DocketTech

Hiring

Litigation IT Vetting Guide

How to evaluate eDiscovery vendors, trial technology providers, and courtroom AV specialists

- Key certifications and qualifications for litigation IT providers
- Security and compliance requirements (SOC 2, FedRAMP, encryption)
- 10 red flags that indicate an unreliable vendor
- Sample vetting questionnaire you can send to providers

Key Certifications & Qualifications

Litigation IT is an unregulated industry — there are no mandatory licenses or bar-equivalent certifications. This makes vetting critical. The certifications below are voluntary but signal demonstrated competency, security awareness, and professional commitment.

eDiscovery & Litigation Technology Certifications:

Certification	Issuing Body	Focus Area	Significance
ACEDS Certification	Association of Certified E-Discovery Specialists	eDiscovery processes, law, technology	Most recognized eDiscovery credential; ~3,000 holders
RCA (Relativity Certified Administrator)	Relativity	Relativity platform administration	Required for Relativity workspace management
Relativity Expert	Relativity	Advanced Relativity skills	Highest Relativity-specific credential
Everlaw Certifications	Everlaw	Reviewer, Admin, Litigation Support Manager	Platform-specific competency levels
CTTS (Certified Trial Technology Specialist)	LitPro Academy	Trial presentation technology	Focused on courtroom technology
Certified TrialDirector Trainer	IPRO	TrialDirector proficiency	Software-specific certification
LTC4 Core Competency	Legal Technology Core Competencies Certification Coalition	Legal technology fundamentals	Broad legal tech competency; industry standard for law firm training

Security & Compliance Certifications

Certification	What It Means	Why It Matters
SOC 2 Type II	Independent audit of security controls over 6-12 months	Required by most Am Law 200 firms for vendor selection

Certification	What It Means	Why It Matters
FedRAMP	Federal government cloud security authorization	Required for government litigation work
ISO 27001	International information security management standard	Demonstrates formalized security program
HIPAA Compliance	Health data privacy and security	Required when handling medical records in litigation
PCI DSS	Payment card data security	Relevant for financial fraud litigation
Encryption (AES-256)	Military-grade data encryption at rest and in transit	Baseline expectation for all litigation data

SOC 2 Type II is the minimum.

If your litigation IT vendor cannot produce a current SOC 2 Type II audit report, they have not submitted to independent security verification. For Am Law 200 firms, this is typically a hard requirement.

Security & Data Handling Requirements

Non-Negotiable Security Standards for Litigation Data

Checklist

- [ ] **SOC 2 Type II report** current (within 12 months)
- [ ] **Data encrypted at rest** (AES-256 minimum)
- [ ] **Data encrypted in transit** (TLS 1.2+ minimum)
- [ ] **Multi-factor authentication** enforced for all user accounts
- [ ] **Role-based access control** (RBAC) with audit logging
- [ ] **Data residency** — data stored in U.S. data centers (not offshore)
- [ ] **Right to audit** — client can request security documentation
- [ ] **Data destruction** — documented process for end-of-matter data deletion
- [ ] **Incident response plan** — documented procedure with notification timeline
- [ ] **Background checks** — all staff with data access have passed criminal background screening
- [ ] **Cyber liability insurance** — minimum $5M coverage
- [ ] **Business continuity / disaster recovery** — documented plan with tested RPO/RTO

> **Privilege and work product data cannot be hosted offshore or on unvetted infrastructure.**
>
> If your vendor subcontracts hosting to a third party, verify that the subcontractor meets the same security standards.

How to Verify Vendor Qualifications

Step-by-step verification process

Request the vendor's SOC 2 Type II audit report. Review the auditor's opinion letter and any exceptions noted. If the vendor has never completed a SOC 2 audit, this is a significant concern.

Verify platform certifications. For Relativity partners, check the Relativity partner directory. For ACEDS-certified individuals, search the ACEDS directory.

Request case references — specifically from cases of similar size and complexity. Ask references about: data security, responsiveness, cost accuracy vs. estimates, and courtroom performance.

Conduct a data security questionnaire. Most Am Law 200 firms have standardized vendor security assessments. If you don't have one, use the Shared Assessments Standardized Information Gathering (SIG) questionnaire.

Review the vendor's standard MSA (Master Service Agreement) and SOW (Statement of Work) templates. Key terms to verify:

- [ ] Data ownership clause (client owns all data)
- [ ] Data destruction timeline (within 30 days of matter close)
- [ ] Liability cap (should cover potential breach costs)
- [ ] Subcontractor disclosure (must list all third-party services used)
- [ ] Pricing escalation protections (rates locked for engagement duration)

Ask for a technology demonstration. For trial technology providers, request a mock presentation using sample exhibits. For eDiscovery vendors, request a platform walkthrough with your specific use case.

10 Red Flags of an Unreliable Litigation IT Vendor

1. **No SOC 2 Type II report.**
   If the vendor has never undergone an independent security audit, you have no assurance that client data is properly protected. For litigation data, this is disqualifying.

2. **Cannot explain their pricing model clearly.**
   If the vendor can't provide a clear, written explanation of per-GB, per-user, and per-project costs — with no hidden fees — their invoices will surprise you.

3. **No litigation-specific experience.**
   IT companies that primarily serve non-legal clients (healthcare, retail, finance) lack familiarity with privilege review, production protocols, and courtroom technology requirements.

4. **Single point of failure (one-person shop for critical trial tech).**
   If your hot seat operator gets sick the morning of trial, who's the backup? Ensure the vendor has redundancy for mission-critical roles.

5. **Offshore data processing without disclosure.**
   If your litigation data is being processed in India, the Philippines, or Eastern Europe without your knowledge and consent, the vendor is violating basic security trust.

6. **No data destruction policy.**
   After matter close, client data must be destroyed per agreed-upon timelines. A vendor without a documented destruction process may retain your data indefinitely.

7. **Legacy technology only.**
   Vendors still running on-premise Relativity Server (not RelativityOne), using outdated TrialDirector versions, or lacking AI review capabilities are behind the market.

8. **No backup or redundancy for trial.**
   Trial technology requires backup equipment — a second laptop, backup hard drive, and backup internet connection. A vendor who arrives with one laptop and no backups is gambling with your trial.

9 **Poor communication and responsiveness.**
During trial, issues arise at 6 AM and 10 PM. If the vendor is unreachable outside 9-5 business hours, they are not trial-ready.

10 **Cost estimates consistently wrong.**
If references report that actual costs regularly exceeded estimates by 30%+, the vendor is either incompetent at scoping or deliberately lowballing.

eDiscovery Vendor Selection Decision Matrix

Two-column layout

HIRE A FULL-SERVICE eDiscovery VENDOR WHEN

- Case involves 50+ GB of data across multiple custodians
- Cross-border data collection (GDPR, data privacy issues)
- Government investigation or regulatory matter
- Multi-party litigation requiring complex production protocols
- Your firm lacks in-house litigation support staff
- Privileged data requires managed review with detailed logging

SELF-SERVICE PLATFORM SUFFICIENT WHEN

- Case involves < 25 GB of data
- Single-custodian or limited data sources
- Firm has trained litigation support staff
- Budget-conscious cases where vendor management overhead is prohibitive
- Even here: ensure the platform has SOC 2 certification and proper encryption

Vendor Type Comparison

Factor	Full-Service Vendor	Self-Service Platform	In-House Team
Cost (per-GB equivalent)	$25–$75/GB	$5–$25/GB	$3–$10/GB (platform cost only)
Project management	Included	Self-managed	Self-managed
Security oversight	Vendor-managed + SOC 2	Platform SOC 2 only	Firm IT manages
Scalability	High — vendor handles surges	Limited by subscription	Limited by staff
Best for	Complex, large, high-stakes	Mid-size, routine	Firms with existing lit support

Sample Vetting Questionnaire

Litigation IT Vendor Vetting Questionnaire — Send This Before Hiring

Copy and send these questions to any eDiscovery vendor, trial technology provider, or courtroom AV specialist you're considering.

1. Security & Compliance

- Do you have a current SOC 2 Type II audit report? Can we review it?
- Where is client data physically stored? (Data center locations)
- Do you use any offshore subcontractors for data processing or review?
- What is your data encryption standard (at rest and in transit)?
- What is your incident response plan? What is your breach notification timeline?
- Do you carry cyber liability insurance? What are your policy limits?

2. Certifications & Qualifications

- What certifications do your team members hold (ACEDS, RCA, Relativity Expert, CTTS)?
- How many years has your firm been providing litigation technology services?
- How many trials has your team supported in the past 12 months?
- What eDiscovery platforms do you support (Relativity, Everlaw, DISCO, Nuix)?

3. Trial Technology Capabilities

- What courtroom presentation software do you use (TrialDirector, OnCue, Sanction)?
- Do you provide backup equipment for all trial technology?
- What is your plan if the primary hot seat operator is unavailable?
- Can you support remote/hybrid trial proceedings?
- Do you offer war room setup and support?

4. Pricing & Terms

- Can you provide an all-inclusive per-GB rate for eDiscovery (processing + hosting + AI review)?
- What is your hot seat operator daily rate? What does it include?
- What are your after-hours / overtime rates during trial?
- Do you charge for courtroom site surveys?
- What is your cancellation/postponement policy?

5. References & Track Record

- Can you provide 3 attorney references from trials in the past 12 months?
- Can you provide references from cases of similar size and complexity?
- What is your average cost variance (estimated vs. actual)?

DocketTech

DocketTech

The most comprehensive directory of litigation IT providers in the United States

Search providers at dockettech.com