Permission Planning Worksheet

Use this worksheet to draft practical boundaries for one customer-facing AI agent use case. Decide what the agent may do, what it may only propose, when approval is required, and what system evidence must record the decision.

Use case snapshot

Field	Notes
Business task	
Customer request or situation	
Agent role	
Business owner	
Technical owner	

Permission levels: Inform means the agent may explain or retrieve information. Recommend means it may propose an action for a person or approved workflow to decide. Act within limits means it may execute only when the stated conditions are met. Request approval means it must route the action before execution. Not permitted means the agent must not propose or execute the action.

Action inventory

Agent action	Permission level	Routine limit	Approval trigger	Evidence to retain

Action inventory continued

Agent action	Permission level	Routine limit	Approval trigger	Evidence to retain

Approval request checklist

Approval request item	What to include
Customer request summary	
Action the agent proposes	
Action the agent is authorized to execute	
Policy or business rule involved	
Reason approval is required	
Evidence reviewed by the system	
Approver and result	

Test scenarios

Scenario type	Scenario to test
Routine case	
Boundary case	
Exception case	
Prohibited action	
Record review	

Implementation questions

- Which controls enforce the limits described here?
- Where does the approval request appear, and who can approve it?
- What system record proves what happened?
- What should happen when approval is unavailable?
- How will the team detect repeated exceptions or policy drift?