

PRACTICE QUESTIONS

ISACA

Advanced in AI Governance

SHARED BY [u/Dapper-Sparrow-3572](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 18, 2026

EXAM ISACA Advanced in AI Governance

Shared by [u/Dapper-Sparrow-3572](#) on aiexamcerts

10 practice questions for the ISACA Advanced in AI Governance exam, each followed by its answer and a short explanation. More free sets and the full practice exam: aiexamcerts.com/isaca/advanced-in-ai-governance. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. In the three lines of defense model, management control is the first line, risk oversight is the second, and independent _____ is the third.

Answer: assurance (also accepted: internal audit)

The third line provides independent assurance, and in most organizations that role sits with internal audit reporting to the audit committee. The first line owns and runs controls, while the second line sets risk policy and challenges them. Management self-review is not independent, so it cannot fill the third line.

2. A risk register lists model bias in loan approvals as a high risk. Which action best supports effective risk oversight?
 - A Close the entry once the model is deployed
 - B Move the risk to the marketing team's register
 - C Accept the risk silently because the model passed its launch review and no complaints were logged
 - D Assign a risk owner, set bias metrics and thresholds, report on a cycle

Answer: D

A named owner, measurable bias metrics with thresholds, and regular reporting to the risk committee turn a register entry into managed oversight. Closing the entry at deployment ignores that bias can emerge later in production. Moving the risk to an unrelated team removes the accountable owner rather than managing the risk.

3. Which role is best placed to independently verify that an AI governance program is operating as designed?
 - A The model developer who built the system
 - B The internal audit function, reporting to the audit committee
 - C The product manager who owns the revenue target for the customer analytics product line
 - D The vendor's sales engineer

Answer: B

Internal audit is independent of the management that runs the AI program and reports to the audit committee, so it can test whether controls operate. The model developer is part of the management being checked, which makes self-verification a conflict. A vendor's sales engineer has a commercial interest in the result, so that role cannot provide independent assurance.

4. Which two properties matter most when choosing storage for AI training data that must be auditable? (Choose two.)
- A Immutable or versioned records of the exact dataset used for each model release
 - B The fastest possible write speed, regardless of access logging
 - C Unrestricted read access so every data scientist can copy files freely
 - D Retention of access and change logs for the datasets
 - E Automatic deletion of all raw data after its first use

Answer: A, D

Versioned or immutable dataset records let an auditor see exactly what trained each release, and retained access and change logs show who touched that data. Write speed and open access do not make data auditable, and unrestricted copying weakens control. Deleting raw data after first use removes the evidence an audit would need to re-check the training inputs.

5. Human reviewers of a high-impact AI system approve nearly every flagged case within seconds. What is the most important governance concern?
- A The reviewers are using too few GPUs for their workload, so the review queue builds up at peak times
 - B Oversight has become nominal, so the human review may not be meaningful
 - C The system is too accurate to need any human review
 - D The approval log contains too much detail

Answer: B

When reviewers approve in seconds, the human oversight required for the decision exists on paper only, which undermines accountability. GPU capacity is not the governance issue, and accuracy never removes the need for oversight on high-impact decisions. Detailed approval logs support review, so they are not a concern in themselves.

6. Board reporting on AI risk is most useful when it summarizes trends in incidents, control failures and risk appetite breaches, not only the number of AI projects.
- A True
 - B False

Answer: A (True)

True. Trends in incidents, control failures and appetite breaches show whether risk is rising or being contained, which is what directors need to oversee. A count of projects reveals activity but says nothing about exposure.

7. A company plans to use an AI vendor that processes employee performance data outside the country where staff work. Which step should come first in the risk assessment?
- A Sign the contract and review the data flows afterwards
 - B Negotiate a lower price before reviewing the privacy terms
 - C Assume the vendor's security certification covers all transfer and privacy obligations
 - D Map data flows, legal basis and transfer mechanism before approval

Answer: D

Mapping data flows, the legal basis and any cross-border transfer mechanism determines whether the vendor can be used at all, so it must come before approval. Signing first and reviewing later reverses that order and creates exposure. A security certification does not by itself establish that cross-border transfers or the organization's own legal obligations are satisfied.

8. Under the NIST AI Risk Management Framework, the function that establishes policies, roles and a risk-aware culture across the organization is named _____.

Answer: GOVERN

GOVERN is the cross-cutting NIST AI RMF function that sets policies, accountability structures and culture for AI risk. The other functions, MAP, MEASURE and MANAGE, deal with context and risk identification, assessment, and treatment. Mixing GOVERN up with MANAGE is a common error, since MANAGE covers responding to risks rather than setting the structure around them.

9. Which design principle best supports reusing a feature across several AI models without rebuilding it each time?
- A A governed feature store with definitions, owners and version history
 - B Copying features into each team's personal notebook
 - C Storing feature definitions only as screenshots in the project wiki, reviewed at each release
 - D Hard-coding feature values into each consuming application

Answer: A

A governed feature store with definitions, owners and versions allows consistent reuse, and it shows which model depends on which feature version. Personal notebook copies drift apart over time and fail when a source changes. Screenshots and hard-coded values cannot be validated, versioned or reused safely.

10. Which practice best supports incident response when a production AI system produces harmful outputs?
- A Wait for the next quarterly model review before acting
 - B Delete the logs so the incident cannot be reproduced
 - C Severity levels, a rollback procedure and a root-cause post-incident review
 - D Ask the vendor to decide alone without informing the business owner or the risk committee

Answer: C

Predefined severity levels and a rollback or disable procedure let the organization contain harm quickly, and a post-incident review finds the root cause so it is not repeated. Waiting for a quarterly review leaves harmful outputs live for months. Deleting logs destroys the evidence needed for investigation and accountability.