INTELLISYNC GOVERNANCE

Canadian Responsible AI Governance

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

Why AI Governance Matters

Most organizations deploy AI tools before establishing governance rules.

The model works.
The demo looks impressive.

But once deployed into real workflows the risks multiply.

AI systems can generate financial commitments, legal interpretations, customer communications, and operational decisions without human review.

Without clear guardrails organizations expose themselves to:

- reputational damage
- compliance violations
- contractual risk
- customer trust erosion

INTELLISYNC GOVERNANCE

Common AI Governance Failures

1. Undefined Purpose

Many AI deployments do not clearly define what the AI is allowed to do.

Without purpose boundaries, systems begin producing outputs outside their intended role.

2. Missing Topic Restrictions

AI models can produce financial, legal, or medical advice even when the organization never intended them to do so.

3. No Human Escalation

If there is no defined escalation rule, AI outputs can be delivered directly to customers without human oversight.

Governance Architecture

AI Governance Architecture

Three-layer approach to responsible AI implementation

SYSTEM ARCHITECTURE OVERVIEW

Three-layer architecture with clear separation of concerns

INTELLISYNC GOVERNANCE

Step 1: Define AI Purpose

A clearly defined AI purpose prevents the system from expanding into unintended operational roles.

Purpose definition is the first layer of responsible AI governance.

Quick Governance Actions

Before defining prompts or workflows, complete the following checks:

- List every AI system currently used in your organization
- Document the exact task each AI system performs
- Identify which teams rely on each AI tool
- Confirm whether AI outputs are used internally or sent externally

Most organizations discover they have more AI usage than leadership realizes.

Be explicit about what the AI is allowed to do.

Primary function:

(e.g., Draft first-response customer service emails)

Secondary function:

PURPOSE CLARITY SCORE

AI Purpose Definition

65%

RISK LEVEL: MEDIUM

INTELLISYNC GOVERNANCE

Step 2: Set the Forbidden Topics

Certain topics should never be generated by AI systems without human review.

Defining forbidden topics prevents accidental legal, financial, or reputational exposure.

Quick Governance Actions

Ask the following questions before defining AI boundaries:

- Could the AI generate financial commitments or pricing?
- Could the AI interpret legal or compliance requirements?
- Could the AI expose internal business data?
- Could the AI provide healthcare or safety advice?
- Could the AI compare your company with competitors?

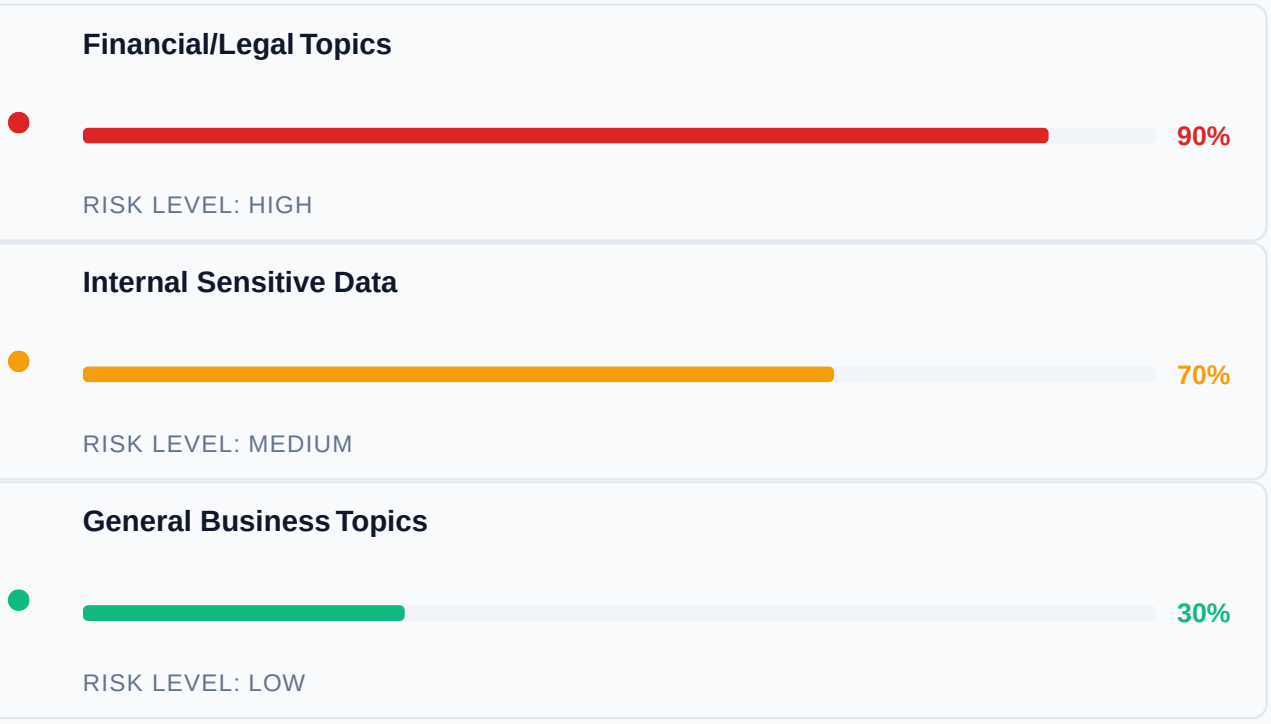
If the answer to any of these questions is yes, the topic should be restricted or routed to human review.

List the boundaries. What is the AI explicitly forbidden from generating or discussing?

- [ ] Canadian financial advice or pricing commitments
- [ ] Canadian legal or compliance recommendations
- [ ] Internal Canadian HR policies and compensation details
- [ ]

- [ ] Speculating about unannounced Canadian products/services
- [ ] Canadian healthcare or medical advice
- [ ] Comparisons with Canadian competitors

BOUNDARY ENFORCEMENT RISK



INTELLISYNC GOVERNANCE

Step 3: Establish Escalation Rules

AI systems should never operate without a defined human escalation path.

Escalation ensures high-risk outputs are reviewed before delivery to customers, partners, or the public.

Quick Governance Actions

Define the conditions where AI must defer to a human. Examples include:

- customer complaints or refund requests
- legal language or contract references
- emotionally charged messages
- financial commitments or pricing negotiations
- safety, medical, or regulatory questions

Escalation rules prevent AI systems from making decisions that require human judgement.

When does a human need to step in?

Confidence Thresholds:

If the AI is unsure about a response, what happens? (e.g., If confidence is below 80%, route the draft to a manager)

High-Risk Triggers:

What specific words or topics require human review? (e.g., "refund", "lawsuit", "angry")

Final Approval:

Who hits "send" on the final output?

ESCALATION COVERAGE

Human Oversight Coverage

RISK LEVEL: MEDIUM

INTELLISYNC GOVERNANCE

AI Governance Readiness Check

Review your organization's current governance maturity:

- [ ] Our AI systems have a clearly defined operational purpose
- [ ] We have documented forbidden topics
- [ ] We have human escalation thresholds
- [ ] Our prompts include enforceable system guardrails
- [ ] AI outputs are reviewed before delivery

If you cannot confidently check all five boxes, your organization likely lacks a complete AI governance framework.

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

Don't Deploy AI Without Guardrails.

IntelliSync helps Canadian businesses design operational AI systems with enforceable governance rules, escalation workflows, and compliance-aligned architectures. If your

organization is experimenting with AI but lacks a clear governance framework, now is the time to establish one.

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

Schedule an AI Governance Assessment

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