INTELLISYNC GOVERNANCE

Canadian AI Risk & Fallback Planner

A practical governance worksheet for Canadian organizations deploying AI.

AI systems can generate powerful results — but without clear operational boundaries they can also create regulatory, legal, and reputational risk.

This framework helps organizations define guardrails, escalation rules, and operational limits before deploying AI in real business workflows.

INTELLISYNC GOVERNANCE

AI Resilience Context

Most organizations deploy AI features without preparing for operational failures.

The model works during demos.
Responses appear accurate during testing.

But in production environments failures eventually occur.

Common failure conditions include:

- model provider outages
- hallucinated regulatory or compliance information
- cross-border data routing errors
- unexpected spikes in operational cost

Without a defined fallback strategy, AI systems quickly become a single point of operational failure.

This planner helps Canadian organizations prepare for those scenarios before they occur.

INTELLISYNC GOVERNANCE

AI Risk Assessment

Risk Assessment Matrix

Visualize and prioritize your AI system risks

RISK ASSESSMENT MATRIX

Risk levels based on data sensitivity and access patterns

How to Use This Matrix

Use this matrix to identify the most likely failure modes in your AI systems.

Each scenario should be evaluated across two dimensions:

- **Impact** — how severely Canadian operations would be affected
- **Probability** — how likely the event is to occur

High-impact and high-probability scenarios should receive immediate fallback planning.

1. Scenario Planning

How to Build Failure Scenarios

Effective resilience planning starts by identifying the most realistic ways an AI system could fail.

Focus on operational risks rather than technical edge cases. Examples include:

- infrastructure outages
- incorrect regulatory guidance
- security or data routing failures
- unexpected vendor downtime

For each scenario define:

- the operational impact
- the fallback system
- the responsible owner

This ensures your team can respond quickly during real incidents.

Map your failure modes. What breaks, what's the impact, and what's the backup plan?

Scenario 1: The Model Provider is Down (Canadian Operations)

Impact: [Low/Medium/High] - Canadian customer service bot stops answering.

Fallback: Switch to Canadian-based standard search / Display "AI services temporarily unavailable" banner.

Owner: Canadian IT Ops /

Scenario 2: The AI Hallucinates Canadian-Specific Wrong Answers

Impact: [Low/Medium/High] - Bad advice about Canadian regulations or compliance.

Fallback: Automated email retraction / Canadian legal team outreach.

Owner: Canadian Customer Success /

Scenario 3: Cross-Border Data Transfer Violation

Impact: [Low/Medium/High] - Canadian data sent to non-compliant jurisdiction / PIPEDA violation.

Fallback: Immediate Canadian data routing / Activate Canadian-only processing.

Owner: Canadian Privacy Officer /

INTELLISYNC GOVERNANCE

Resilience Safeguards

Quick AI Resilience Actions

Before deploying AI into production workflows, confirm the following safeguards exist:

- a documented fallback if the AI provider becomes unavailable
- human escalation paths for incorrect AI outputs
- clear routing for Canadian data residency requirements
- defined ownership for AI system maintenance

If any of these safeguards are unclear, your organization may be operating AI systems without adequate resilience planning.

SCENARIO RISK ASSESSMENT

70%

RISK LEVEL: MEDIUM

2. Assign Control Ownership

Why Ownership Matters

AI systems introduce new operational responsibilities that often fall between teams.

Without clearly defined ownership:

- prompt changes may go unreviewed
- API credentials may remain unrotated
- performance issues may go undetected

Defining responsible roles ensures the AI system remains secure, compliant, and operational over time.

Who holds the keys? Document the specific roles responsible for:

Approving changes to the core system prompt:

Name/Role:

Managing and rotating API keys:

Name/Role:

Reviewing the weekly AI performance dashboard:

Name/Role:

CONTROL CLARITY SCORE

Role Assignment Coverage

60%

RISK LEVEL: MEDIUM

3. Track Performance Metrics

Why Monitoring Is Critical

AI systems require continuous monitoring to ensure they operate safely and efficiently.

Unlike traditional software systems, AI outputs can degrade gradually over time due to:

- model updates
- prompt changes
- data drift
- increased system load

Monitoring key signals helps detect problems early before they impact customers or operations.

What signals will you audit to ensure the AI is operating safely?

- [ ] Latency (Is the model responding quickly?)
- [ ] Refusal Rates (Is the AI declining to answer too often?)
- [ ] Human Override Rate (How often do humans have to edit the AI's drafts?)
- [ ] Cost per Interaction (Are you overpaying for simple queries?)

MONITORING COVERAGE

Performance Metrics Coverage

RISK LEVEL: MEDIUM

INTELLISYNC GOVERNANCE

AI Resilience Readiness Check

Use this quick assessment to evaluate your organization's resilience planning.

- [ ] Our AI systems have defined fallback mechanisms.
- [ ] We know which team owns each AI system.
- [ ] We have escalation procedures for incorrect AI outputs.
- [ ] Canadian data routing rules are documented.
- [ ] Performance metrics are monitored regularly.

If more than two of these items are unclear, your organization likely lacks a formal AI resilience strategy.

AI GOVERNANCE ALERT
Most organizations deploy AI before establishing operational guardrails.

Build Resilient AI Systems

AI systems should not become operational single points of failure. IntelliSync helps Canadian organizations design resilient AI architectures with fallback systems, escalation workflows, and continuous compliance monitoring.

WHAT INTELLISYNC HELPS YOU IMPLEMENT

- Map AI data flows and system dependencies
- Design guardrails and escalation workflows
- Implement AI resilience and fallback strategies
- Align AI operations with Canadian privacy expectations

RECOMMENDED NEXT STEP

Book a Canadian AI Resilience Assessment with IntelliSync. We will: • map your AI failure scenarios • design fallback architectures • implement monitoring and governance controls

SCHEDULE A CONVERSATION **info@intellisync.ca**