing phase
B. Model deployment phase
C. Model training phase
D. Model design phase

Answer: D

NEW QUESTION 140
Which AI model is BEST suited to ensure explainability in an HR department??s pre- screening tool for candidate resumes?

A. Support vector machine
B. Neural network
C. Decision tree
D. Gradient boosting machine

Answer: C

NEW QUESTION 144
An organization's CIO provided the AI steering committee with a list of AI technologies in use and tasked them with categorizing the technologies by risk. Which of the following should the committee do FIRST?

A. Begin grouping similar AI products and solutions together
B. Identify vulnerabilities related to the technologies in use
C. Ensure the AI technologies are included in the asset inventory
D. Assess risk levels based on risk appetite and regulatory requirements

Answer: C

NEW QUESTION 147
How can an organization best remain compliant when decommissioning an AI system that recorded patient data?

A. Perform a post-destruction risk assessment
B. Ensure backups are tested and access controls are audited
C. Update governance policies based on lessons learned
D. Ensure a certificate of destruction is received and archived

Answer: D

NEW QUESTION 149
To ensure the ethical and responsible use of AI, which of the following AI usage policy metrics is MOST important for an organization to monitor?

A. Frequency of policy consultations by employees
B. Number of reported policy violations
C. Number of AI projects that have undergone policy compliance review
D. Frequency of policy reviews and updates

Answer: C

NEW QUESTION 152
To ensure AI tools do not jeopardize ethical principles, it is MOST important to validate that:

A. The organization has implemented a responsible development policy
B. Outputs of AI tools do not perpetuate adverse biases
C. Stakeholders have approved alignment with company values
D. AI tools are evaluated by the privacy department before implementation

Answer: B

NEW QUESTION 155
Which BEST addresses hallucination risk in AI systems?

A. Human oversight
B. Recursive chunking
C. Automated output validation
D. Content enrichment

Answer: A

NEW QUESTION 159
Which of the following methods provides the MOST effective protection against model inversion attacks?

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

Answer: C

NEW QUESTION 164
Which of the following controls BEST mitigates the risk of data poisoning?

A. Data set restoration
B. Data validation
C. Digital watermarking
D. Intrusion detection

Answer: B

NEW QUESTION 168
During the creation of a new large language model (LLM), an organization procured training data from multiple sources. Which of the following is MOST likely to address the CISO's security and privacy concerns?

A. Data augmentation
B. Data minimization
C. Data classification
D. Data discovery

Answer: B

NEW QUESTION 169
Which of the following is the GREATEST risk inherent to implementing generative AI?

A. Lack of employee training
B. Unidentified asset vulnerabilities
C. Inadequate return on investment (ROI)
D. Potential intellectual property violations

Answer: D

NEW QUESTION 171
Which of the following would BEST help to prevent the compromise of a facial recognition AI system through the use of alterations in facial appearance?

A. Enhancing training data to increase variance
B. Monitoring the system for misuse cases
C. Fine-tuning the AI model to decrease hallucinations
D. Implementing a secondary AI system to confirm images

Answer: A

NEW QUESTION 174
A vendor switched its chatbot??s AI model without due diligence, causing unethical investment advice. What control BEST prevents this scenario?

A. Master services agreement
B. Change management
C. Shared responsibility model
D. Data minimization

Answer: B

NEW QUESTION 176
Which of the following AI data management techniques involves creating validation and test data?

A. Training
B. Annotating
C. Splitting
D. Learning

Answer: C

NEW QUESTION 181
A security assessment revealed that attackers could access sensitive company data through chat interface injection. What is the BEST mitigation?

A. Conducting regular security audits
B. Manually reviewing AI model outputs
C. Implementing input validation and templates
D. Ensuring continuous monitoring and tagging

Answer: C

NEW QUESTION 183
Which of the following factors is MOST important for preserving user confidence and trust in generative AI systems?

A. Bias minimization
B. Access controls and secure storage solutions
C. Transparent disclosure and informed consent
D. Data anonymization

Answer: C

NEW QUESTION 188
Which of the following controls BEST mitigates the inherent limitations of generative AI models?

A. Ensuring human oversight
B. Adopting AI-specific regulations
C. Classifying and labeling AI systems
D. Reverse engineering the models

Answer: A

NEW QUESTION 192
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AAISM Practice Exam Features:

* AAISM Questions and Answers Updated Frequently

* AAISM Practice Questions Verified by Expert Senior Certified Staff

* AAISM Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AAISM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year