

AI Vendor Due Diligence Checklist

A Practical Framework for Evaluating AI in Regulated Environments

Before you sign with an AI vendor, make sure you can answer these questions. The right AI vendor won't just impress you in a demo — they'll earn your trust through structure, restraint, and proof.

1. Architectural Design

- Is compliance logic governed by deterministic rules — and can the vendor explain where AI is used vs. policy-aligned workflows?
- Was the system built for compliance realities, or is it a general model with compliance language wrapped around it?

2. Auditability & Explainability

- Can every AI-assisted decision be fully reconstructed — with a trail of inputs, rules applied, and outputs?
- Could you answer a regulator's question about a specific AI-assisted decision made two years ago?

3. Disclosure & Content Integrity

- Does the system enforce approved disclosure language — or does AI generate, rewrite, or "improve" regulatory text? (Red flag if yes.)
- Is every disclosure decision logged, defensible, and traceable to its source?

4. Signal Quality & Supervision

- Does the system prioritize precision over volume — with measurable false positive reduction?
- Does the platform extend into communications supervision and internet monitoring — or end at content approval?

5. Operational Impact

- Does AI reduce manual workload without creating new model-tuning or validation obligations?
- Are efficiency gains measurable, repeatable, and documented — not just claimed?

6. Data Privacy & Firm Data Controls

- Is your firm's data fully segregated from model training — and can the vendor state which third-party model providers are involved?
- Would you be comfortable explaining this data flow to a regulator?

7. Post-Approval Visibility

- Does the platform connect compliance decisions to how content is actually distributed and used by advisors in the field?
- Does real-world usage data flow back upstream — or does the system go dark after approval?

8. Compliance Accountability

- Was this platform built by former CCOs and practitioners — or by AI researchers?
- How long has this vendor operated under regulatory scrutiny? Years of defensible outcomes — or promises?

The Bottom Line: A strong AI compliance platform earns trust through restraint, structure, and proof. The strongest connect compliance to supervision, distribution, and field intelligence — so firms move faster because they are safer, not in spite of it.

Red Oak — Move Faster. Stay Compliant. Grow AUM.

