

PRACTICE QUESTIONS

ISACA

Advanced in AI Security Management

SHARED BY [u/Jolly-Badger-4194](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM ISACA Advanced in AI Security Management

Shared by [u/Jolly-Badger-4194](#) on aiexamcerts

10 practice questions for the ISACA Advanced in AI Security Management exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/isaca/advanced-in-ai-security-management. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. Which role is best placed to own the security requirements for an organization's AI systems across their lifecycle?
 - A The data labeling contractor who prepares the training sets and checks annotation quality each week
 - B The individual data scientist who trains each model
 - C An AI security manager or AI risk owner with authority over design and deployment approvals
 - D The marketing lead responsible for product announcements

Answer: C

A named AI security manager or risk owner with approval authority can apply requirements from design through retirement. The data scientist who trains a model is the tempting choice because that person knows the system best, but individual builders cannot independently accept risk. Labeling contractors and marketing leads have no authority over security requirements.

2. Shadow AI, meaning unsanctioned AI tools used by staff, can expose confidential data outside the organization's control.
 - A True
 - B False

Answer: A (True)

When staff paste data into unsanctioned AI services, the data may be retained, used for training or exposed to parties outside the organization's controls. Governance therefore has to detect and address shadow AI. The statement is true, and discouraging it through policy alone is rarely enough.

3. What is the main purpose of a threat model for an AI system?
 - A To estimate the number of servers and GPUs required for the training cluster, including its backup and disaster recovery capacity
 - B To list the names of all employees who use the system
 - C To identify how attackers could reach and manipulate the system, and which controls mitigate those paths
 - D To compare the system's accuracy against a competitor's tool

Answer: C

A threat model maps attacker goals, entry points and abuse paths, and it links each path to mitigating controls. Server counts are a tempting planning concern, but they are not threat analysis. Staff lists and accuracy comparisons do not reveal how the system can be attacked.

4. The risk that remains after controls have been applied is called _____ risk.

Answer: residual

Residual risk is the exposure left after existing controls are applied, and it is the amount that management must accept or further reduce. Inherent risk is a tempting answer because it is the starting exposure before controls, but it is not what remains. Residual risk is the figure used for acceptance decisions.

5. Which two activities belong in a secure AI model development lifecycle? (Choose two.)

- A Threat modeling at design time before significant development begins
- B Skipping design reviews to reach the market sooner
- C Publishing the training pipeline credentials in the team wiki
- D Adversarial robustness testing before each production release
- E Retiring test suites once the first release is complete

Answer: A, D

Threat modeling at design time and adversarial robustness testing before release both build security into the lifecycle rather than adding it at the end. Skipping design reviews is a tempting way to save time, but it leaves design flaws to be found later. Publishing credentials and retiring test suites both weaken security.

6. Which network control best limits the exposure of an internal AI inference service?

- A Private network connectivity with access restricted to approved application identities
- B A public IP address with no authentication for easier testing
- C Open inbound access from all networks during development
- D A shared guest network used by visitors, contractors and staff for general internet access and testing

Answer: A

Restricting the service to private connectivity and approved identities limits who can call it and reduces the attack surface. A public endpoint with no authentication is a tempting shortcut for testing, but it exposes the model to anyone. Open development access and guest networks have the same flaw.

7. Which logging practice best supports investigation of AI system misuse?
- A Logging only the total number of requests per day
 - B Recording prompts, outputs, tool calls and identities in a protected log store with retention rules
 - C Deleting logs after each session to protect storage space, reduce retention cost and simplify routine audit tasks
 - D Writing logs to the same disk the model reads from

Answer: B

Capturing prompts, outputs, tool calls and identities in a protected store with retention rules gives investigators the evidence they need. Request counts are a tempting metric, but they omit what was asked and done. Deleting logs per session and storing them beside model files undermine both retention and integrity.

8. Retraining a model on newly collected production data does not require a security review, because the model architecture has not changed.
- A True
 - B False

Answer: B (False)

Retraining changes the model's learned behavior and the data it depends on, which can introduce new risks such as poisoning or privacy leakage. Architecture stability does not guarantee security stability. The statement is false.

9. What does a post-incident review primarily produce?
- A A ranking of the engineers involved in the incident
 - B A marketing summary highlighting the product's strengths and its newest customer features
 - C A decision to remove the incident from the risk register
 - D Corrective actions with owners and deadlines, plus updates to controls and procedures

Answer: D

A post-incident review produces assigned corrective actions and updates to controls and procedures so the same failure is less likely. Ranking engineers is a tempting blame-oriented output, but it discourages reporting and does not fix causes. Marketing summaries and register removal avoid the learning the review should produce.

10. Which resilience measure best protects an AI system's availability during a vendor outage?
- A A tested failover to an alternative model or provider with defined performance limits
 - B Relying on the vendor's status page as the only monitoring
 - C Subscribing to a single provider with no contingency plan
 - D Waiting for the outage to end before reviewing the architecture and the service targets

Answer: A

A tested failover to an alternative model or provider with defined limits keeps the service running within acceptable quality. Watching the vendor status page is a tempting monitoring approach, but it only reports the outage. A single provider with no contingency plan and waiting for recovery add no resilience.