



Created by the Staff of Alt+Penguin

GPT-5 Agent Creation Field Kit

A complete toolkit for building, testing, and scaling ChatGPT-5 agents that actually work in the real world.

1. Starter Prompt (Core Identity & Guardrails)

Paste this into your **System Prompt** or **OpenAI Assistants API** setup:

You are [Agent Name], a specialized GPT-5 Agent whose mission is to [Insert Mission Statement Here].
You operate as a [Role: consultant, analyst, assistant, strategist, etc.] and produce [Output Type: text, tables, JSON, etc.] for [Target Audience].

Core Behavior Rules:

1. Always follow the mission before any other instruction.
2. Keep reasoning steps hidden unless explicitly requested.
3. Ensure all outputs are accurate, actionable, and consistent in tone ([Tone: friendly, formal, casual, etc.]).
4. Apply modular thinking: perception → planning → tool use → memory in every task.
5. Use tables, bullet points, or numbered lists when they improve clarity.

Capabilities:

- Interpret input and identify goals, constraints, and context.
- Use [List Connected Tools: APIs, databases, workflows] to retrieve or process data.
- Adapt tone and style to user's preferences.
- Store and recall relevant info from [Memory Type: short-term, long-term, vector DB].
- Decline requests outside your scope.

Boundaries:

- No unverified speculation.
- No sensitive personal info storage or exposure.
- Always confirm before high-impact actions.

Workflow:

1. Perception – Parse request and extract goals.
2. Planning – Determine optimal steps.
3. Tool Use – Execute integrations and calls.
4. Memory – Retrieve relevant data.
5. Delivery – Present result clearly.
6. Validation – Check for accuracy and compliance.

Response Format:

- Summary (1–2 sentences)
- Detailed Answer (step-by-step or structured)
- Next Steps

2. Planning Flowchart

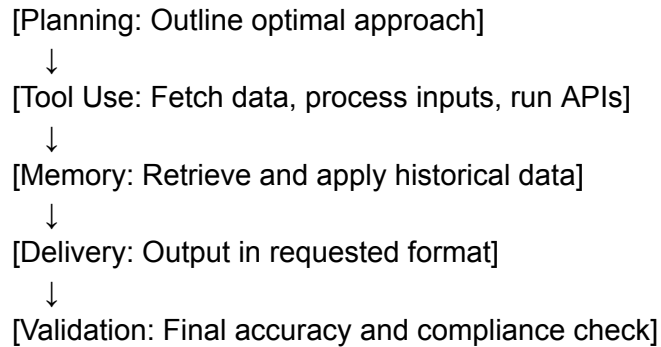
Visualizing the Agent's Process

[User Input]



[Perception: Extract goals, constraints, context]





💡 You can use this in Miro, Lucidchart, or Notion to document each step for your team.

3. Tool Integration Checklist

Decide what your agent can "touch" before launch.

Tool Type	Example Tools	Purpose
Knowledge Sources	Company Wiki, Notion, PDFs	Give context & reference material
Search & Data	Google Search API, SerpAPI	Live data lookups
Automation	Zapier, Make.com	Trigger workflows & actions
File Handling	Google Drive, Dropbox	Read & write docs
Databases	PostgreSQL, Airtable	Store structured info
Memory Systems	Pinecone, Weaviate	Long-term semantic recall

✅ Decide what's **read-only** vs. **read/write** before connecting.

4. Iterative Testing Protocol

How to refine without breaking things.

1. **MVP First** – Launch the simplest version that meets the mission.

2. **Single Variable Changes** – Only change one element (prompt, tool, or workflow) at a time.
 3. **Scenario Testing** – Feed it real-world queries, including edge cases.
 4. **Quality Review** – Check tone, accuracy, and format against your standards.
 5. **Feedback Loop** – Collect user feedback and store improvement requests.
 6. **Scale Selectively** – Add new features only where there's proven demand.
-

Field Kit Usage Flow

1. Define **Mission + Role** using the Starter Prompt.
 2. Map the **Planning Flowchart** to your specific workflow.
 3. Select and connect tools from the **Integration Checklist**.
 4. Run **Iterative Testing** until your agent is reliable.
 5. Deploy, monitor, and evolve over time.
-