

PRACTICE QUESTIONS

CompTIA

CY0-001

CompTIA SecAI+

SHARED BY [u/Wise-Byte-4963](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	CompTIA CY0-001, CompTIA SecAI+

Shared by [u/Wise-Byte-4963](#) 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. In the NIST AI Risk Management Framework, which function is responsible for establishing policies, roles, accountability and risk tolerance for AI systems across the organization?
 - A Map
 - B Govern
 - C Measure
 - D Manage

Answer: B

Govern sets the policies, roles, accountability structures and risk tolerance that shape how the other functions operate. Map is the tempting distractor, since it also comes early and frames each AI system's context, but it identifies context and risks rather than setting organizational policy. Measure assesses identified risks, and Manage prioritizes and acts on them.

2. The EU AI Act tier that bans practices outright, such as social scoring by public authorities, is called _____ risk.

Answer: unacceptable

The unacceptable risk tier covers practices the Act prohibits outright, which is a different category from systems that are merely regulated. High risk is the tempting distractor, since high-risk systems face strict obligations, but they remain permitted when they meet them.

3. Which OWASP Top 10 for LLM Applications entry covers a model acting on unvalidated output, such as running a generated shell command or passing generated SQL straight to a database?
 - A System prompt leakage
 - B Improper output handling
 - C Vector and embedding weaknesses
 - D Unbounded consumption

Answer: B

Improper output handling covers downstream components that trust model output without validation, which can enable injection or code execution. Excessive agency is the tempting distractor, since it also concerns what the model causes systems to do, but it is about giving the model more tools and permissions than it needs. System prompt leakage, embedding weaknesses and unbounded consumption describe different risks.

4. Data poisoning changes the training data so that the trained model behaves incorrectly, and it differs from evasion because evasion modifies inputs at inference time.

- A True
- B False

Answer: A (True)

Poisoning manipulates the data used to train the model, which changes learned behavior, while evasion alters inputs presented to an already trained model. The statement is true, and the distinction matters because the controls differ: data provenance for poisoning, and input validation and robustness testing for evasion.

5. Which two statements about model supply chain risk are correct? (Choose two.)

- A A model downloaded from a public hub is automatically safe because it has many downloads
- B A model's license and origin are part of its risk profile and should be recorded in an inventory
- C Dependencies of a model-serving stack do not need to be scanned because they are not the model itself
- D Running an unknown model inside a sandbox is unnecessary once the file hash has been checked
- E Pretrained models from public hubs should be verified for integrity and provenance before use

Answer: B, E

Verifying integrity and provenance for public models, and recording licenses and origin in an inventory, are the controls that address supply chain risk. Download counts are the tempting distractor, since popularity feels like assurance, but popular artifacts can still be malicious or tampered with. Serving-stack dependencies are part of the attack surface, and a matching hash does not show that the model behaves safely.

6. A team wants to store model weights in a format that cannot execute code when loaded and that supports fast memory-mapped access. Which format fits best?

- A Python pickle
- B Safetensors
- C Serialized Java objects
- D Shell scripts that embed weights as text

Answer: B

Safetensors stores tensors without executable code and is designed for safe, fast loading, which is why it is preferred for distributing weights. Pickle is the tempting distractor, since it is the default in many ML workflows, but loading it can execute code. Serialized Java objects and shell scripts carry the same kind of execution risk and are not designed for tensor storage.

7. Before a new model version goes live, which step most directly confirms that it still meets the organization's security requirements?
- A Checking that the model's file name matches the release ticket
 - B Confirming that the training run finished without an error message and that the loss curve looks smooth in the dashboard
 - C Running a security evaluation with adversarial test cases and comparing results with the previous version
 - D Asking the data scientist who built it whether it looks fine

Answer: C

A security evaluation with adversarial test cases checks the new version against the same requirements as before, and comparing results shows any regression. Checking the file name is the tempting distractor, since it is part of release hygiene, but it says nothing about behavior. A clean training run and informal review do not test security properties.

8. A model file format that stores tensors without executable code and is recommended over pickle is called _____.

Answer: safetensors

Safetensors stores tensor data without a code execution path and supports fast loading. Pickle is the tempting distractor, since it is the common default in ML workflows, but it can run code during deserialization.

9. Which log data is most useful for detecting prompt injection that led an AI agent to call an unexpected tool?
- A The sequence of tool calls, arguments and retrieved sources recorded for each agent session
 - B Only the total number of requests per hour across the platform
 - C The data center's CPU temperature readings from the cooling system, sampled every minute for each rack in the building
 - D The list of browsers used by employees who accessed the tool

Answer: A

Session-level records of tool calls, their arguments and the retrieved sources show what the agent did and what content influenced it. Hourly request totals are the tempting distractor, since they reveal spikes, but they do not explain which action was taken or why. Temperature readings and browser lists do not describe agent behavior.

10. An organization wants alerts when an AI system's responses begin to contain sensitive identifiers. Which control fits best?
- A A quarterly manual review of a random sample of responses only
 - B An output detector that scans responses for identifier patterns and raises an alert or blocks the response
 - C A dashboard that shows average response length and token counts without any content checks on the text of the responses
 - D A rule that the model must sign each reply with the developer's name

Answer: B

An output detector scans responses in near real time for identifier patterns and can alert or block before the data reaches the user. A quarterly sample review is the tempting distractor, since sampling is useful, but it detects leaks months after they occur. Length dashboards and signatures do not inspect content for sensitive data.