Exam Questions AAISM

ISACA Advanced in AI Security Management (AAISM) Exam

https://www.2passeasy.com/dumps/AAISM/

NEW QUESTION 1
Which testing technique is BEST for determining how an AI model makes decisions?

A. Red team
B. Black box
C. White box
D. Blue team

Answer: C

NEW QUESTION 2
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 3
An organization has requested a developer to apply AI algorithms to existing modules in order to improve customer service quality. At this stage, which of the following should be considered FIRST?

A. The developer may need to be held accountable for business inquiries raised by customers
B. IT management may need to revise the service agreement if AI behavior cannot be predefined
C. Project sponsors may need to agree on a phased approach in order to ensure safe release
D. The organization may need to explain the performance of the applied AI algorithm

Answer: B

NEW QUESTION 4
When evaluating a third-party AI service provider, which of the following master services agreement provisions is MOST critical for managing security risk?

A. Prohibiting the use of customer data for model training
B. Restricting query volume thresholds
C. Sharing real-time log information
D. Guaranteeing unlimited model retraining requests

Answer: A

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
Which of the following employee awareness topics would MOST likely be revised to account for AI-enabled cyber risk?

A. Clean desk policy
B. Social engineering
C. Malicious insider threats
D. Authentication controls

Answer: B

NEW QUESTION 8
Which of the following is the MOST serious consequence of an AI system correctly guessing the personal information of individuals and drawing conclusions based on that information?

A. The exposure of personal information may result in litigation
B. The publicly available output of the model may include false or defamatory statements about individuals
C. The output may reveal information about individuals or groups without their knowledge
D. The exposure of personal information may lead to a decline in public trust

Answer: C

NEW QUESTION 9
The PRIMARY purpose of adopting and implementing AI architecture within an organizational AI program is to:

A. Deploy fast and cost-efficient AI systems
B. Provide a basis for identifying threats and vulnerabilities
C. Align AI system components with business goals
D. Ensure powerful and scalable AI systems

Answer: C

NEW QUESTION 10
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 10
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 13
A retail organization implements an AI-driven recommendation system that utilizes customer purchase history. Which of the following is the BEST way for the organization to ensure privacy and comply with regulatory standards?

A. Conducting quarterly retraining of the AI model to maintain the accuracy of recommendations
B. Maintaining a register of legal and regulatory requirements for privacy
C. Establishing a governance committee to oversee AI privacy practices
D. Storing customer data indefinitely to ensure the AI model has a complete history

Answer: B

NEW QUESTION 15
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 17
An organization is deploying a large language model (LLM) and is concerned that input manipulations may compromise its integrity. Which of the following is the MOST effective way to determine an acceptable risk threshold?

A. Restrict all user inputs containing special characters
B. Deploy a real-time logging and monitoring system
C. Implement a static risk threshold by limiting LLM outputs
D. Assess the business impact of known threats

Answer: D

NEW QUESTION 22
What BEST protects trade secrets related to AI technologies during their life cycle?

A. Enforcing trademark rights
B. Restricting access to sensitive data
C. Patenting AI algorithms and data
D. Watermarking AI output

Answer: B

NEW QUESTION 23
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 25
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 28
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 29
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. Conducting periodic penetration testing
B. Using historical data to train AI detection software
C. Utilizing machine learning (ML) algorithms to ensure responsible use
D. Implementing manual monitoring of potential alerts

Answer: B

NEW QUESTION 32
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
An organization develops and implements an AI-based plug-in for users that summarizes their individual emails. Which of the following is the GREATEST risk associated with this application?

A. Lack of application vulnerability scanning
B. Data format incompatibility
C. Insufficient rate limiting for APIs
D. Inadequate controls over parameters

Answer: D

NEW QUESTION 38

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 41
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 44
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 45
AI developers often find deep learning systems difficult to explain PRIMARILY because:

A. Knowledge dynamically changes without logs
B. Neural network architectures include statistical methods not fully understood
C. Algorithms rely on probability theories
D. Training data is spread across public domains

Answer: B

NEW QUESTION 47
As organizations increasingly rely on vendors to develop AI systems, which of the following is the MOST effective way to monitor vendors and ensure compliance with ethical and security standards?

A. Conducting regular audits of vendor processes and adherence to AI development guidelines
B. Requiring vendors to monitor their adherence to ethics and security standards
C. Mandating that vendors share source code and AI documentation with the contracting party
D. Allowing vendors to self-attest ethical AI compliance and implement benchmark monitoring

Answer: A

NEW QUESTION 48
Which of the following is the MOST effective way to mitigate the risk of deepfake attacks?

A. Relying on human judgment for oversight
B. Limiting employee access to AI tools
C. Validating the provenance of the data source
D. Using a general-purpose large language model (LLM) to detect fraud

Answer: C

NEW QUESTION 50
Which of the following recommendations would BEST help a service provider mitigate the risk of lawsuits arising from generative AI??s access to and use of internet data?

A. Activate filtering logic to exclude intellectual property flags
B. Disclose service provider policies to declare compliance with regulations
C. Appoint a data steward specialized in AI to strengthen security governance
D. Review log information that records how data was collected

Answer: A

NEW QUESTION 52
The PRIMARY ethical concern of generative AI is that it may:

A. Produce unexpected data that could lead to bias

B. Cause information integrity issues
C. Cause information to become unavailable
D. Breach the confidentiality of information

Answer: B

NEW QUESTION 53
Which of the following is the MOST important consideration when an organization is adopting generative AI for personalized advertising?

A. Fraud risk
B. Reputational risk
C. Commercial risk
D. Regulatory risk

Answer: D

NEW QUESTION 57
Employees are regularly using open-source generative AI without guidance. What should be the CISO??s GREATEST concern?

A. Model hallucinations
B. Data leakage
C. Lack of monitoring
D. Policy violations

Answer: B

NEW QUESTION 60
When using AI as part of incident response, which of the following BEST ensures the automation aligns with regulatory and governance obligations?

A. Use deep learning models to autonomously classify all incidents
B. Train the AI incident response platform to mirror legacy response workflows and log containment
C. Apply anomaly detection models to filter incoming threats and automate containment
D. Implement a tiered automation strategy where severity ratings inform the need for human oversight

Answer: D

NEW QUESTION 61
An organization decides to use an anomaly-based intrusion detection system (IDS) integrated with a generative adversarial network–enabled AI tool. The integrated tool would MOST effectively detect intrusions by leveraging:

A. synthetic intrusion data to train the tool??s components
B. validation data sets to enable highly realistic AI decisions
C. automated rule creation to increase model performance
D. classified real intrusion data based on labeled data

Answer: A

NEW QUESTION 62
An organization is planning to commission a third-party AI system to make decisions using sensitive data. Which of the following metrics is MOST important for the organization to consider?

A. Model response time
B. Service availability
C. Accessibility rating
D. Accuracy thresholds

Answer: D

NEW QUESTION 65
Which of the following BEST describes an adversarial attack on an AI model?

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

Answer: B

NEW QUESTION 68
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 73
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 76
Which of the following security framework elements BEST helps to safeguard the integrity of outputs generated by AI algorithms?

A. Risk exposure due to bias in AI outputs is kept within an acceptable range
B. Ethical standards are incorporated into security awareness programs
C. Management is prepared to disclose AI system architecture to stakeholders
D. Responsibility is defined for legal actions related to AI regulatory requirements

Answer: A

NEW QUESTION 77
A data scientist creating categories and training an algorithm on large data sets is performing which learning technique?

A. Supervised
B. Reinforcement
C. Unsupervised
D. Machine learning (ML)

Answer: A

NEW QUESTION 79
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 80
Which of the following should be the MOST important consideration when conducting an AI impact assessment?

A. Achieve business objectives
B. Effect on employee retention
C. Security awareness training
D. Reputation of the organization

Answer: A

NEW QUESTION 82
An organization recently introduced a generative AI chatbot that can interact with users and answer their queries. Which of the following would BEST mitigate hallucination risk identified by the risk team?

A. Performing model testing and validation
B. Training the foundational model on large data sets
C. Ensuring model developers have been trained in AI risk
D. Fine-tuning the foundational model

Answer: D

NEW QUESTION 84
A financial organization uses AI to detect potential fraudulent activities but is concerned about the impact of potential data poisoning. Which of the following controls would BEST mitigate this risk?

A. Being transparent with customers about the data sources
B. Implementing an updated and tested break-glass policy
C. Delivering AI-specific security awareness training
D. Using training data from multiple sources

Answer: D

NEW QUESTION 89
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 92
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. Rely primarily on vendor-provided security features and seek third-party certifications
B. Map identified AI threats to enterprise control catalogs and integrate AI-specific safeguards where gaps exist
C. Apply AI-specific controls from external frameworks without customization and initiate monitoring to expedite compliance
D. Postpone control selection until deployment and address risk through enhanced monitoring

Answer: B

NEW QUESTION 96
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. Lack of sufficient computing resources for the AI system
B. Excessive reliance on external consultants for model design
C. Absence of metrics and dashboards for analysts
D. Insufficient model validation and change control processes

Answer: D

NEW QUESTION 99
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 102
An organization is commissioning a third-party AI system using sensitive data. Which metric is MOST important to consider?

A. Accessibility rating
B. Model response time
C. Accuracy thresholds
D. Service availability

Answer: C

NEW QUESTION 106
Which of the following is the MOST effective defense against cyberattacks that alter input data to avoid detection by the model?

A. Conducting periodic monitoring activities on the model??s decisions
B. Enhancing model robustness through adversarial training
C. Implementing restricted access to the model??s internal parameters
D. Applying differential privacy controls on training datasets

Answer: B

NEW QUESTION 111
When implementing a generative AI system, which of the following approaches will BEST prevent misalignment between the corporate risk appetite and tolerance?

A. Ensuring effective AI key performance indicators (KPIs)
B. Performing an AI impact assessment
C. Creating and maintaining an AI risk register
D. Establishing and monitoring acceptable levels of AI system risk

Answer: D

NEW QUESTION 114
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 119
Which phase of the AI data life cycle presents the GREATEST inherent risk?

A. Monitoring
B. Maintenance
C. Preparation
D. Training

Answer: D

NEW QUESTION 124
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 127
A global organization has experienced multiple incidents of staff copying confidential data into public chatbots and acting on the model outputs. Which of the following is MOST important to reduce short-term risk when launching an AI security awareness initiative?

A. Blocking access to public large language models (LLMs) at the network perimeter
B. Requiring employees to complete an annual generic phishing and deepfake awareness module
C. Delivering role-based and scenario-driven AI security training mapped to policy and job functions
D. Publishing an AI acceptable use policy and collecting e-signatures of employees

Answer: C

NEW QUESTION 130
A programmer suspects an AI system is inferring sensitive user information. What is the BEST action?

A. Inform the governance panel
B. Suggest fine-tuning
C. Conduct a code review
D. Alert the CIO

Answer: A

NEW QUESTION 135
Which of the following BEST strengthens information security controls around the use of generative AI applications?

A. Ensuring controls exceed industry benchmarks
B. Monitoring AI outputs against policy
C. Implementing a kill switch
D. Validating AI model training data

Answer: B

NEW QUESTION 136
An organization has implemented a natural language processing model to respond to customer questions when personnel are not available. A pre-implementation security assessment revealed attackers could access sensitive company data through a chat interface injection attack. Which of the following is the BEST way to prevent this attack?

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

Answer: C

NEW QUESTION 140
A financial organization is concerned about the risk of prompt injection attacks on its customer service chatbot. Which of the following controls BEST addresses this concern?

A. Human-in-the-loop

B. Input validation
C. Increasing model parameters
D. Continuous monitoring

Answer: B

NEW QUESTION 141
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 146
After deployment, an AI model??s output begins to drift outside of the expected range. Which of the following is the development team??s BEST course of action?

A. Take the AI model offline
B. Adjust the hyperparameters of the AI model
C. Create an emergency change request to correct the issue
D. Return to an earlier phase in the AI life cycle

Answer: D

NEW QUESTION 148
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 151
A viral video shows a blurry person making claims about a product safety issue. The video has random low-quality sections. This MOST likely represents what threat?

A. Hallucinations
B. Model drift
C. Data poisoning
D. Deepfake

Answer: D

NEW QUESTION 155
The PRIMARY purpose of adopting and implementing AI architecture as part of an organizational AI program is to:

A. ensure the development of powerful, efficient, and scalable AI systems
B. deploy fast and cost-efficient AI systems for rapidly changing environments
C. align the system components of AI with the business goals of the organization
D. provide a basis for identification of threats and vulnerabilities

Answer: C

NEW QUESTION 158
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 161
An organization plans to leverage AI in the software development process to speed up coding. Which of the following should the information security manager do FIRST?

A. Conduct an impact assessment
B. Train developers to verify AI output
C. Update the security policy to include AI controls

D. Perform a cost-benefit analysis

Answer: A

NEW QUESTION 166
Which of the following is the GREATEST concern when a vendor enables generative AI features for an organization's critical system?

A. Access to the model
B. Proposed regulatory enhancements
C. Security monitoring and alerting
D. Bias and ethical practices

Answer: A

NEW QUESTION 169
Which of the following is the MOST critical key risk indicator (KRI) for an AI system?

A. The accuracy rate of the model
B. The amount of data in the model
C. The response time of the model
D. The rate of drift in the model

Answer: D

NEW QUESTION 171
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 tolerance
B. Risk threshold
C. Risk register
D. Risk appetite

Answer: D

NEW QUESTION 175
Which of the following information is MOST important to include in a centralized AI inventory?

A. Ownership and accountability of AI systems
B. AI model use cases
C. Training data sets
D. Foundation model and package registry

Answer: A

NEW QUESTION 176
Secure aggregation enhances the security of federated learning systems by:

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

Answer: D

NEW QUESTION 179
When robust input controls cannot prevent prompt injections in an LLM, what is the BEST compensating control?

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

Answer: D

NEW QUESTION 183
Which of the following will BEST reduce data bias in machine learning (ML) algorithms?

A. Adopting a more simplified model
B. Utilizing unstructured data sets
C. Diversifying the model training data
D. Securing the model training data

Answer: C

NEW QUESTION 185
Which strategy BEST ensures generative AI tools do not expose company data?

A. Conducting an independent AI data audit
B. Implementing a solution prohibiting input of sensitive data
C. Testing AI tools before implementation
D. Ensuring AI tools comply with local regulations

Answer: B

NEW QUESTION 187
Which of the following AI system vulnerabilities is MOST easily exploited by adversaries?

A. Inaccurate generalizations from new data by the AI model
B. Weak controls for access to the AI model
C. Lack of protection against denial of service (DoS) attacks
D. Inability to detect input modifications causing inappropriate AI outputs

Answer: B

NEW QUESTION 189
Which of the following approaches BEST enables the separation of sensitive and shareable data to prevent an AI chatbot from inadvertently disclosing confidential information?

A. Zero Trust
B. Sandboxing
C. Siloing
D. Containerization

Answer: C

NEW QUESTION 194
Which of the following BEST describes the role of model cards in AI solutions?

A. They are primarily used to visualize the performance of AI models
B. They are used to automatically fine-tune AI models by adjusting hyperparameters based on user feedback
C. They provide a standardized way to document the training data and AI model use cases
D. They help developers create synthetic data and train AI models

Answer: C

NEW QUESTION 199
An organization is implementing an AI-based credit assessment engine using internal and third-party customer data. Which of the following BEST aligns with data management controls for the AI life cycle?

A. Documented procedures for data sourcing, lineage tracking, and quality validation
B. Use of hashed identifiers to anonymize datasets used for model validation and internal analytics
C. Encrypted isolation and dynamic access controls on training data pipelines
D. Limitation of model training to structured data from vetted sources to minimize ingestion risk

Answer: A

NEW QUESTION 201
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 202
An organization plans to implement a new AI system. Which of the following is the MOST important factor in determining the level of risk monitoring activities required?

A. The organization??s risk appetite
B. The organization??s number of AI system users
C. The organization??s risk tolerance
D. The organization??s compensating controls

Answer: C

NEW QUESTION 207
What is the GREATEST benefit of performing AI security risk assessments?

A. Updating the risk register
B. Implementing privacy controls
C. Enabling risk prioritization
D. Securing appropriate funding

Answer: C

NEW QUESTION 209
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 212
Which of the following strategies BEST ensures generative AI tools do not expose company data?

A. Conducting an independent AI data audit
B. Testing AI tools before implementation
C. Implementing a solution to prohibit the input of sensitive data
D. Ensuring AI tools are compliant with local regulations

Answer: C

NEW QUESTION 216
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 221
Which of the following would MOST effectively ensure an organization developing AI systems has comprehensive data classification and inventory management?

A. Creating a centralized team to oversee the classification of data used in AI projects
B. Conducting quarterly audits of AI data sets for anomalies and missing metadata
C. Establishing a manual process to categorize data based on business needs and regulatory compliance
D. Implementing an automated data cataloging tool that integrates with all organizational data repositories

Answer: D

NEW QUESTION 223
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. Reverse-engineering the model using social engineering
D. Conducting denial-of-service attacks on AI APIs

Answer: B

NEW QUESTION 228
Implementing which of the following would MOST effectively address bias in generative AI models?

A. Data augmentation
B. Data minimization
C. Adversarial training
D. Fairness constraints

Answer: D

NEW QUESTION 232
What is the GREATEST concern when a vendor enables generative AI features for an organization??s critical system?

A. Security monitoring and alerting
B. Bias and ethical practices
C. Proposed regulatory enhancements
D. Access to the model

Answer: D

NEW QUESTION 235
A critical AI system shows biased outcomes. What is the BEST course of action?

A. Activate the kill switch
B. Conduct audits of data and model
C. Perform root cause analysis to identify mitigation
D. Retrain the model with a new diverse dataset

Answer: C

NEW QUESTION 239
AI developers often find it difficult to explain the processes inside deep learning systems PRIMARILY because:

A. Training data input for learning is spread throughout the public domain and continues to change
B. Generated knowledge dynamically changes in memory without being tracked by change history logs
C. Applied algorithms are based on probability theories to improve system performance
D. Neural network architectures can include statistical methods that are not fully understood

Answer: D

NEW QUESTION 242
Which of the following is the MOST critical success factor for an AI implementation project?

A. Developing and using model cards
B. Ensuring AI risk is captured in the risk register
C. Mapping data throughout the life cycle
D. Obtaining senior management buy-in

Answer: D

NEW QUESTION 246
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 248
Embedding unique identifiers into AI models would BEST help with:

A. Preventing unauthorized access
B. Tracking ownership
C. Eliminating AI system biases
D. Detecting adversarial attacks

Answer: B

NEW QUESTION 251
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 253
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 258
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AAISM Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AAISM Product From:

https://www.2passeasy.com/dumps/AAISM/

Money Back Guarantee

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