

Agent Ownership & Risk Mapping Canvas (FREE)

MBCC • Agent Ops Control Plane™ — outcome-first, governance-first delivery

How to use (5 minutes):

- 1) Fill each section with short bullets.
- 2) Identify one 'kill switch' owner.
- 3) List top 3 risks.
- 4) Decide the first gated action.

1) Use Case & Outcome

What workflow are you automating? What does success look like?

2) Data Boundaries

What data can the agent access? What is prohibited?

3) Tools & Permissions

Which tools/APIs can it call? What requires approval?

4) Ownership & Authority

Who owns this agent? Who can stop it? Who approves changes?

5) Runtime Guardrails

Allowlist/denylist, budgets, rate limits, PII masking, escalation

6) Observability & Audit

What must be logged? What alerts matter? How do we prove what happened?

7) Top Risks

List top risks + mitigations (quiet erosion risks count)

8) Go/No-Go Gate

What must be true before production? What triggers rollback?