

## PRACTICE QUESTIONS

CertiProf

# AIAM

## AI Agent Manager Professional Certification

SHARED BY [u/Swift-Packet-1490](#) on aiexamcerts

---

EDITION Free Set 1

---

QUESTIONS 10

---

SHARED October 15, 2026

---

EXAM CertiProf AIAM, AI Agent Manager Professional Certification

---

Shared by [u/Swift-Packet-1490](#) on aiexamcerts

10 practice questions for the CertiProf AIAM exam, AI Agent Manager Professional Certification, each followed by its answer and a short explanation. More free sets and the full practice exam:

[www.aiexamcerts.com/certiprof/aiam](http://www.aiexamcerts.com/certiprof/aiam). Spotted a mistake? Email [support@aiexamcerts.com](mailto:support@aiexamcerts.com) with the exam code AIAM and the question number.

1. In the ReAct pattern, what do the reasoning and acting steps refer to?
  - A Compressing the prompt before each model call
  - B Alternating reasoning traces with tool actions and observations
  - C Running two models in parallel and voting on the answer
  - D Training the model with reinforcement learning from human feedback

**Answer: B**

ReAct interleaves reasoning traces with actions such as tool calls, then feeds each observation back into the next reasoning step. Prompt compression and voting ensembles are plausible architecture ideas, but they do not define ReAct. Reinforcement learning from feedback is a model training method rather than an agent loop.

2. An autonomous system that perceives its environment, plans, and takes actions toward a goal is called an AI \_\_\_\_\_.

**Answer: agent**

An AI agent combines reasoning, planning and tool use in a loop until a goal is met. A chatbot answers each message without acting on external systems, which is the tempting but narrower description.

3. A team wants to diagnose why an agent chose a poor path, not just whether it failed. Which evaluation approach fits best?
  - A A single pass-fail score on the final answer only
  - B Trajectory review of each step, tool call and observation
  - C Counting how many users clicked the agent button in the interface
  - D Comparing only the length of the system prompt across versions

**Answer: B**

Trajectory review examines the sequence of reasoning, tool calls and observations, which shows where the path went wrong. A pass-fail score on the final answer is the tempting shortcut, but it hides why the run failed. Click counts and prompt length say little about decision quality.

4. Tool schemas give the model the names, descriptions and parameters it needs to call a tool.
- A True
  - B False

**Answer: A (True)**

This is true. The schema describes what the tool does and what arguments it accepts, which is the information the model uses to produce a valid call.

---

5. Which two controls reduce the risk of excessive agency? (Choose two.)
- A Limiting the tools to those the task actually needs
  - B Granting write access to every system by default
  - C Requiring approval for irreversible actions
  - D Running the agent with a shared administrator account
  - E Removing audit logs to save storage space

**Answer: A, C**

Restricting tools to what the task needs and requiring approval for irreversible steps keep the agent's power matched to its purpose. Default write access and shared administrator accounts grant far more power than necessary. Removing audit logs removes the evidence needed to detect misuse.

---

6. Which practice is most reliable for detecting regressions after changing an agent's prompt or tools?
- A Reviewing one manually chosen example after each change
  - B Shipping the change and waiting for user complaints to arrive
  - C Running a fixed regression suite of representative tasks
  - D Increasing the model temperature so responses show more variety

**Answer: C**

A fixed regression suite of representative tasks runs the same cases before and after each change, so differences are attributable and repeatable. A single hand-picked example is the tempting quick check, but it samples too little to catch regressions. Waiting for complaints and raising temperature both make results less predictable.

---

7. Which protocol standardizes how AI applications connect models to external tools and data sources?

- A Simple Mail Transfer Protocol
- B Model Context Protocol
- C Border Gateway Protocol
- D Secure Shell Protocol

**Answer: B**

The Model Context Protocol defines a common way for AI applications to discover and use tools, resources and prompts exposed by servers. The mail, routing and remote shell protocols are real standards, but they serve unrelated purposes. Choosing one of them would mismatch the agent integration layer.

8. In a design where one agent breaks a goal into subtasks and assigns them to specialist agents, the pattern is called orchestrator-\_\_\_\_\_.

**Answer: worker**

The orchestrator-worker pattern separates coordination from execution, with the orchestrator planning and the workers carrying out subtasks. A peer-to-peer design lacks a central coordinator, which is the tempting alternative.

9. Which risk is most specific to multi-agent systems compared with a single agent?

- A Tokenizer mismatch between two models in one prompt
- B Loss of GPU memory during a single inference call
- C Slow response times for a single user session
- D Cascading errors passed between agents that trust each other's output

**Answer: D**

When agents consume each other's outputs without validation, one bad result can propagate and grow through the chain. Tokenizer mismatch and memory loss are technical issues that can occur in any system. Latency for one session is a performance concern rather than a failure path unique to multi-agent designs.

10. Why is storing customer secrets in agent long-term memory risky?

- A Memory stores are too small to hold any meaningful text
- B Long-term memory always deletes data after a single day
- C Recalled content can leak into other responses or sessions
- D Vector databases cannot index any personal information at all

**Answer: C**

Recalled memory can surface in unrelated answers or be exposed across tenants if access is not scoped, so sensitive values should not be stored there casually. Size limits are not the real concern, and automatic deletion is not a standard guarantee. Vector databases can index text, so the risk is about access and retention rather than indexing.