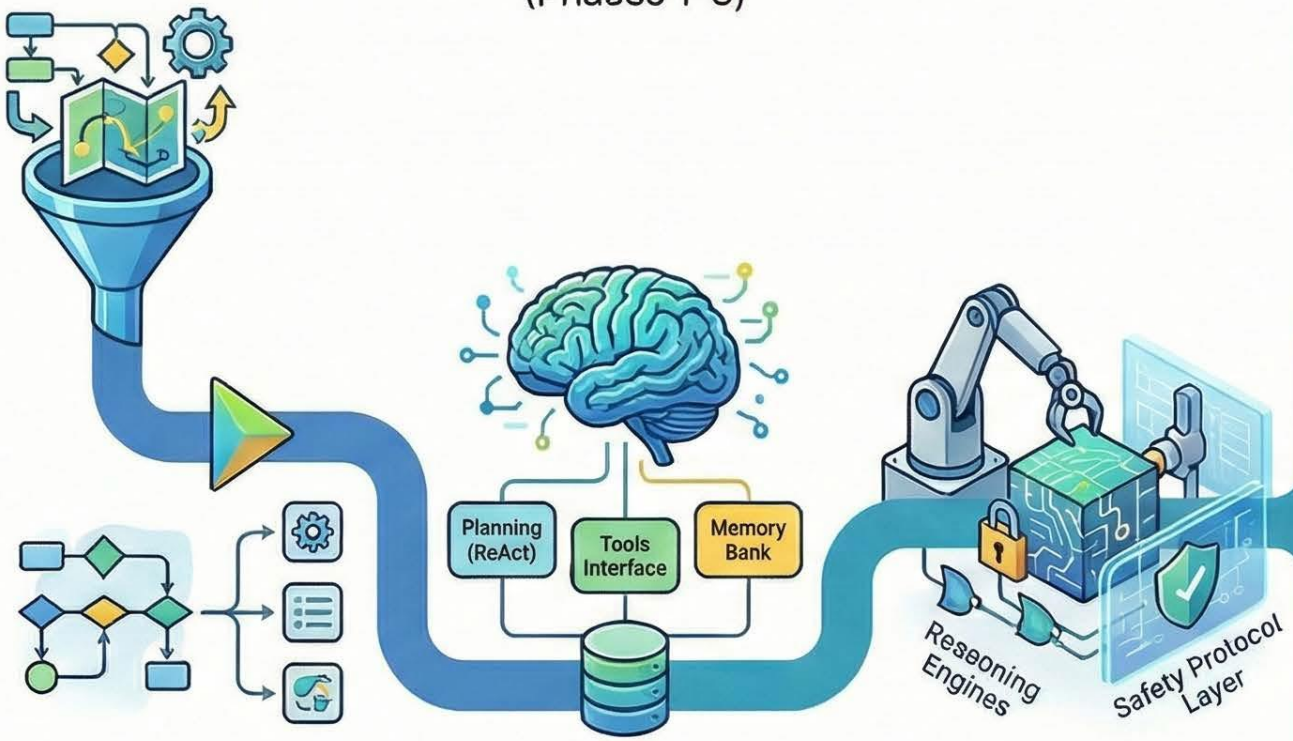
The AI Agent Lifecycle: From Design to Operation

DESIGN & DEVELOPMENT
(Phases 1-3)

OPERATIONS & GOVERNANCE
(Phase 4 & Outcomes)



1. Define the Use Case
Identify tasks for automation and map business workflows to agent capabilities.

2. Architect the Agent's Core
Select planning models (e.g., ReAct), tools, and memory architecture.

3. Build with Safeguards
Develop multi-step reasoning abilities with built-in safety guardraile.

4. Implement AgentOps
Establish real-time monitoring, fallure recovery, and security sandboxing.

Mitigate Critical Risks
Prevents rogue behavior, incorrect tool use, and endless loops.

Receive Core Deliverables
Includes architecture blueprints, an AgentOps dashboard, and safety configurations.