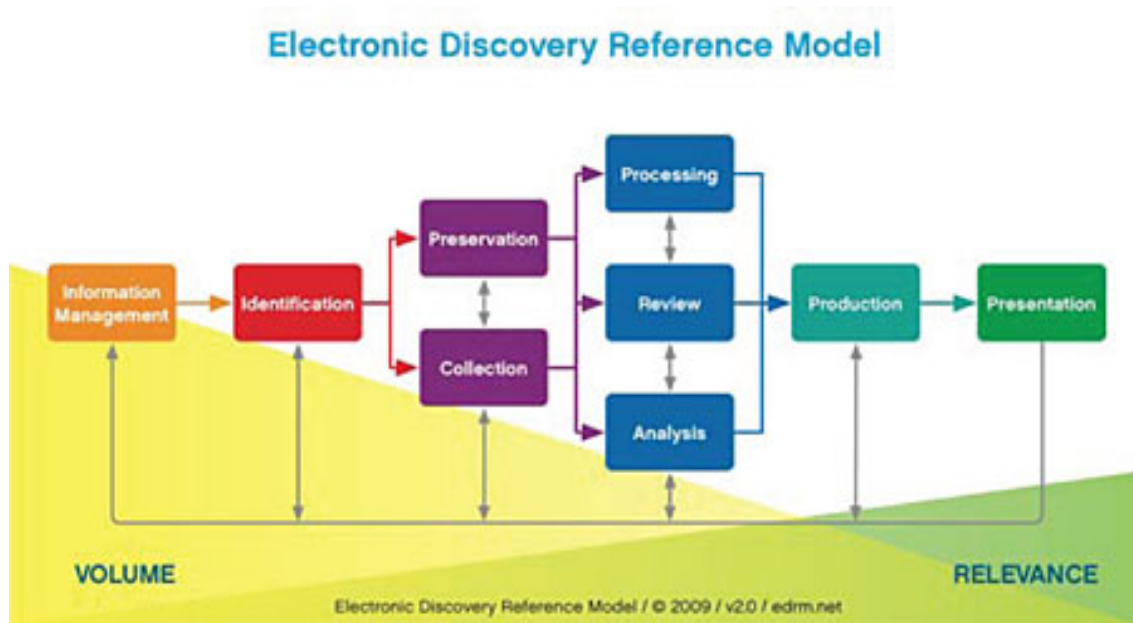


I. Some Key Considerations In Whether To Engage An E-Discovery Vendor (Or Vendors)

- A. It is difficult to decide whether to retain a vendor if you don't know what *your* organization can do and at what cost.
- B. Know your organization's E-Discovery capabilities "now" and *keep your knowledge current*.
- C. Know your capabilities in specific relation to the various components of the *Electronic Discovery Reference Model* ("EDRM") (subcomponents not shown below, but important).



See: <http://www.edrm.net>

- D. For example, has your organization purchased (and obtained necessary training and certifications, where available) to use certain E-Discovery tools (e.g., EnCase® Forensic)? Are they trained and knowledgeable in ESI chain-of-custody procedures?
- E. Do your IT personnel have time to *focus* on E-Discovery issues?
- F. Are your IT personnel likely to be good or bad witnesses if their depositions are taken? If key IT personnel are not experienced in defending their work in litigation, that is a reason to seek out an outside vendor.

- G. What is the exposure potential in the litigation? (“Proportionality” concept)
- H. Is “inaccessible” ESI potentially subject to discovery?
- I. Are your in-house personnel experienced in E-Discovery “*project management*” and project tracking? Is the potential magnitude of the ESI and the litigation exposure large enough to make project management and tracking a substantial undertaking?
- J. Can *agreements* be reached with opposing counsel (particularly early in case) that may eliminate need for an E-Discovery vendor or some vendor services (e.g., agreements on simple formats for production of ESI, agreed “keyword” searching, and types of metadata, if any, to be produced)?
- K. Is the volume of likely ESI beyond the capacity of in-house E-Discovery tools (if any)?
- L. Will “legacy” ESI be the subject of discovery? If so, do you have the necessary software to read and process it? If not, you will potentially need a vendor with that capability.
- M. Will forensically defensible ESI capture be necessary? If so, do you have properly trained IT personnel? Do you have appropriate electronic tools? (See ¶ 4 above)
- N. Will metadata be important? If so, do you have personnel in-house who know how to capture ESI without altering metadata?
- O. Will electronic searches be used (or potentially advisable) to identify and cull ESI? If so, is the nature of the ESI and the issues that must be translated into search terms such that sophisticated search software (including conceptual searching) is advisable? Are additional areas of subject matter expertise needed for defensible searches (e.g., statistics, linguistics)?
- P. Are there identifiable, material potential advantages to having an “independent” (vendor) witness ready to testify to all or parts of ESI collection, processing and production process?
1. The more the issues are opinions, rather than historic fact, the more potentially important an independent vendor witness may be, versus an in-house IT witness.
 2. The more “aggressive” opposing counsel is, the more important an independent witness may be.
 3. The more ESI-sophisticated opposing counsel and their E-Discovery consultant (if any) are may be relevant to whether you should engage an E- Discovery vendor.
- Q. Is the nature of ESI you anticipate seeking *from* the opposing party such that you will need expertise you do not have to determine in what format and how you should request it to be sure you can use it? (e.g., database information).
- R. Are there gaps in the E-Discovery expertise in litigation counsel that could be materially bolstered by a vendor?

S. Is your in-house and outside litigation team big enough to warrant the inclusion of ESI in a case management database that is accessible from several locations? If so, that consideration may weigh in favor of an outside vendor who will have those capabilities.

T. Is the format of production likely to be native format? If so, a native format production may be best handled by an outside vendor who can clone hard drives or servers and easily produce native format files. In-house operations are not usually proficient in this type of production.

U. Map out the potential sources of ESI in your organization that could be relevant to the litigation. The more sources that are identified, the more likely that an outside vendor should be retained.

II. **Some Key Considerations In Selecting An E-Discovery Vendor (Or Vendors)**

A. Vendor Background

1. Gather information about the company

a. Factors to consider

- i. Years in business
- ii. Track record of providing product or service
- iii. Check client references and court opinions involving vendors

b. Company obligations/warranties

- i. Insurance and licenses
- ii. Privilege issues
- iii. Confidentiality guarantees
- iv. Pricing methods

1. Number of options for processing ESI for review and production can make it difficult to compare proposals.
2. Majority of ESI was traditionally converted to TIFF or PDF for review and production.
3. More prevalent for vendors to allow review in native format.
4. Prior predominance of conversion to image led to a pricing system based on a per-page basis.
5. Cost of conversion represented a significant portion of overall cost.
6. More data is being reviewed in native format so pricing is moving toward volume- or gigabyte-based pricing.
7. Any steps to reduce amount of data to be produced will reduce the cost of the project.

2. Gather information about the personnel

- a. Experience level
- b. Screening of employees?
- c. Ability to guarantee work by a specific date
- d. Will the vendor need to hire inexperienced staff to complete the project?

3. Project Security

- a. Vendor should describe what is done to ensure that a document has not been changed.
- b. Amenability of Escrow— For large projects, inquire about the ability to escrow software code, instruction manuals, and documentation to guard against the vendor's financial instability.
- c. Chain of custody issues
- d. Vendor should confirm that a complete, exact copy of the data is stored.
- e. What happens when a project is over? What happens to electronic and hardcopy data?
- f. What happens if the vendor is acquired or files for bankruptcy?
- g. Security of data from hackers and viruses
- h. Is the information appropriately stored?
- i. Consider building safety and security

4. Discuss subcontracting issues

- a. Establish a process for disclosure and approval of subcontracts.
- b. Vendor and subcontractor should certify that they are free of conflicts.
- c. Subcontractors should be held to same security standards as vendor.

5. Conflicts issues

- a. Vendors may be privy to confidential information about the client's information management system.
- b. Important to ensure no conflicts from the outset.
- c. Ensure that a conflicts check is performed on any subcontractor.
- d. Watch for business conflicts—vendor may have previously been retained by a competitor of the client.
- e. Apply conflicts rules that apply to lawyers to potential vendors.

B. Determine the types of services needed

1. Types of services

- a. Consulting/Professional services
 - i. testimony
 - ii. analysis of IT infrastructure
 - iii. recommendation of discovery plan

b. Data Collection/Processing

- i. data/file management
- ii. data harvesting
- iii. data filtering
- iv. e-mail processing
- v. redaction

c. Data Recovery/Forensics

- i. Legacy data restoration
- ii. Backup systems/enterprise backup
- iii. Reverse engineering
- iv. Damaged media
- v. Password protected files

d. Hosting/Review/Production/Delivery

- i. Data/website hosting
- ii. Review/support
- iii. Production

e. Litigation Support

- i. Scanning/copying/OCRing
- ii. Coding
- iii. Conceptual organization

2. Identifying Specific Vendors

- a. Request for Information should lead to identification of group of vendors
- b. Request for project proposals to smaller group of vendors
- c. Items to consider in RFP
 - i. Project Overview— Define the problem, the number and type of information resources, the systems on which the information resides, timeliness, scope, relevancy, and court orders.
 - ii. Management— Explain role of client, counsel and staff in the management of the work; explain lines of communication and procedures for status reporting.
 - iii. Requirements Description— Describe for vendor the technical requirements, specific services, volume, time constraints, and required quality.
 - iv. Vendor Process and Infrastructure— Ask vendor to describe how the project will be completed. How will surprises be handled?
 - v. Processing Methods

- vi. Quality Control— Will the vendor institute any quality control measures for the project?
- vii. Recommendations from previous clients

C. New Developments

1. Certification Programs

- a. Many vendors are becoming certified in different protocol.
- b. No process in place for certifying the certification programs.
- c. Some programs are fairly limited

2. Online Repositories

- a. Store electronic versions of documents on the Internet
- b. Remote access
- c. Costs starting to go down
- d. Per gigabyte data and processing load fee and monthly fee
- e. Remote searches

3. Records Management

- a. Retention policies are the cornerstone of defensible preservation and collection methods.
- b. Question the vendor as to whether their protocol complies with the enterprise's records management and retention policies.

4. Meet and Confer Requirement—Rule 26(f)—include vendors?

- a. Rule 26(f) directs parties to discuss ESI discovery during discovery planning conference
- b. Consider: capabilities of computer systems used by the parties, forms in which ESI could be produced, whether the information is accessible, preservation of ESI, and how claims of privilege and work product will be addressed
- c. Rule 26(f) implies that the conference should be attended by persons from the law firm, client, or electronic discovery vendor (maybe all three) to ensure that necessary information is exchanged