Law Firm Implementation

CounselCore.ai Implementation Plan

A controlled, phased approach to introducing sovereign AI inside the firm.

Implementation Principle

CounselCore is introduced with the same discipline applied to document management, records retention, security, and other high-risk systems: defined scope, approved data, permission-aware access, measurable validation, and staged expansion.

The Approach

01 Assessment

Define the pilot, data boundary, permissions, and governance requirements.

02 Controlled Pilot

Deploy for a limited group and corpus, then validate security and usefulness.

03 Expansion

Extend only after review, approval, training, and an operating plan.

Prepared for CounselCore.ai Law Firm Briefings

July 2026

A Gated Path From Assessment to Responsible Expansion

The firm controls each decision point. Progress depends on security, governance, and user validation - not a predetermined rollout schedule.

01 Assessment

Purpose

Select a bounded use case and document the technical, legal, and governance requirements.

Core Work

Stakeholder Alignment
Data-Source Inventory
Permission and Ethical-Wall Mapping
Pilot Charter and Success Measures

Exit Gate **Approved Pilot Charter**

02 Controlled Pilot

Purpose

Operate CounselCore with limited users and approved data inside the agreed firm-controlled environment.

Core Work

Environment Configuration
Controlled Document Ingestion
Access-Control Validation
User Training and Structured Feedback

Exit Gate **Pilot Review and Governance Decision**

03 Expansion

Purpose

Extend use only after the firm confirms controls, outcomes, support ownership, and rollout sequencing.

Core Work

Outcome Review
Practice-Group Sequencing
Workflow Integration
Training, Support, and Review Cadence

Exit Gate **Approved Expansion Plan**

Controls That Apply Throughout

- **Firm-Controlled Environment** No unapproved external processing.
- **Least-Privilege Access** Existing permissions and ethical walls remain authoritative.
- **Source-Linked Outputs** Answers are reviewed against the underlying firm documents.
- **Auditable Use** Logging and review expectations are defined before the pilot.
- **Staged Approvals** The firm decides whether and how to proceed after each gate.

Phase 1

Assessment

Typical Range: 2-4 Weeks

Define the pilot boundary before any firm data is introduced.

Phase Goal

Create a shared, documented understanding of the use case, data, permissions, architecture, and success criteria.

Exit Gate

Approved Pilot Charter With Named Owners and Defined Controls.

Workstream	Firm Participants	Deliverable	Completion Signal
Executive Alignment and Pilot Objective	Managing partner; CIO; risk leader	Pilot Objective and Decision Structure	An executive sponsor, service owner, and decision group are named.
Use-Case Selection	Practice leaders; KM; pilot attorneys	One Bounded, High-Value Pilot Use Case	The task is repeatable, reviewable, and suitable for a limited pilot.
Data-Source Inventory	IT; KM; records management	Approved Source List and Data Boundary	Eligible repositories, matter types, and exclusions are documented.
Permissions and Ethical-Wall Mapping	Information security; general counsel; risk	Access-Control Requirements	Existing matter permissions and ethical walls are mapped to the pilot.
Deployment Architecture	CIO; infrastructure; security	Architecture Decision and Security Review	The firm approves the hosting, network, identity, logging, and backup model.
Pilot Charter and Success Measures	Steering group; pilot-user lead	Signed Pilot Charter	Scope, users, review duties, measures, timeline, and stop conditions are agreed.

Gate Principle The firm reviews the evidence and decides whether to proceed, revise the scope, or stop.

Phase 2

Controlled Pilot

Typical Range: 6-10 Weeks

Validate CounselCore with a limited corpus, defined users, and active governance oversight.

Phase Goal

Test the approved use case inside the firm-controlled environment while validating access, grounding, workflow fit, and support needs.

Exit Gate

Documented Pilot Review and Governance Decision.

Workstream	Firm Participants	Deliverable	Completion Signal
Environment Configuration	IT; infrastructure; security	Configured Pilot Environment	Identity, network, storage, logging, backup, and support access are verified.
Controlled Document Ingestion	KM; records; matter owners	Approved Pilot Corpus	Only authorized documents are indexed and traceable to their original source.
Permission Validation	Information security; risk; test users	Access-Control Test Record	Matter restrictions and ethical walls work for positive and negative test cases.
Grounding and Quality Validation	Pilot attorneys; KM; practice lead	Reviewed Test Set and Findings	Users can trace outputs to sources and identify limits or failure modes.
User Onboarding and Training	Pilot-user lead; learning team	Role-Based Pilot Training	Users understand permitted uses, verification duties, and escalation paths.
Monitoring and Structured Feedback	Service owner; pilot users; risk	Issue Log and Pilot Outcome Report	Security events, quality issues, workflow feedback, and remediations are documented.

Gate Principle The firm reviews the evidence and decides whether to proceed, revise the scope, or stop.

Phase 3

Expansion and Steady-State Operation

Extend access only after the pilot controls, outcomes, ownership, and support model have been reviewed and approved.

Workstream	Firm Participants	Deliverable	Completion Signal
Pilot Outcome Review	Steering group; pilot users	Documented Findings and Open Issues	The firm accepts the pilot findings and required remediations.
Governance Approval	General counsel; risk; security	Approved Use Policy and Control Set	Permitted uses, prohibited uses, logging, and escalation are documented.
Rollout Sequencing	Practice leaders; KM; IT	Practice-Group Expansion Plan	Eligible groups, data sets, and rollout order are approved.
Workflow Integration	IT; KM; records; security	Documented Operating Workflow	CounselCore fits approved systems, retention, and matter-management practices.
Training and Change Management	Practice leaders; learning team	Role-Based Training and Adoption Plan	Users understand permitted use, review duties, and escalation paths.
Operations and Support	Named service owner; help desk	Support Model and Review Cadence	Ownership, incident response, maintenance, and periodic review are assigned.

Evidence Required Before Expansion

- **Data Boundary** Approved information remained inside the agreed environment.
- **Traceability** Outputs could be reviewed against the underlying firm documents.
- **Operations** A named owner, support path, and review cadence were established.
- **Access Control** Users could reach only the matters and sources already authorized.
- **Governance** Permitted use, review responsibility, logging, and escalation were documented.
- **User Validation** Pilot users confirmed the workflow was useful for the approved use case.