

PRACTICE QUESTIONS

ISACA

Advanced in AI Security Management

SHARED BY [u/Crisp-Moose-2490](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM ISACA Advanced in AI Security Management

Shared by [u/Crisp-Moose-2490](#) 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 AI security metric best shows that governance is working across the organization?
 - A The total number of AI pilots launched this year across all business units and product lines
 - B The percentage of AI systems with a completed security assessment and a named owner
 - C The average inference latency across all AI endpoints
 - D The volume of training data stored in the data lake

Answer: B

The share of AI systems with a completed security assessment and a named owner shows that controls reach the whole estate. Pilot counts are a tempting activity measure, but they show ambition rather than control. Latency and storage volume describe performance and capacity, not governance.

2. The AI security function that defines how AI risk is assessed, accepted and reported to the board is called AI _____.

Answer: governance

AI governance defines accountability, policies and oversight for AI security and risk. Model management is a tempting label because models are central to the activity, but it covers operational lifecycle tasks. Governance is the layer that sets authority for those tasks.

3. Which risk treatment option is appropriate when an AI use case's residual risk exceeds the organization's appetite?
 - A Accept the residual risk because the vendor has a strong reputation in its market
 - B Reduce the risk further with additional controls, or stop the use case
 - C Ignore the residual risk because it was calculated before launch
 - D Transfer every risk to the end users through the terms of service

Answer: B

When residual risk is above appetite, the organization must reduce it with more controls or stop the use case. Accepting risk because a vendor is reputable is a tempting shortcut, but reputation does not reduce the organization's exposure. Ignoring residual risk or transferring it to users is not a valid treatment.

4. An AI risk register should record the affected business process, data classification and risk owner for each entry.
- A True
 - B False

Answer: A (True)

A useful AI risk entry links the risk to the business process it affects, the sensitivity of the data involved and a named owner to drive treatment. Without these, the register cannot support prioritization or accountability. The statement is true.

5. Which two measures help secure an AI model supply chain? (Choose two.)
- A Downloading pretrained weights from unknown mirrors for speed
 - B Verifying the checksums and provenance of pretrained model files
 - C Disabling dependency scanning to reduce build times
 - D Accepting unsigned packages when a deadline is close
 - E Maintaining a software bill of materials that lists model dependencies

Answer: B, E

Checksum and provenance verification confirm that a pretrained file is genuine, and a software bill of materials lists dependencies for tracking vulnerabilities. Unknown mirrors are a tempting shortcut for speed, but they expose the pipeline to tampered weights. Disabling scanning and accepting unsigned packages both remove safeguards.

6. What is the main security concern with storing secrets such as API keys inside prompts or training data?
- A They increase the model's accuracy on coding tasks
 - B They reduce the amount of memory the model requires during inference and batch processing
 - C They make the model's output formatting more consistent
 - D They can be exposed through model outputs, logs or later retrieval

Answer: D

Secrets placed in prompts, logs or training data can leak through outputs or be retrieved later by users or attackers. A small accuracy gain is a tempting but irrelevant effect, since secrets do not improve quality. Memory use and output formatting are unrelated to the exposure.

7. Which step best protects against a model being deployed with an unvetted dependency?
- A Installing the newest version of every library automatically as soon as each release appears
 - B Allowing developers to add packages from any source
 - C Skipping the dependency manifest for faster builds
 - D Scanning dependencies and rejecting components that fail vulnerability or license checks

Answer: D

Scanning dependencies and rejecting failing components stops known-vulnerable or non-compliant packages from reaching production. Automatic upgrades to the newest version are a tempting way to stay current, but newest does not mean vetted. Unrestricted sources and skipped manifests remove visibility and control.

8. Before a model is released, security _____ checks the model and its surrounding system against defined attack and misuse cases.

Answer: testing

Security testing exercises the model and its surrounding system against defined attack and misuse cases before release. Code review is a tempting pre-release activity, but it examines source rather than behavior under attack. Security testing is the step that tests the system as an attacker would.

9. Which metric best reflects the resilience of an AI service to failure?
- A The number of AI features listed on the product page
 - B Mean time to detect and recover from degraded AI behavior, measured against defined service targets
 - C The average length of each user's conversation history
 - D The total number of prompt templates stored in the repository for all teams, projects and environments in use

Answer: B

Time to detect and recover from degraded behavior, measured against targets, shows how well the service absorbs failures. Feature counts are a tempting product measure, but they do not show resilience. Conversation length and template counts describe usage and content, not recovery.

10. Which practice improves the resilience of AI-dependent business processes?

- A** Making the model the only option for every business process
- B** Removing human staff from processes that depend on AI
- C** Defining manual fallback procedures and tested rollback options for when the model is unavailable
- D** Scheduling AI outages during peak business hours to test readiness and measure the impact on customer demand

Answer: C

Manual fallbacks and tested rollback options keep essential processes running when the model is unavailable or untrusted. Making AI the only option is a tempting efficiency choice, but it removes the safety net. Removing staff and testing during peak hours both increase disruption.