

PRACTICE QUESTIONS

ISACA

Advanced in AI Audit

SHARED BY [u/stellarsummit1984](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM ISACA Advanced in AI Audit

Shared by [u/stellarsummit1984](#) 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. Which element of an AI governance framework most directly links organizational objectives to the AI systems that are built?
- A A list of programming languages approved for developers, with one required development environment
 - B An AI policy and inventory that record each system's purpose, owner and risk rating
 - C A quarterly newsletter about industry AI trends
 - D A standard template for slide decks used in steering meetings

Answer: B

An AI policy sets the rules for use, and an inventory records what systems exist, why they exist and who owns them. Together they tie business objectives to specific systems. A list of languages, a newsletter and a slide template are useful artifacts, but they do not create traceability between goals and deployed systems.

2. The standard that specifies requirements for an AI management system is ISO/IEC _____.

Answer: 42001

ISO/IEC 42001 is the AI management system standard that organizations can be certified against. It sits alongside ISO/IEC 23894, which gives guidance on AI risk management. The blank asks for the number of the management system standard.

3. Which technique is used to identify risks in an AI system by imagining how it could fail or be misused?
- A A load test that measures how many users can log in at once, since concurrency drives most AI risks
 - B Threat modeling or a structured risk workshop covering misuse and failure scenarios
 - C A code review that checks indentation and naming conventions
 - D A financial audit of the software license costs

Answer: B

Threat modeling and structured workshops explore how an AI system could be attacked, misused or fail, which is what risk identification requires. Load testing measures capacity rather than failure scenarios. Code style checks and license audits are useful controls but do not find AI-specific risks such as misuse or harmful output.

4. Risk ratings for AI systems should be reviewed when the data, the model or the use case changes materially.
- A True
 - B False

Answer: A (True)

Changes can alter both likelihood and impact, so a rating based on an older configuration may no longer hold. Reassessment at defined triggers keeps the risk picture accurate. This is a basic expectation of a risk-based approach.

5. Which TWO practices support data quality for an AI training pipeline? (Choose two.)
- A Deleting outliers without documenting the reason
 - B Defining validation rules for ranges, formats and required fields
 - C Replacing missing values with the most common value without recording it
 - D Assuming that a dataset is clean once it has loaded into the training environment without an error
 - E Monitoring completeness and freshness of the incoming data

Answer: B, E

Automated validation rules, completeness monitoring and reconciliation detect data problems at the point they enter the pipeline. Undocumented deletion of outliers and silent imputation both change the data without a trace. Auditors expect each transformation to be recorded and justified.

6. What is the main purpose of separating training, validation and test datasets?
- A To make the model train faster on the same records, since fewer training examples shorten each pass
 - B To estimate how well the model generalizes to data it has not seen during training
 - C To hide the test results from the business owner
 - D To store the datasets on different cloud regions

Answer: B

Keeping validation and test data separate from training gives an honest estimate of generalization and helps detect overfitting. Speed, secrecy and storage location are not the purpose of the split. An auditor checks that the split is documented and the test set is not used for tuning.

7. A team uses the test set repeatedly to choose hyperparameters. What is the audit concern?
- A The team is saving time by reusing the same data, which keeps the project within budget and on schedule
 - B The model will become more accurate on the test set automatically
 - C The test set is no longer independent, so the reported performance may be optimistic
 - D The test set is now too large to store efficiently

Answer: C

Using the test set to make decisions leaks information into the model selection, which inflates the reported result. Reusing data saves effort but compromises independence. Repeated use does not improve accuracy, and the storage size is not the concern.

8. A data quality dimension that describes whether all required values are present is called _____.

Answer: completeness

Completeness measures whether required fields and records are present, and missing values are a common cause of model bias and errors. Auditors test completeness against defined rules. The blank asks for the data quality dimension.

9. Which OWASP resource lists the most critical security risks for applications built on large language models?
- A OWASP Top 10 for Large Language Model Applications
 - B OWASP Top 10 for mobile banking apps only, since mobile banking is the only category needing a list
 - C The Payment Card Industry Data Security Standard
 - D The ISO 9001 quality management standard

Answer: A

The OWASP Top 10 for LLM applications lists risks such as prompt injection, sensitive information disclosure and insecure output handling. The mobile banking list and PCI DSS address other domains. ISO 9001 is a quality management standard, not a list of AI application risks.

10. Which attack tries to infer whether a specific record was part of a model's training data?

- A Denial of service through traffic flooding
- B Membership inference attack
- C Cross-site request forgery on a login form
- D SQL injection against a payroll database

Answer: B

A membership inference attack tests whether a record was in the training set, which can reveal sensitive information about individuals. Flooding traffic, forged web requests and database injection target different parts of the system. Auditors include this risk when training data is personal or confidential.