OPERATIONAL INTELLIGENCE

AI Resilience Planner

A worksheet for preparing AI-supported workflows for failure, drift, ownership gaps, degraded context, and operational recovery.

WHAT THIS TEMPLATE HELPS YOU DECIDE

Move beyond generic risk lists by mapping failure modes to fallback paths, owners, monitoring signals, recovery evidence, and operating cadence.

BEST FOR

- Teams making AI part of a recurring business workflow
- Operations that rely on model availability, retrieval quality, or tool execution
- Leaders who need confidence before AI becomes business-critical

OUTPUTS

- Failure scenarios tied to business impact
- Named fallback owners and recovery actions
- Monitoring signals for operational intelligence

STEP 1

Name the failure modes

AI resilience starts with concrete operating scenarios. Do not ask only whether the model is accurate. Ask what happens when the workflow cannot be trusted.

Workflow risk frame

Business workflow
Name the recurring operation this AI system supports.

Critical dependency
Model provider, retrieval source, integration, permission, approval queue, or data feed.

Customer or operational impact
Describe what breaks for the business if the system degrades.

Common failure modes

- [ ] Model or API provider outage
- [ ] Retrieval returns stale, incomplete, or unauthorized context
- [ ] Tool execution fails after the model recommends an action
- [ ] Prompt or workflow change creates inconsistent behavior
- [ ] Cost, latency, or volume spike changes operating economics
- [ ] Human approval queue becomes the bottleneck

STEP 2

Design fallback paths

A fallback is not a vague backup plan. It is a defined operating route that keeps the business moving when AI support is unavailable, unsafe, or incomplete.

Fallback map

Failure signal	What exactly tells the team that the AI workflow is degraded?
Fallback route	What manual, deterministic, or reduced-scope process takes over?
Owner	Who decides whether to activate, maintain, or exit the fallback?
User message	What should customers or internal users see during degradation?
Recovery proof	What evidence shows the workflow is safe to restore?

A resilient AI-native workflow can degrade gracefully. Users should know what changed, operators should know who owns it, and leadership should see evidence of recovery.

STEP 3

Create the operating cadence

Resilience is not a one-time launch checklist. It is an operating rhythm: monitor, review, tune, and keep ownership current.

Monitoring signals

- [ ] Latency and availability by workflow
- [ ] Retrieval quality, missing-source rate, and stale-context incidents
- [ ] Human override, rejection, and edit rates
- [ ] Tool call failures and retry outcomes
- [ ] Escalation volume by topic, team, and customer segment
- [ ] Cost per successful workflow completion

Review cadence

Daily	Which incidents or broken workflows must be visible immediately?
Weekly	Which exception patterns should be reviewed with operators?
Monthly	Which architecture changes, tools, or policy updates require leadership review?
After incident	What gets documented before the system is considered stable again?