IXSOR. RESOURCE / FRAMEWORK
ixsor.com/resources/frameworks/vendor-diligence-six-observation-framework · AI implementation for legal practitioners · Not legal advice

[RESOURCE / FRAMEWORK]

AI Vendor Diligence — the Six-Observation Framework.

An analytical structure for evaluating any AI vendor against ABA Model Rule 1.6 confidentiality requirements. Six observations applied to every vendor, scored as ACCEPTABLE / REQUIRES REDLINE / WALK-AWAY. Operationalises the AI vendor diligence catalogue and gives the firm a repeatable artifact for each procurement decision.

USE CASE: AI VENDOR EVALUATION; PROCUREMENT DECISIONS; RULE 1.6 CONFIDENTIALITY ASSESSMENT; MULTI-VENDOR COMPARISON

CATEGORY: PROCUREMENT & VENDOR DILIGENCE **TOOLS:** ANY AI VENDOR

READ THIS FIRST

IXSOR is not a law firm and this is not legal advice. This resource is a starting artifact you, the lawyer, customize and apply with judgment. Verify every assertion against primary sources. Cross-check against your jurisdiction's rules and your specific situation before relying on it. Full disclaimer below.

The framework

Apply this to every candidate vendor (or every analytical question of this type). Score each observation. Compare across instances. Document the result.

Download as PDF

COPY

```
AI VENDOR DILIGENCE FRAMEWORK
The Six-Observation Method
_____________________________________________

Vendor: _____________________________________
Tool / product: _____________________________
Tier evaluated: _____________________________
DPA executed?: [ ] Yes  [ ] No  [ ] Pending
Date of evaluation: _________________________
Evaluator: __________________________________

Each of the six observations is scored:
   A = ACCEPTABLE        (terms support Rule 1.6 / firm policy)
   R = REQUIRES REDLINE  (negotiable; track which clauses)
   W = WALK-AWAY         (do not contract on these terms)

═════════════════════════════════════════════
OBSERVATION 1 — TRAINING DATA RIGHTS
═════════════════════════════════════════════

The question: Can the vendor train its models on customer prompts and
outputs, or use them for "product improvement"?

What to look for:
   • Default training-on-prompts language
```

- Opt-out vs opt-in
- Whether the enterprise tier has different terms
- Whether the DPA explicitly carves out customer data

Acceptable:
- Explicit, affirmative no-training-on-customer-data clause
- DPA confirms the clause applies to all customer data
- Customer can audit / verify

Walk-away:
- Default training-on-prompts with opt-out only
- Vendor reserves "improvement" rights without definition
- No DPA available

Score: [A / R / W] Notes: _____

═══

OBSERVATION 2 — RETENTION WINDOWS

═══

The question: How long does the vendor retain prompts, outputs, conversations, metadata, and any derived data?

What to look for:
- Retention period (60 days? 1 year? indefinite?)
- Distinction between prompt history and metadata
- Soft-delete vs hard-delete
- Customer right to demand deletion

Acceptable:
- 30-90 day retention with customer-initiated deletion
- Hard delete confirmation
- Documented deletion mechanism

Walk-away:
- Indefinite retention
- "Soft delete only" / data persists in backups indefinitely
- Customer cannot trigger deletion

Score: [A / R / W] Notes: _____

```
═══════════════════════════════════════════════════
OBSERVATION 3 — SUB-PROCESSOR CHAIN
═══════════════════════════════════════════════════

The question: Who else, beyond the vendor, has access to customer data
in the course of providing the service?

What to look for:
   • Cloud infrastructure (AWS, GCP, Azure)
   • Underlying model providers (OpenAI, Anthropic, Google)
   • Support and customer-success tooling
   • Analytics providers
   • Where each is located (jurisdiction matters for GDPR / CCPA)

Acceptable:
   • Stable URL listing all sub-processors
   • Customer notice obligation before sub-processor changes
   • Customer right to object to a new sub-processor

Walk-away:
   • Sub-processor list not disclosed
   • Vendor reserves right to add sub-processors without notice
   • Sub-processors include parties whose terms are weaker than the
vendor's

Score: [ A / R / W ]    Notes: _____________________

═══════════════════════════════════════════════════
OBSERVATION 4 — GOVERNMENTAL DISCLOSURE
═══════════════════════════════════════════════════

The question: Under what circumstances will the vendor disclose
customer data to law enforcement, regulators, or governments?

What to look for:
   • Standard "we comply with legal process" language
   • Customer-notice obligation before disclosure (where legal)
   • Whether the vendor commits to challenge overly broad process
   • Any specific carve-outs

Acceptable:
```

- Customer-notice obligation where legally permissible
- Commitment to narrow / challenge overly broad process
- Annual transparency report

Walk-away:
- Discretionary disclosure under broadly drawn clauses
- No customer notice
- No commitment to challenge

Score: [A / R / W] Notes: _____

═══

OBSERVATION 5 — ANONYMISATION CLAIMS

═══

The question: Does the vendor claim to anonymise customer data, and does the anonymisation method actually work?

What to look for:
- Defined anonymisation method (k-anonymity, differential privacy)
- Whether anonymised data is treated as outside customer data
- Re-identification protections

Acceptable:
- Specific, documented anonymisation method
- Contractual commitment that anonymised data not be re-identified
- Anonymised data covered by the same protections as raw data

Walk-away:
- "Anonymised" means just stripping the customer name
- Anonymised data carved out of customer protections entirely
- Aggregation that reveals customer identity

Score: [A / R / W] Notes: _____

═══

OBSERVATION 6 — TIER DIFFERENTIATION

═══

The question: Are protections at the consumer / free tier the same as at the enterprise tier? What activates the better protections?

What to look for:

- Whether the customer is on the right tier
- DPA execution as the activator
- Marketing claims vs operative contract terms
- What happens if a user accidentally drops to a lower tier

Acceptable:

- Enterprise tier is clearly demarcated
- DPA execution is documented
- All users in the customer's organisation are at the protected tier
- No silent tier-flipping

Walk-away:

- Marketing claims about enterprise terms not in the contract
- Free / consumer tier comingled with enterprise tier
- DPA terms apply only to "designated" users (rather than all)

Score: [A / R / W] Notes: _____

═══

SUMMARY

═══

Total observations: 6
Acceptable (A): ___
Requires redline (R): ___
Walk-away (W): ___

Overall recommendation:

- [ ] PROCEED — all observations Acceptable
- [ ] PROCEED WITH REDLINES — Requires Redline issues addressed
- [ ] DO NOT PROCEED — one or more Walk-Away triggers
- [ ] DEFER — additional information required

Specific redline asks (if any):

1. _____
2. _____
3. _____

Walk-away triggers (if any):

```
1. _____________________________________________

Decision date: _____________________________________
Decision-maker: ____________________________________

This completed framework is filed with the firm's vendor-diligence
records as part of the procurement audit trail.
```

How to use it

INPUTS / FILL-INS

The vendor’s privacy policy AND data-protection addendum (DPA) for the tier you’re evaluating. Marketing materials are not sufficient; the operative contract terms are.

For incumbent vendors, also gather: any prior DPAs, communications about sub-processor changes, and the firm’s prior procurement notes on this vendor.

What you get

OUTPUT

A completed 6-observation evaluation with explicit scores and notes. Becomes a firm-internal procurement record retained per the firm’s vendor-diligence policy.

Verification — what the lawyer must do

- **Get the operative contract terms in writing.** Marketing claims do not count. The DPA, the privacy policy, and the master service agreement are the operative documents.
- **Compare across vendors.** The framework is most useful when applied to 2-3 candidates and the scores compared.
- **Document, file, and re-evaluate.** Re-evaluate at contract renewal or when the vendor announces material changes.

> **⚠ Risks and failure modes**
>
> - **Marketing-page risk:** Vendors' marketing pages overstate what their actual contracts deliver. Always evaluate against operative documents.
> - **Tier-flipping risk:** A vendor may quietly migrate users between tiers. Confirm in writing that all firm users are on the protected tier.
> - **Drift risk:** Vendor terms change. A vendor that scored Acceptable today may not score Acceptable next year. Re-evaluate at renewal.

Citations and further reading

- IXSOR: AI vendor diligence catalogue — the underlying analysis this framework operationalises.
- IXSOR: Legal Practice Management Software 2026 — worked examples applied to four PMS vendors.
- ABA Model Rule 1.6.
- ABA Formal Opinion 512.

- IXSOR Resources: AI Vendor Privacy Policy Analyzer — the prompt that runs Phase 1 of the framework against any vendor's privacy policy.

Source: https://ixsor.com/resources/frameworks/vendor-diligence-six-observation-framework · © 2026 Ixsor LLC · Free to use, attribution appreciated · This is not legal advice.

A note on using IXSOR Resources

These resources are educational tools written by a consultant, not legal advice from an attorney. **IXSOR is not a law firm and Dan Hughes is not licensed to practise law.** Using a template, checklist, framework, or prompt from this site does not create an attorney-client relationship and does not substitute for legal advice from a licensed attorney in your jurisdiction.

The resources are written to be useful in general; they cannot be tailored to your specific facts, jurisdiction, practice area, ethics regime, client circumstances, or matter posture. Differences in any of those can change the right answer materially.

If you use these resources in client work, you remain responsible for verifying their accuracy against primary sources, satisfying your duty of competence under Model Rule 1.1, meeting your duty of candor under Rule 3.3, protecting client confidences under Rule 1.6, and supervising any non-lawyer use under Rule 5.3. The *Mata v. Avianca* line of cases is a reminder that the lawyer who signs the document is the lawyer who answers for it.

Some uses of these resources can cause real damage if applied without judgment. Sanctions, malpractice claims, ethics complaints, breached confidentiality, and bar discipline have all followed AI use that the lawyer did not check carefully. **Consult your own ethics counsel for anything that matters.**

Resources are provided *as is*, without warranty of any kind, express or implied. To the extent permitted by law, IXSOR and Ixsor LLC disclaim liability for any damages

arising from your use of these resources.

If you find an error or have a correction, write to hello@ixsor.com and we will fix it.

SET IN	INTER · IBM PLEX MONO
REGISTERED	IXSOR LLC · NORTH CAROLINA · USA
JURIS.	50 STATES · DISTRICT OF COLUMBIA
ALIGNED	ABA MODEL RULES · FORMAL OP. 512 (2024) · TASK FORCE 2ND REPORT (DEC 2025)
NOT	A LAW FIRM · A VENDOR · A RETAINER
LEGAL	PRIVACY · TERMS · COOKIES · PRIVACY CHOICES
RIGHTS	© 2026 IXSOR LLC · ALL ARTIFACTS CLIENT-OWNED

IXSOR® / TERM 2026 · RALEIGH NC · USA / © IXSOR LLC
AI IMPLEMENTATION · FOR THE PRACTICE OF LAW