Isaca AAISM Practice Questions

Shared by Aguilar on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A large financial services organization is integrating a third-party AI solution into its critical fraud detection system. Which of the following is the BEST way for the organization to reduce risk associated with AI vendor and supply chain dependencies?

Options:

A- Conducting annual vulnerability assessments of the fraud detection system after integration
B- Focusing on performance testing to ensure the solution meets operational requirements
C- Establishing contractual agreements requiring vendors to provide evidence of secure development practices
D- Implementing isolated virtual environments to validate the integration of the fraud detection system with the solution

Answer:

C

Explanation:

AAISM emphasizes supplier assurance through contractual obligations as the foundational control for AI supply chain risk. Contracts should require verifiable evidence of secure development practices (e.g., secure SDLC, model and data provenance documentation, SBOM/MBOM where applicable, vulnerability disclosure, patch SLAs, audit rights, incident notification, and regulatory compliance assertions). This creates enforceable, continuous assurance beyond point-in-time tests.

* A is necessary but reactive and limited to your environment.

* B addresses performance, not supply chain security.

* D is a good isolation/validation practice but does not create vendor accountability across the lifecycle.

Question 2

Question Type: MultipleChoice

Which option best is the MOST important factor to consider when selecting industry

frameworks to align organizational AI governance with business objectives?

Options:

A- Risk tolerance
B- Risk threshold
C- Risk register
D- Risk appetite

Answer:

D

Explanation:

According to AAISM governance principles, the risk appetite of the organization is the most important factor in selecting appropriate frameworks for AI governance. Risk appetite defines the level of risk an organization is willing to accept in pursuit of its objectives, ensuring frameworks are aligned with strategic goals. Risk tolerance and thresholds are operational measures derived from appetite, and the risk register is a documentation tool. The foundational consideration for framework alignment is the organization's risk appetite.

AAISM Exam Content Outline -- AI Governance and Program Management (Risk Appetite in Governance Alignment)

AI Security Management Study Guide -- Framework Selection and Business Strategy

Question 3

Question Type: MultipleChoice

An organization implementing an LLM application sees unexpected cost increases due to excessive computational resource usage. Which vulnerability is MOST likely in need of mitigation?

Options:

A- Excessive agency
B- Sensitive information disclosure
C- Unbounded consumption

D- System prompt leakage

Answer:

C

Explanation:

AAISM categorizes unbounded consumption (also known as ''resource exhaustion'' or ''infinite queries'') as an AI-specific vulnerability where attackers (or faulty prompts) trigger excessive computation, leading to high costs and degraded service.

This aligns precisely with unexpected large compute bills.

Excessive agency (A) refers to unsafe autonomy, while disclosure (B) and prompt leakage (D) do not relate to compute overuse.

==========

Question 4

Question Type: MultipleChoice

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

Options:

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

Explanation:

AAISM emphasizes that data governance over the full AI life cycle is foundational. The official content describes effective AI data management as including documented procedures for: (1) how data is sourced, (2) how lineage is tracked from origin to model, and (3) how data quality is validated and monitored. This ensures transparency, accountability, and auditability, which are especially critical in regulated areas like credit assessments. While hashing identifiers (B) and encryption/access controls (C) are important privacy and security mechanisms, they are partial controls within a broader governance framework and do not, on their own, establish end-to-end life-cycle management. Limiting training to structured data (D) is a design choice and may reduce risk but is neither sufficient nor required as a best practice. Option A directly reflects AAISM's prescribed governance controls for AI data throughout its life cycle.

==========

Question 5

Question Type: MultipleChoice

In a new supply chain management system, AI models used by participating parties are interactively connected to generate advice in support of management decision making. Which of the following is the GREATEST challenge related to this architecture?

Options:

A- Establishing clear lines of responsibility for AI model outputs
B- Identifying hallucinations returned by AI models
C- Determining the aggregate risk of the system
D- Explaining the overall benefit of the system to stakeholders

Answer:

A

Explanation:

The AAISM governance framework notes that in multi-party AI ecosystems, the greatest challenge is ensuring clear accountability for AI outputs. When models from different parties interact, responsibility for errors, bias, or harmful recommendations can be unclear, leading to disputes and compliance gaps. While aggregate risk assessment and error identification are significant, they are secondary to the fundamental governance requirement of establishing transparent lines of responsibility. Without defined accountability, no stakeholder can reliably manage or mitigate risks. Therefore, the greatest challenge in such a distributed architecture is responsibility for AI outputs.

AAISM Study Guide -- AI Governance and Program Management (Accountability in Multi-Party Systems)

ISACA AI Governance Guidance -- Roles and Responsibilities in AI Collaboration

Question 6

Question Type: MultipleChoice

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

Options:

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

Explanation:

AAISM prescribes risk-based, human-in-the-loop orchestration for safety-critical or regulated actions. A tiered automation strategy that gates autonomy by incident severity, data sensitivity, and regulatory requirements ensures accountability, auditability, and proportionality, satisfying governance obligations. Full autonomy (A) risks non-compliance; simply mirroring legacy workflows (B) may not meet current obligations; broad auto-containment (C) lacks necessary oversight controls.

==========

Question 7

Question Type: MultipleChoice

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?

Options:

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

Explanation:

AAISM governance practices state that before categorizing technologies by risk, the first step is to ensure that all AI systems are documented in the organizational asset inventory. A complete inventory provides the foundation for subsequent risk analysis, accountability, and governance. Grouping solutions, identifying vulnerabilities, and assessing risk levels come afterward, once inventory accuracy is established. Without confirming that the technologies are recorded in the inventory, risk categorization may miss critical assets.

AAISM Study Guide -- AI Governance and Program Management (AI Inventories as a Prerequisite to Risk Analysis)

ISACA AI Security Management -- Asset Visibility and Risk Categorization