Tanimawo AI Academy

ADVANCED

Build an AI Agent with Tools

Function calling, the agent loop, and the guardrails every agent needs

Free guide

About 20 minutes to read

tanimawoai.com

Free AI training every Sunday
with Dr. Daniel Tanimawo

© 2026 Dr. Daniel Tanimawo · Tanimawo AI Academy · tanimawoai.com · Free to download and share with credit. Selling, rebranding or removing this notice is not allowed.

What makes it an agent

An agent is a model in a **loop** that can call **tools** (functions you write): look up data, do calculations, search, send a draft for approval. The model decides which tool to call; your code runs it and sends the result back.

Tool (function) calling

You describe each tool with a name, a description and a JSON schema for its inputs. The model replies either with text or with a request to call a tool.

```
import json
from openai import OpenAI

client = OpenAI()

def get_class_time(city):
    times = {"lagos": "Sunday 8:00 PM",
             "london": "Sunday 8:00 PM in summer, 7:00 PM in winter",
             "houston": "Sunday 2:00 PM in summer, 1:00 PM in winter"}
    return times.get(city.lower(), "Unknown city")

TOOLS = [{
    "type": "function",
    "function": {
        "name": "get_class_time",
        "description": "Get the local time of the weekly class in a city.",
        "parameters": {
            "type": "object",
            "properties": {"city": {"type": "string"}},
            "required": ["city"],
        },
    },
}]
```

TANIMAWO AI ACADEMY
tanimawoai.com · Dr. Daniel Tanimawo

© 2026 Dr. Daniel Tanimawo · Tanimawo AI Academy · tanimawoai.com · Free to download and share with credit. Selling, rebranding or removing this notice is not allowed.

The agent loop (with limits)

```
def run_agent(goal, max_steps=5):
    messages = [
        {"role": "system", "content": "You help students. Use tools when needed."},
        {"role": "user", "content": goal},
    ]
    for step in range(max_steps):
        r = client.chat.completions.create(
            model="gpt-4.1-mini", max_tokens=400,
            messages=messages, tools=TOOLS)
        msg = r.choices[0].message
        if not msg.tool_calls:
            return msg.content
        messages.append(msg)
        for call in msg.tool_calls:
            args = json.loads(call.function.arguments)
            if call.function.name == "get_class_time":
                result = get_class_time(**args)
            else:
                result = "Unknown tool"
            messages.append({"role": "tool",
                             "tool_call_id": call.id,
                             "content": result})
    return "Stopped: step limit reached."

print(run_agent("What time is the class in London and in Houston?"))
```

Guardrails every agent needs

Guardrail	Why
Step limit (max_steps)	Prevents endless loops and runaway costs
Token and budget limits	A hard stop on spending
Allow-list of tools	The model can only use what you provide
Validate tool inputs	Never trust arguments blindly (types, ranges, permissions)
Human approval for risky actions	Sending, paying, deleting or posting needs a person's OK
Logs of every step	Debugging and accountability
Treat web content as untrusted	Pages and documents can contain hidden instructions

> Design tools to be **safe by default**: a tool that drafts an email is safer than one that sends it.

TANIMAWO AI ACADEMY · tanimawoai.com · Dr. Daniel Tanimawo

© 2026 Dr. Daniel Tanimawo · Tanimawo AI Academy · tanimawoai.com · Free to download and share with credit. Selling, rebranding or removing this notice is not allowed.

Good tool design

- One clear job per tool, with a precise description
- Return short, structured results (not whole web pages)
- Return helpful errors (“City not found; try a capital city”)
- Make actions **reversible** where possible

Testing agents

- [ ] Run 20 realistic goals and check every step, not just the final answer.
- [ ] Include tricky goals: missing information, impossible requests, harmful requests.
- [ ] Measure steps, tokens and cost per goal.
- [ ] Re-run the tests whenever you change the prompt, model or tools.

Keep learning, free

Join the free live AI class every Sunday at 8 PM Nigeria time with Dr. Daniel Tanimawo. Register at **tanimawoai.com**, watch past classes on the Replays page, and download more free guides.

Share this guide with a friend who wants to learn AI.

TANIMAWO AI ACADEMY
tanimawoai.com · Dr. Daniel Tanimawo

© 2026 Dr. Daniel Tanimawo · Tanimawo AI Academy · tanimawoai.com · Free to download and share with credit. Selling, rebranding or removing this notice is not allowed.