

PRACTICE QUESTIONS

ISACA

Advanced in AI Audit

SHARED BY [u/Eager-Gecko-9377](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM ISACA Advanced in AI Audit

Shared by [u/Eager-Gecko-9377](#) on aiexamcerts

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

1. The NIST AI Risk Management Framework is organized around four core functions. Which set is correct?
- A Plan, Build, Test and Release
 - B Collect, Clean, Train and Deploy
 - C Govern, Map, Measure and Manage
 - D Identify, Protect, Detect and Respond

Answer: C

The NIST AI RMF 1.0 uses Govern, Map, Measure and Manage as its four core functions, with Govern cutting across the others. Plan, Build, Test and Release describes a software lifecycle rather than the framework. Collect, Clean, Train and Deploy describes a data pipeline. Identify, Protect, Detect and Respond belongs to the NIST Cybersecurity Framework, which is a related but different framework.

2. Internal audit should recommend specific AI model designs to developers, since audit is the most technical function in the organization.
- A True
 - B False

Answer: B (False)

Internal audit provides independent assurance and should not design or build the controls it audits. Its recommendations focus on risk, control gaps and evidence, while developers retain responsibility for design decisions. Blurring those roles weakens independence.

3. ISO/IEC 23894 provides guidance that is most closely related to which topic?
- A Cloud storage pricing for large datasets, including long-term discounts and cross-region transfer costs
 - B Keyboard layout standards for data entry
 - C Risk management for artificial intelligence
 - D Physical security of server rooms

Answer: C

ISO/IEC 23894 gives guidance on managing risks specific to AI, and it is designed to align with general risk management practice. Storage pricing, keyboard layouts and physical security are outside its scope. It is one of the standards an auditor might cite when assessing an AI risk process.

4. The degree of risk that an organization is willing to accept in pursuit of its objectives is called its risk _____.

Answer: appetite

Risk appetite is the broad amount of risk the organization is willing to pursue to meet its objectives, set by management and approved at the appropriate level. Risk tolerance is related but narrower, describing acceptable variation around specific objectives. The blank asks for the term for the accepted level of exposure.

5. Which TWO controls reduce risk for a generative AI application that uses retrieved documents? (Choose two.)

- A Trusting all retrieved documents because they are stored internally
- B Giving the model unrestricted access to every system so it can answer faster
- C Filtering retrieved content for sensitive data before it reaches the model
- D Sending every retrieved document to the model in full so it never has to decide which passage matters
- E Limiting the tools and actions the model can trigger without human approval

Answer: C, E

Retrieved text can carry injected instructions or sensitive data, so filtering it and limiting the actions the model can trigger reduce exposure. Trusting internal documents assumes they are safe, and unrestricted access to systems expands the impact of any manipulation. Those options are the tempting shortcuts that an auditor would flag.

6. Which artifact documents a model's intended use, performance limits and evaluation results for users and reviewers?

- A A firewall rule set
- B A payroll schedule
- C A marketing brochure for the product line
- D A model card

Answer: D

A model card records intended use, limitations, performance across relevant groups and evaluation conditions. Firewall rules, payroll schedules and marketing brochures do not document model behavior or limits. Auditors look for model cards as evidence of transparency and fitness for purpose.

7. Which practice gives the strongest evidence that a model version deployed to production is the one that was approved?
- A A model registry that links the approved version identifier to the deployed artifact and its evaluation record
 - B A file named final_model on a shared drive, since the team agreed the name on day one
 - C A verbal confirmation from the data scientist that the version is correct
 - D A screenshot of the deployment dashboard taken last month

Answer: A

A model registry links the approved version to the artifact and its evidence, which allows auditors to trace deployment to approval. A file named final is easily overwritten, and verbal confirmation is not evidence. An old screenshot does not prove what is running today.

8. Removing a sensitive attribute such as gender from a dataset is always sufficient to prevent unfair outcomes.
- A True
 - B False

Answer: B (False)

Other features can act as proxies that carry the same information, so removing the attribute alone does not remove bias. Fairness testing of outcomes is needed. Simply deleting a column is not a complete control.

9. Which metric is used to measure whether the values in a dataset are accurate and consistent with reality?
- A The number of columns in the dataset, since more fields carry more information and so are more accurate
 - B The file format of the dataset
 - C The color scheme of the data dashboard
 - D Data accuracy and consistency checks against authoritative sources

Answer: D

Data quality is judged by accuracy, completeness and consistency, which are checked against authoritative sources or defined rules. Column counts, file formats and dashboard colors do not show whether the values are correct. Auditors should not accept format as a proxy for quality.

10. Which control reduces the risk that a poisoned training dataset affects a production model?
- A Deleting all log files after each training run, so an attacker cannot reconstruct the training data
 - B Using the same dataset for every model version without review
 - C Provenance checks and integrity validation on training data before each training run
 - D Allowing any contributor to add records without verification

Answer: C

Poisoned records can be introduced through untrusted sources, so verifying provenance and validating integrity before training reduces that risk. Deleting logs removes evidence. Reusing data without review and accepting unverified contributions both increase exposure to poisoning.