

PRACTICE QUESTIONS

CompTIA

CY0-001

CompTIA SecAI+

SHARED BY [u/snappylambda1980](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	CompTIA CY0-001, CompTIA SecAI+

Shared by u/snappylambda1980 on aiexamcerts

10 practice questions for the CompTIA CY0-001 exam, CompTIA SecAI+, each followed by its answer and a short explanation. More free sets and the full practice exam: www.aiexamcerts.com/comptia/cy0-001. Spotted a mistake? Email support@aiexamcerts.com with the exam code CY0-001 and the question number.

1. Under the EU AI Act, which risk tier applies to AI systems that are prohibited outright, such as social scoring by public authorities?

- A High risk
- B Limited risk, with transparency duties for chatbots and generated media
- C Unacceptable risk
- D Minimal risk

Answer: C

The Act bans AI practices that pose an unacceptable risk, including social scoring by public authorities and certain manipulative techniques. High risk is the tempting distractor, since those systems face strict obligations but remain permitted once they meet requirements. Limited risk carries transparency duties, and minimal risk systems face no specific obligations under the Act.

2. Strong overall accuracy on a model's test set is sufficient evidence that the model performs fairly for every user group.

- A True
- B False

Answer: B (False)

Overall accuracy can hide large gaps between groups, so fairness needs evaluation broken down by group and by relevant error types. The statement is false. The tempting assumption is that a single aggregate metric reflects every subgroup.

3. An attacker sends carefully modified images to an image classifier so that a stop sign is read as a speed limit sign, without changing the model. Which attack category is this?

- A Data poisoning during the training phase
- B Model inversion to reconstruct training faces
- C Evasion attack using adversarial examples
- D Membership inference against the training set

Answer: C

Modifying inputs at inference time to cause misclassification is an evasion attack, which uses adversarial examples. Data poisoning is the tempting distractor, since it also manipulates model behavior, but poisoning changes the training data rather than the input at inference. Model inversion and membership inference are privacy attacks that try to learn about the training data.

4. An adversarial example is an input with small, deliberate changes that cause a model to misclassify it, and this attack class is known as _____ attack.

Answer: evasion

Evasion attacks modify inputs at inference time so that a trained model produces the wrong output, often with changes that are hard for people to notice. Poisoning is the tempting distractor, since it also causes misclassification, but it works through the training data.

5. Which two practices protect an AI API key used by a deployed application? (Choose two.)

- A Store the key in a secrets manager and inject it at runtime with access limited to the service
- B Commit the key to the repository so every developer can run the application locally
- C Rotate the key on a schedule and immediately after any suspected exposure
- D Embed the key in the mobile app bundle so that it works offline for every user
- E Share one key across all environments, including development and production

Answer: A, C

A secrets manager with runtime injection and scheduled plus event-driven rotation keep the key out of code and limit how long an exposed key remains useful. Committing keys to the repository is the tempting distractor, since it makes local setup easy, but it places the secret in history where it is hard to remove. Embedding keys in client bundles and sharing them across environments both expose the credential or widen its use.

6. A company must prove that the model deployed to production is the same artifact that passed review. Which control provides the strongest assurance?

- A Renaming the model file to include the release date
- B Storing the model on a shared drive that everyone can edit
- C Cryptographically signing the model artifact and verifying the signature before deployment
- D Comparing only the file size and the creation date of the deployed and reviewed models before the release is approved

Answer: C

A cryptographic signature over the artifact, verified before deployment, proves the content has not changed since review. Renaming the file is the tempting distractor, since names are often used to track versions, but a name can be changed without changing the content. A shared editable drive and file size checks do not establish integrity.

7. Training data for a fraud model includes customer records with national identifiers that the model never uses. Which control best applies to the risk of this unnecessary data?
- A Encrypt the identifiers and keep them in the training set so that future features can use them without another review
 - B Copy the identifiers into the model's prompt for explainability
 - C Publish the identifiers in the model card for transparency
 - D Remove the identifiers during data preparation, since the model does not need them

Answer: D

Removing unused identifiers during preparation applies data minimization and shrinks the exposure if the dataset is leaked. Encrypting and retaining them is the tempting distractor, since encryption is a real safeguard, but keeping unneeded sensitive fields still widens the risk. Placing identifiers in prompts or model cards would expose them directly.

8. Restricting the outbound network access of a model-serving container limits what an attacker can exfiltrate if the container is compromised.
- A True
 - B False

Answer: A (True)

Restricting egress blocks the connections a compromised container would use to send data out or download additional tools. The statement is true, and it complements least privilege and read-only filesystems. The tempting mistake is assuming that inbound restrictions alone limit data theft.

9. A security team needs evidence of whether a deployed model's behavior has changed since its approval. Which practice provides this?
- A A one-time evaluation at launch that is never repeated
 - B A ping test confirming that the server responds
 - C Scheduled re-evaluation of the deployed model against its approved test suite, with results recorded
 - D A count of employees who logged in to the tool this month

Answer: C

Scheduled re-evaluation against the approved suite, with recorded results, detects behavior drift and gives auditable evidence over time. A launch-only evaluation is the tempting distractor, since it was valid once, but it cannot show what changed later. Ping tests and login counts do not measure model behavior.

10. During an incident in which a model leaked training data, which first step best preserves evidence for investigation?
- A Retrain the model immediately on a clean dataset and delete the old artifacts so the rollback path is not confused later
 - B Restart every service so that the problem is cleared from memory
 - C Email the leaked content to all employees to explain the situation
 - D Snapshot the relevant logs, model artifacts and access records before making changes

Answer: D

Snapshotting logs, artifacts and access records before changes keeps the facts available for root cause analysis and disclosure decisions. Retraining and deleting artifacts is the tempting distractor, since it feels like a fix, but it destroys the evidence needed to understand the leak. Restarting services clears memory-resident evidence, and mass emailing spreads the leaked content.