CAHILL CONSULTANTS

AI Pilot Governance
Starter Kit

Pre-flight governance tools for regulated-industry AI pilots

FREE EDITION

INSURANCE · HEALTHCARE · FINANCIAL SERVICES

cahillnet.com

START HERE

Govern the pilot before you run it

Most AI pilots in regulated environments don't fail on the technology. They fail on review — when legal, compliance, or the steering committee asks questions the team didn't decide before launch. Data boundaries get discovered mid-flight. Controls get retrofitted under pressure. Nobody agreed in advance on what would end the pilot. By then, the cost of fixing it is high and the credibility damage is done.

This kit front-loads those decisions. It is vendor-neutral — the four tools work with any AI platform — and it is deliberately lightweight. Use it to get a pilot to a defensible starting line, fast.

WHAT'S INSIDE

1. **Pilot Readiness Checklist** — a go/no-go gate across six domains.
2. **Use Case Risk Assessment** — a five-dimension screen with banded outcomes.
3. **Governance Review Agenda** — a ready-to-run meeting structure.
4. **Data Boundary Quick Reference** — a four-tier “what can go in” table.

What this is — and isn't. A starter kit gets you to launch. It is not the full control library, regulatory crosswalk, or incident framework a production rollout needs. The last page maps each tool to where the depth lives.

TOOL 01

AI Pilot Readiness Checklist

A go/no-go gate. Work it before granting access. If any item under **Data Boundaries** or **Legal & Compliance** is unchecked, the pilot is not ready to launch — regardless of how ready the rest looks.

SPONSORSHIP & SCOPE

- [ ] A named executive sponsor is accountable for pilot outcomes.
- [ ] There is a written problem statement and two to four measurable success criteria.
- [ ] The pilot is time-boxed (6–12 weeks recommended) with a defined end date.
- [ ] Scope is limited to a single department or workflow.

DATA BOUNDARIES

- [ ] A data classification scheme exists and pilot data has been classified.
- [ ] The highest data tier in scope is documented.
- [ ] Regulated data (PHI, PII, PCI, MNPI) is out of scope, or covered by an approved agreement.
- [ ] A prohibited-data list has been published to all participants.

LEGAL & COMPLIANCE

- [ ] Applicable regimes are identified (e.g. HIPAA, GLBA, SOX, GDPR/UK GDPR, PCI-DSS, CCPA/CPRA, state AI laws).
- [ ] An AI Acceptable Use Policy has been issued and acknowledged by participants.
- [ ] Legal / compliance has reviewed and approved the use case.
- [ ] Record-retention and litigation-hold implications have been assessed.

VENDOR & TECHNICAL

- [ ] A vendor security and data-handling review is complete.
- [ ] Data-retention and training-use terms are understood (confirm no training on your data; confirm the retention window).
- [ ] Access is scoped to least privilege (role-based where available).
- [ ] An audit log / activity trail is available and retained.

PEOPLE & READINESS

- [ ] The pilot cohort is selected, with named participants.
- [ ] Baseline training is delivered before access is granted.
- [ ] An escalation and incident-reporting path is defined and communicated.

MEASUREMENT & EXIT

- [ ] Baseline metrics are captured before the pilot starts.
- [ ] Success KPIs are defined and instrumented.
- [ ] Explicit kill criteria are agreed — the conditions that end the pilot early.

LAUNCH GATE

Any unchecked item under **Data Boundaries** or **Legal & Compliance** is a stop. Resolve it before the pilot begins, not during review.

TOOL 02

Lightweight Use Case Risk Assessment

Score every candidate use case across five dimensions before it enters a pilot. This is an additive screen for triage — not a substitute for a formal risk assessment. Score each dimension 1 (low), 2 (moderate), or 3 (high) using the anchors below.

Dimension	1 — Low	2 — Moderate	3 — High
Data sensitivity	Public / non-sensitive internal data only	Confidential internal data; no regulated data	Regulated / restricted data (PHI, PII, PCI, MNPI, privileged)
Decision autonomy	Assistive drafting only; a human authors every output	Human reviews and approves before any action	System can act or trigger effects without per-item approval
Regulatory exposure	No regime materially implicated	One regime; established controls exist	Multiple regimes, or an area of active scrutiny
Reversibility / blast radius	Errors easily caught and reversed; internal only	Errors recoverable with effort	Hard to reverse, or reaches customers / regulators / public
External visibility	Internal tooling only	Informs customer-facing work but staff-gated	Reaches customers, claimants, patients, or the public directly

SCORE THE BAND (SUM OF THE FIVE)

Total	Band	Required governance posture
5–7	**Low**	Standard pilot governance. Eligible to proceed under the readiness checklist.
8–11	**Medium**	Elevated oversight: a named reviewer, QA sampling of outputs, and a mid-pilot governance review.
12–13	**High**	Senior governance approval before launch; mandatory human-in-the-loop; enhanced logging.
14–15	**Do not pilot**	Redesign to lower the data tier or autonomy, or route to a formal risk process outside the pilot track.

OVERRIDE RULE

Any use case that scores **3 on both Data sensitivity and Decision autonomy** is treated as **High** or above, regardless of its total. Sensitive data plus unsupervised action is the combination that hurts.

WORKSHEET

Use case	Data	Auton.	Reg.	Rev.	Vis.	Total	Band

TOOL 03

Governance Review Meeting Agenda

A ready-to-run structure for the body that oversees the pilot. Run it every two weeks while the pilot is active; move to monthly once it stabilizes. Target 60 minutes.

ATTENDEES (BY ROLE)

Executive sponsor (chair) · Compliance / Legal · Security / IT · Data owner(s) · Pilot lead · use-case owners as needed.

#	Item	Purpose	Time
1	**Prior actions & decisions**	Status of items carried from the last review.	5 min
2	**Risk register review**	New or changed risks; status of open mitigations.	10 min
3	**Use case intake & risk band**	Score new candidates; approve, condition, or decline.	10 min
4	**Data & compliance check**	Boundaries holding; any regulated-data exposure; policy exceptions.	10 min
5	**Incident & near-miss review**	What happened, root cause, corrective actions.	10 min
6	**Metrics & value review**	KPIs against baseline; progress toward success criteria.	5 min
7	**Decisions & approvals**	Go / no-go, scope changes, and the conditions attached.	5 min
8	**Actions & owners**	Assign every action with a named owner and due date.	5 min

CLOSE EVERY REVIEW WITH ONE QUESTION

“Has anything changed that would trip our kill criteria?” If the answer is yes and the pilot is still running, that is the decision to make in the room — not later.

TOOL 04

Data Boundary Quick Reference

A fast answer to the question that derails most pilots: *what is allowed to go into the AI tool?* Map your data to one of four tiers and apply the pilot rule. When a record could plausibly sit in two tiers, classify up — never down.

Tier	Typical examples	Pilot rule
T1 — Public	Marketing copy, published materials, open data.	**Permitted.**
T2 — Internal	Non-sensitive operational data, general internal documents.	**Permitted** with standard controls.
T3 — Confidential	Customer records, financials, contracts, non-public business data.	**Permitted only** with documented approval and access controls; review vendor retention terms first.
T4 — Restricted	PHI, full PII, payment-card data, material non-public information, privileged or legal-hold material.	**Prohibited** from pilot AI input unless explicitly covered by a legal / compliance-approved agreement. Default: do not input.

THE ONE RULE THAT PREVENTS MOST INCIDENTS

T4 / Restricted data does not enter a pilot AI tool by default. If someone believes an exception is justified, that is a decision for legal and compliance — in writing — before the data moves, not an individual judgment call.

How the four tools fit together. Classify the data (Tool 04), score the use case (Tool 02), clear the gate (Tool 01), then keep it honest in review (Tool 03). That sequence is the whole governance loop for a pilot, in one pass.

WHERE TO GO DEEPER

From a defensible pilot to an audit-ready rollout

This kit covers the pre-flight decisions. It does not include the full control library, regulatory crosswalks, weighted scoring model, or incident playbooks a regulated rollout needs. Each tool here has a fully developed counterpart:

- **Readiness Checklist** → **Cowork Pilot Playbook**
  full pilot charter, cohort design, and workflow catalog
- **Use Case Risk Assessment** → **Enterprise AI Governance Toolkit**
  weighted composite scoring, ISO/IEC 42001 crosswalk, ABA Model Rules, state-law mapping
- **Governance Review Agenda** → **Enterprise AI Governance Toolkit**
  the complete governance operating model and 32-control set
- **Data Boundary Reference** → **Data Classification Matrix**
  T1–T4 tiers with full usage mapping
- **(Not included here) Incidents** → **Incident Response Playbook**
  P1–P4 severity, scenario playbooks, regulator engagement

Explore the full suite **cahillnet.com**
Implementation guides, governance toolkits, and pilot playbooks for regulated industries.

Built from the frameworks Cahill Consultants uses in enterprise engagements across insurance, healthcare, and financial services.

© 2026 Cahill Consultants LLC, Provided for general information only and not legal or compliance advice. Validate against your own obligations.