

PRACTICE QUESTIONS

ISACA

Advanced in AI Risk

SHARED BY [u/Upbeat-Otter-5400](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	ISACA Advanced in AI Risk

Shared by u/Upbeat-Otter-5400 on aiexamcerts

10 practice questions for the ISACA Advanced in AI Risk 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-risk. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. A chief risk officer wants AI risk reported on the same scale as every other enterprise risk. Which approach best achieves that?
 - A Create a separate AI-only rating scale with its own color codes
 - B Exclude AI from enterprise risk reporting until models are in production for a full year
 - C Map AI risks to the existing enterprise risk taxonomy and rating criteria
 - D Report only model accuracy scores to the board each quarter

Answer: C

Mapping AI risks onto the existing enterprise taxonomy and rating criteria lets the board compare AI exposure with other risks and apply the same escalation rules. A separate AI-only scale is the tempting option because it looks tailored, but it cannot be compared with other risks and fragments reporting. Reporting only model accuracy ignores security, legal and ethical exposure.

2. Shadow AI, meaning unsanctioned use of AI tools by employees, is only a security concern and not a governance or risk concern.
 - A True
 - B False

Answer: B (False)

Shadow AI creates governance risk because data may leave approved boundaries, decisions may rely on unvalidated outputs, and accountability for those decisions is unclear. Security is one dimension, but privacy, legal and quality risks are equally relevant. The statement is false because it narrows a governance issue to a single risk category.

3. Which assessment is most suitable for identifying harm to individuals from an AI system that influences housing eligibility decisions?
 - A A code coverage review of the inference service and its unit tests
 - B A load test of the prediction endpoint under peak traffic
 - C A fundamental rights or algorithmic impact assessment covering affected groups
 - D A comparison of vendor license prices across several competing AI providers

Answer: C

A fundamental rights or algorithmic impact assessment examines how the system affects individuals and groups, including discrimination and access to essential services. A load test is a tempting technical check, but it measures capacity rather than harm. Code coverage and license price comparisons do not identify impacts on people.

4. The principle that an AI system should provide understandable reasons for its outputs to users and auditors is called _____.

Answer: explainability (also accepted: explainable AI)

Explainability is the ability to give understandable reasons for a model's outputs, which supports user trust, contestation and audit. Accuracy is the tempting answer because it is the metric most often reported, but accuracy does not explain how a result was reached. Explainability addresses the reasoning that accuracy leaves hidden.

5. Which two metrics help detect model degradation in production? (Choose two.)

- A A rising error rate on recently labeled production samples
- B Stable accuracy measured only on the original training set
- C A shift in the distribution of input features
- D The monthly cloud storage bill
- E The count of employees assigned to the project

Answer: A, C

A rising error rate on recent labeled samples and a shift in input feature distributions both reveal that the model is drifting away from its validated behavior. Stable accuracy on the training set is a tempting reassurance, but it cannot reveal production degradation. The storage bill and staff counts have no bearing on model quality.

6. Which control best limits the damage an LLM-based agent could cause if it were manipulated into misusing its tools?

- A Unlimited API keys shared across all agents
- B A shared administrator account used by the agent for all of its tool actions and integrations
- C Least-privilege tool permissions with human approval for high-impact actions
- D Hard-coded passwords stored inside the prompt

Answer: C

Granting only the tool permissions an agent needs, and requiring human approval for high-impact actions, limits what a manipulated agent can do. Broad credentials are a tempting convenience because they reduce friction, but they multiply the damage a manipulation can cause. Hard-coded passwords and shared administrator accounts make abuse easier and harder to trace.

7. Which access control principle should govern the stores that hold model training data?
- A Open read access for all analysts in the company to speed up experimentation
 - B A shared service account used by every team
 - C Public read access with logging turned on
 - D Role-based access with approval workflows and audit logging

Answer: D

Role-based access with approval workflows and audit logs grants each user only what their role needs and records who accessed what. Open access for all analysts is a tempting way to speed up experimentation, but it removes the need-to-know boundary. A shared service account and public access both destroy accountability for data use.

8. An AI risk dashboard should show only metrics that are favorable to the business, so that executives are not alarmed.
- A True
 - B False

Answer: B (False)

A risk dashboard exists to show the exposures leadership needs to see, including unfavorable trends and breached thresholds. Showing only favorable metrics hides the signals that drive decisions and undermines governance. The statement is false.

9. Which practice best manages risk across an AI model supply chain?
- A Using the latest unvetted open-source model weights without any review or testing
 - B Maintaining an inventory of model components, versions and their provenance
 - C Keeping all components in one private folder with no versioning
 - D Ignoring dependency updates to keep the system stable

Answer: B

An inventory of components, versions and provenance shows what the system is built from and where each part came from, which is essential when a component is found to be flawed. Adopting the newest open-source weights is a tempting way to improve quality, but it skips vetting. Unversioned storage and ignored updates both remove the visibility that supply chain management needs.

10. Which contract clause best supports incident response with an AI vendor?
- A A right for the vendor to delay notifications indefinitely
 - B A requirement that the customer pays for all incident investigation costs and legal fees
 - C A defined timeline for breach or model defect notification and cooperation duties
 - D No clause, because the vendor is trusted

Answer: C

A defined notification timeline and cooperation duties let the customer respond quickly and share the evidence needed to contain an AI incident. A vague clause that lets the vendor delay is the tempting but harmful option. Making the customer pay for investigation or omitting the clause entirely leaves the customer without support when it matters.