

This article was published online or in print in the following publications:

Sarbanes-Oxley
COMPLIANCE JOURNAL

NETWORKWORLD eWEEK.COM

WindowsITPro
We're in IT with You

TechRepublic

EVIDENCE FOR HEALTH INFORMATION
EXECUTIVES

10 Things You Should Look for in an In-house eDiscovery Solution

By Ursula Talley

If you work for a mid- to large-size company — say, one with more than \$500M in revenue — you probably are familiar with the problems of eDiscovery. Your enterprise may routinely face five or more litigation matters each year, and you have terabytes of unstructured information that you need to sort through in order to find relevant information and place it on litigation hold.

Worse, that unstructured information is growing dramatically: at a rate of up to 80 percent a year in many enterprises. Unmanaged and unplanned-for eDiscovery tasks increase both risk and headaches for legal, IT, and business unit organizations. Outsourcing eDiscovery to litigation services firms makes sense if you don't have much data or rarely face litigation, but it doesn't make good financial sense as your organization grows. That's particularly true if you work in highly regulated and litigation prone industries such as banking, insurance, energy, or utilities.

Here are 10 tips for choosing an eDiscovery solution that can get up and running quickly, solve the problems you need it to, and pay for itself within months.

1. Make sure your solution covers a broad range of eDiscovery processes as defined by the industry's EDRM (Electronic Discovery Reference Model) standard. Your solution needs to cover everything from information management, identification, preservation, and collection to processing and early case analysis — handing over only the smallest legally defensible set of data to the legal review team. Otherwise, you'll have to cobble together multiple solutions from multiple vendors and create a bigger headache for yourself. Not to mention the compromised audit liability point solutions present.
2. Insist on an open integration platform that supports various email systems, storage systems, archiving systems, and content and document management systems. If you're in the process of migrating data from a Novell server to an EMC Celerra or vice versa, for instance, you'll need something that can read files from both. Your solution should be able to read data from shared file servers, desktops, and laptops, including Macs and PCs, from content management systems such as Microsoft SharePoint and EMC Documentum, as well as from storage systems including EMC Centera, NetAPP, Hitachi, and IBM.

3. Ensure that when you implement your solution, you can execute without impacting employee productivity. Flexible job scheduling allows processing to occur after hours when employees aren't around, and it's essential to be able to perform litigation hold without disrupting the production environment of your knowledge workers.
4. When locking down documents for litigation hold, be sure your system works in conjunction with existing corporate records management policies so you are coordinated with ongoing IT data management functions, such as data backup, migration, and file expiration/deletion. Implementing an effective litigation hold strategy requires close coordination with your corporate records management policies so that documents responsive to an active legal matter are not inadvertently deleted.
5. Be sure you can create a data topology map that identifies electronically stored information by a full complement of variables, including system location, custodian, access time, size, and content type. It's critical to be able to perform pre-discovery profiling of data so you can manage it, know your liability, and quickly respond to legal requests.
6. Your solution will need to make available all relevant and responsive electronically stored information to legal, HR, or audit teams prior to the completion of the collection process. Even while collection and preservation are ongoing, you should be able to call up what's saved, what's indexed, and what's relevant information today.
7. Your solution should be able to interact with electronically stored information without changing the data. It's critical to preserve the integrity of existing data. Don't let your software alter document properties when copying or moving it, because those properties themselves are important to maintain legal defensibility.
8. Check to see if your prospective solution can execute forensically sound collection policies while providing defensible and comprehensive audit logs. These audit trails show where data originally resided, what search terms were applied to collect it, and when copies were made. Attaching unique digital signatures to files before and after they are collected proves that none of the actions performed altered the original content.
9. Your solution needs to provide rich and sophisticated search capabilities. Are you able to search and identify terms and natural language concepts within files, as well as within emails and their attachments? Besides being able to search on common metadata and simple text strings, are you able to perform sophisticated natural language-based searches that can differentiate between Will, the name, or will, the legal document or will, the auxiliary verb? Accuracy provides the smallest legally defensible set of data to be reviewed by the legal team — significantly reducing eDiscovery time and cost.
10. Be sure your solution is easy to deploy and maintain. If you have to spend weeks or months getting a system working before it can even begin accessing, categorizing, and reporting on information, you're at a huge disadvantage. Ideally, look for a self-

contained, out-of-the-box appliance combining hardware, software, and storage, that can provide results back to you within 24 hours.

Bringing eDiscovery in-house is a big step. Many organizations find that in doing it, they're able to save themselves hundreds of thousands of dollars, dramatically reduce the time taken to respond to legal requests, and better organize their own internal processes and data storage. But finding the right solution is key. An incomplete solution that addresses only part of your needs and responds only to yesterday's list of legal requirements is bound to cause more headaches. Take the time for thorough evaluation, and make your decision carefully. You'll be glad you did.

Ursula Talley is vice president of marketing for StoredIQ, a leading provider of enterprise-class Intelligent Information Management solutions that enable organizations to gain visibility and control over business-critical information in order to meet compliance, governance, and legal discovery requirements.