



**White Paper**

**An IT Perspective: What Legal Wants**

**...and Seven Things IT Can Do To Meet Legal's  
Needs**

Sponsored by:



**Note:** *Legal information is not legal advice. Contoural provides information pertaining to business, compliance, and litigation trends and issues for educational and planning purposes. Contoural and its consultants do not provide legal advice. Readers should consult with competent legal counsel.*

## Introduction

Nearly all companies in the course of regular business activities become the target of lawsuits. These vary from common lawsuits, such as employee wrongful termination, to major litigation, such as class action lawsuits. Likewise, companies themselves initiate litigation. Litigation always has been, and will continue to be, a reality of doing business. What is changing, however, is the nature of litigation discovery, its focus on electronic documents and how this impacts IT. New rules are changing how quickly companies have to discover information, increasing the risks for those that are not prepared.

The explosion of electronic documents, along with new regulations, new trends in litigation discovery and how end users handle documents are forcing organizations to re-think their document retention and discovery strategies. According to a recent study from UC Berkeley, more than 96% of all information in an enterprise is in digital format, and even 70% of all paper documents are copies of electronic documents. They are so important that once a lawsuit or investigation has commenced (or is reasonably foreseeable), the failure to retain relevant electronic documents can lead to disastrous consequences: the loss of the lawsuit, monetary or criminal liability for management or the company, and even the death of the business.

These newer trends in discovery are having a great impact on IT. Once an occasional occurrence, discovery is now commonplace with Legal departments making frequent demands on IT organizations. For organizations that are not prepared, the costs of producing electronically stored information, including e-mail and files can be disruptive, expensive and time consuming. For companies that cannot find their information fast enough – the results can be disastrous.

In this new environment of electronic document-focused discovery, instead of waiting for discovery requests to happen, IT organizations are better off anticipating, understanding and preparing for Legal's needs. Working closely together, Legal and IT can develop policies and strategies to become litigation ready. This proactive approach leads to less disruption, more defensible discovery and lower costs.

## Legal Thinks In Terms of Documents

Before the computer age, most non-verbal communications took place or were memorialized on paper. Even with computers, most files can be printed on paper to create a written, readable type of document. Many in IT don't consider an electronic document "official" unless it is classified as such. The law takes a different view. It regards information stored in electronic form as a "document". This means that in a lawsuit, electronic information is subject to discovery – that is, copying by the adverse party – exactly the same as pieces of paper, usually even if the information also is printed in paper form.

Furthermore, IT often views information in terms of data and storage that data resides on. Legal's view is different. It looks at information in terms of documents, which may be saved on different types of media. When a business is involved in a lawsuit or a regulatory request, many types of electronically stored information (often abbreviated as 'ESI') are considered discoverable documents. (See box below).

Ultimately, any information stored in an electronic medium may be a discoverable electronic document.

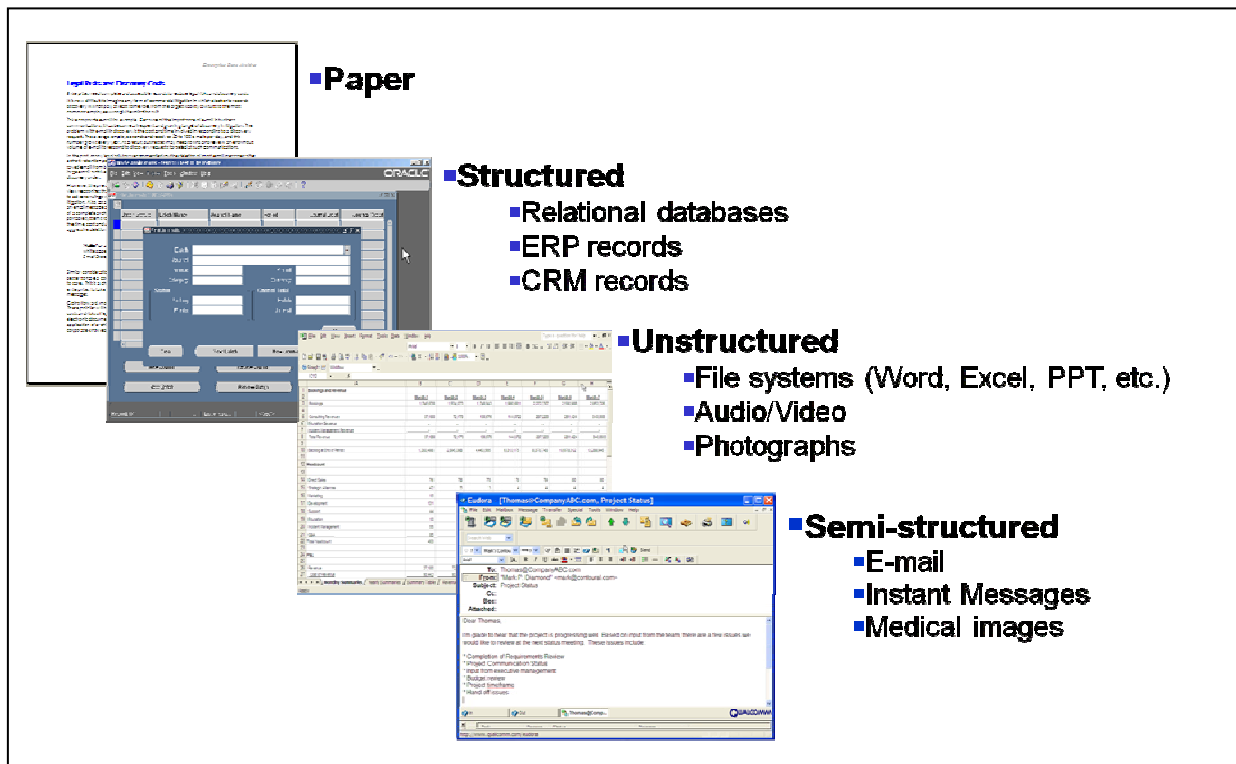


Figure 1. Document Media Types. Documents can be classified into four different media types. Courts are concerned about content, not the type of media of the document.

The impact on IT is clear. The majority of documents are electronic documents. Although IT may consider only some documents as “official” records, the court views all ESI as fair game for discovery. Electronic documents carry the same weight in the eyes of the court as paper documents. IT has become the de facto custodian of much of the organization’s documents.

### What is Driving Legal: Discovery and Now the Amended FRCP

Discovery is the process in which both parties in a lawsuit *discover* relevant information concerning a case. Ordered by the court typically during the initial phases of a lawsuit, discovery can be required for both the plaintiff and the defendant. A business that receives a discovery request that calls for the production of electronic and other documents is under a duty to make a reasonable effort to search its records for responsive communications. Historically, discovery has been focused on finding all paper documents relevant to the case. However, during the past ten years, reflecting the increased use of electronic communications, we have seen a significant shift in focus of discovery efforts to electronically stored information. Litigators have learned that

email and data files can contain significant evidence relevant to a lawsuit. These litigators target these electronic documents first in their discovery efforts.

Since nearly every lawsuit involves discovery, and nearly every discovery focuses on electronic documents, IT organizations need to work closely with their Legal departments. Also, as (unfortunately) litigation tends to be fairly common, IT organizations can be expected to be called into discovery efforts regularly.

“Spoliation” is the term used by courts to describe the improper destruction of evidence, including email and messages. Companies are guilty of spoliation if they destroy evidence (e.g., company records) relevant to litigation with the purpose or intent of preventing the other party from using the evidence against them. Spoliation can occur both through a conscious decision (someone shreds documents knowing they are relevant to a case) or through not following the right processes (as will be discussed below). Unfortunately, spoliation is not only a case of someone consciously deciding to delete evidence. Increasingly, many cases of spoliation occur through *inactivity* to prevent the destruction of email. This includes failure to stop backup tape rotation, reformatting the laptop from a former employee for a new employee, and deleting old email. Routine electronic document deletion programs must be halted immediately when a business learns there is a reasonable probability of a lawsuit or government investigation. There is an unfortunately long list of *former* CIO's who failed to enact effective hold processes, thus exposing their companies to charges of spoliation.

Recent changes have made discovery in some areas easier and in other areas more difficult for IT. The Federal Rules of Civil Procedure (FRCP) are a body of rules focused on governing court procedures for managing civil suits in the United States district courts. While the United States Supreme Court is responsible for promulgating the FRCP, the United States Congress must approve these rules and any changes made to them. A number of important and substantive revisions to the FRCP went into effect on December 1, 2006. These changes represented several years of debate at various levels and will have a significant impact on electronic discovery and the management of electronic data within organizations that operate in the United States. In a nutshell, the changes to the FRCP require organizations to manage their data in such a way that this data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings. IT needs to be aware of some of the changes to the rules.

The changes reflect the reality that discovery of email and other ESI is now a routine, yet critical, aspect of every litigated case. First, the amendments treat ESI differently. Second, they require early discussion of and attention to electronic discovery. Third, they address inadvertent production of privileged or protected materials. Fourth, they encourage a two-tiered approach to discovery – deal with reasonably accessible information and then later with inaccessible data. Finally, they provide a safe harbor from sanctions by imposing a good faith requirement.

Unlike many data retention requirements in specific industries, such as those imposed upon broker-dealers by the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD), the FRCP apply to virtually all organizations in all industries. If an organization can have a civil lawsuit filed against it, then the FRCP should figure prominently into that organization's data management strategy. Obviously, all cases brought after December 1, 2006 will be subject to the new FRCP amendments. However, the Supreme Court has determined that cases filed prior

to this date could be subject to the FRCP if a court determines that undue delay or burden to the parties involved<sup>1</sup> will not be imposed by adherence to the new rules. Many states use the Federal Rules as a model for updating their own rules. We are already seeing changes in many states' civil procedures to become consistent with the FRCP.

### **Important Sections of Amended Federal Rules Impacting IT**

#### **Rule 26(f) – Meet and Confer**

Within 100 days of a suit being filed, the amendment requires the parties to meet and disclose any issues relating to disclosure or discovery of ESI, including form of production, preservation, and privilege/protection issues. This includes the names, types and locations of documents used to support claims. Previously, each side had months, quarters or in some cases years to produce documents. Under these new rules, you must provide the other side with a list of your documents very quickly.

#### **Rule 26(b)(2) – Inaccessible Information**

The amendment clarifies the obligations of a responding party to provide discovery of ESI that is not reasonably accessible (deleted information, information kept on some backup tape systems, and legacy data from systems no longer in use). This portion is good news for IT, as it provides limited relief from having to look at documents at inaccessible locations, and if the other side presses this discovery, the courts may allow "cost shifting" by having the requesting party pay for discovery in inaccessible locations.

#### **Rule 34 Production of Documents**

ESI in Rule 34 authorizes the requesting party to specify the form of production. The requesting party may request documents to be submitted in "native" format. Paper copies of e-mail, for example, may not be sufficient. IT needs to be ready to provide source copies of electronic documents.

#### **Rule 37 – Safe Harbor**

The amendment creates a "safe harbor" that protects a party from sanctions for failing to provide electronically stored information lost because of the routine, good-faith operation of the party's computer system. The court recognizes the need for companies to delete data as an ongoing part of doing business – so long as that data is not reasonably anticipated to be part of litigation.

Perhaps the greatest impact of the FRCP on IT organizations is the Rule 26(f) – Meet and Confer. As this conference happens within 100 days, the actual time for IT to discover all relevant ESI is much less. Within 100 days, IT must find the information, provide it to in-house counsel, in-house counsel typically needs time to review, and then it is passed onto outside counsel, who also needs time to review it. IT often has a matter of weeks to produce this information, and IT often receives tremendous pressure from Legal to produce it quickly.

Finally, all parties in all lawsuits have the responsibility to comply with civil procedures. The burdens are the same regardless of the size of the company. Courts realize that small companies often do not have the same resources as larger companies, but nor do they have as much ESI. Therefore claiming "we are small and therefore did not expect to be held to this standard" is not only foolish, but may set the stage for sanctions by the court for failing to comply.

---

<sup>1</sup> <http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf>

In summary, to meet Legal's needs, IT needs to understand this new world of litigation-driven focus on electronically stored information.

### Effective Litigation Hold and Discovery Processes

The duty to save starts when the lawsuit is "reasonably anticipated." The courts have ruled that duty to preserve documents relevant to litigation begins when companies "knew or should have known" that they are entering litigation. (See box below.) At such a time that they enter or have a reasonable belief they will enter litigation companies should enact a litigation hold, ensuring that all documents relevant to the litigation will be preserved. Legal departments will expect their IT organizations to be able to preserve electronic documents effectively, and be able to locate and retrieve documents quickly.

#### Zubulake vs. UBS Warburg – the 'Gold Standard' for ESI Legal Discovery

The duty to save starts when the lawsuit is "reasonably anticipated". In a 2004 wrongful termination case, for example, an employee filed a claim well after leaving the company. However, the company got in significant trouble with the court for not saving the employee's emails soon after her departure. The court ruled that although the plaintiff did not file her discrimination charge until August 2001, by April 2001, "almost everyone associated with [the plaintiff] recognized the possibility that she might sue," and, hence, negligent destruction after that date by the defendant corporation resulted in sanctions. This obligation to save also applies to regulatory and grand jury investigations. If someone in a company believes that the company will face litigation on an issue, there is an immediate obligation to begin preserving all messages related to that matter.

Good litigation hold processes require close cooperation between Legal and IT. Needless to say, it behooves companies to set up effective litigation hold processes prior to litigation occurring. Good litigation hold processes include the following:

- Determine responsible department and or individual – usually Legal
- How will you communicate a hold action
- Employee acknowledgements of litigation hold
- Date issued
- Scope of the order
- Types of records and any specific content covered
- Locations under hold including potentially employee home workstations
- Employees covered by the notice
- Time frame covered
- Reason for the order

One common refrain we hear from clients is that even though they may have discoverable messages in many different places, it is unlikely that an opponent's attorneys would know where to look. This is where depositions are playing an

important role. Increasingly, we are seeing message administrators and others in IT being called as witnesses in depositions. They are being asked questions such as: “Does the company allow users to save email on the laptops? Do you know any users who do so?” “How many years of backup tapes do you have?” Even if the company has a policy that all email older than sixty days should be deleted, for example, if during the discovery process the opposing party can establish that even a few users saved email on their systems, there is basis to expand the discovery request to all laptops in the organization. We are seeing increasing sophistication in asking the revealing questions in discovery.

How far back does IT need to look in producing email and other electronic documents for discovery? Do you need to find only current email? Often, this is spelled out specifically in the discovery requests and timeframes can go back several years. Increasingly, however, we are seeing discovery requests require all email without a specified time frame. This means you need to search for any and all copies of email concerning this issue, regardless of how far back you need to go. In some cases, both parties will agree to specific keywords, meaning that all messages that contain these keywords must be produced. There could be (and are) some requirements for retrieval that go back farther in time than an organization has records to support the request.

Where do you need to look to find email and other documents? For most state courts and regulatory discovery requests, quite simply, everywhere they reasonably may be expected to exist. This includes email servers, PST files on desktops, laptops, copies of email on backup tapes, disaster recovery archives, etc. In the eyes of the court, there is no difference between email contained in an employee’s inbox on the server and email located on someone’s laptop, even if that someone and his laptop are currently on an extended vacation. The most difficult area to search can be old, archived backup tapes. There is some protection against having to look in “inaccessible” areas in Federal Courts, as discussed previously. Many organizations have years’ worth of backup tapes in offsite storage. Do you know what documents are on those tapes?

### **ESI Data Survey Map**

As part of the preparation for the meet and confer conference described above, IT will be required to produce a data map. The court will also ask: Who are the custodians of these systems? What is the retention policy for each system? Who is responsible for retention periods for these systems? What are the backup policy and practices? What data is inaccessible? The District Court of Delaware, for example, requires a data map which contains the system name, description, scope, character, organization and data formats.

In most cases IT should be prepared to produce the following types of information for the meet and confer conference:

1. A list of the most likely custodians of relevant electronic materials, including a brief description of each person’s title and responsibilities.
2. A list of each relevant electronic system that has been in place during the identified time frame and a general description of each system, including the nature, scope, character, organization, and formats employed in each system. The parties should also include other pertinent information about their electronic documents and whether those electronic documents are of limited accessibility. Electronic documents of limited accessibility may include those created or used

by electronic media no longer in use, maintained in redundant electronic storage media, or for which retrieval involves substantial cost.

- The name of the individual responsible for that party's electronic document retention policies ("the Records Manager or Coordinator"), as well as a general description of the party's electronic document retention policies for the systems identified above.

The tables below show examples of IT responses prepared for a meet and confer.

**Table 1 - Relevant Electronically Stored Information Systems**

Relevant Electronically Stored Information Systems					
Corporate System Designation	Description	Scope (size)	Character (Data Process Flow)	Organization (data structure or schema)	Data Format(s)
Electronic Mail System	Corporate uses Microsoft Exchange 2003 software for internal and external electronic messaging. This software runs on two Microsoft servers.	There are approximately 2000 Exchange mailboxes with a current message store size of just over 200 GB.	Email messages are routed from the Internet or intranet to the Exchange servers. Microsoft Outlook clients on each workstation access the Exchange server to receive or send messages.	Messages, including SMTP headers and attachments, are stored in the Microsoft Exchange store database. They can be retrieved with the appropriate mailbox access permissions by use of MS Outlook.	Email messages are typically stored in the Microsoft Exchange Message Database. Users also have the ability, through the desktop messaging client MS Outlook, to store messages on their local drive or network share. The format can be .MSG for individual messages.
User and Group File Shares	Microsoft Windows Server 2003 is deployed at Corporate to allow centralized management and sharing of desktop application documents.	Documents created by using Microsoft Office are stored on network-attached storage file systems. There are currently about 6,000 GB of such documents.	Corporate users have Microsoft Office applications, such as Word, Excel, PowerPoint, and Access available on their workstations. Documents created by these applications are stored on the network shared file systems.	The desktop application work product files are stored in a standard Windows CIFS structure, with access governed by active directory permission controls.	The network shares store in common Windows file formats, such as .DOC, .XLS, .PPT, etc. and are retrievable using the appropriate MS Office application.
Desktop Personal Computers(PC)	Each user has a pc for network access.	Each PC has a local drive between 50 & 300 GB	Applications run on the local pc's. The MyDocuments folder is re-directed to the network share.	Microsoft Windows XP NTFS file system	PC local drives store in common Windows file formats, such as .DOC, .XLS, .PPT, etc. and are retrievable using the appropriate MS Office application.

Source: Contoural, Inc.

Companies that produce up-to-date ESI Survey Data Maps will find themselves significantly more litigation ready and able to meet the 100 day "Meet and Confer" deadline. More important, companies that can create a strong impression in the meet and confer sessions have both a better chance of limiting discovery in inaccessible locations, but also blunt the ability of the opposing party to use discovery as a weapon against them.

### Effective Document Retention Policies

The cornerstone of IT meeting Legal's needs is an effective enterprise document retention and destruction policy. A good policy clearly spells out what documents (data) need to be saved and for how long. It provides business justification for why information is saved or not saved. It may detail the litigation hold and e-discovery process. From an IT perspective, a good policy creates a type of *Service Level Agreement* between IT and the rest of the business (especially Legal) on what information to retain and for how long.

Attributes of good document retention policies include the following:

*Cover all types of electronic and paper documents* – Good policies cover all types of documents, including e-mail, instant messages, files, databases as well as paper. Likewise, good policies are comprehensive across the enterprise, including all groups and functional areas.

*Are clear and tend to be simpler* – Good policies and their corresponding retention schedules tend to be simpler and hence easier to execute, especially for ESI. It is worse to have a policy you are not following rather than no policy whatsoever. Good policies are those that can be followed consistently.

*Can be automated to the greatest extent possible* – The sheer magnitude of electronically stored information requires automation. Where possible, the document retention and discovery should be automated. This starts with having an “automatable” policy.

*Minimizes manual processes* – Good policies tend to minimize manual processes. Manual processes tend to be more expensive and very difficult to ensure consistent compliance.

*Are legally defensible* – Most enterprise document retention policies will be discovered during the course of litigation. The opposing party will be looking to see if the policy was comprehensive and if it was followed. They will be looking to exploit any gaps between what you said you were going to do and what you actually did.

IT has an important role in crafting policy. IT needs to educate the Legal group on what are the capabilities of technology and how these would impact proposed policies. Likewise, IT needs to analyze and then educate Legal on the medium and long-term costing implications of various policies. Finally, IT needs to be involved in the development of litigation hold processes to ensure that they can be executed quickly and the results will be defensible. In summary, IT needs to be at the table as the policy is being created.

## **Best Practices Summary: Seven Things IT Can Do To Meet Legal’s Needs**

The legal and business environment today requires that IT not only meet Legal’s needs, but effectively become a partner with Legal in ensuring effective document retention and efficient legal discovery. Here’s a summary of things IT can do to meet Legal’s needs:

*Create fast, effective litigation hold processes* – Working with Legal, IT departments need to be able to quickly enact effective, defensible litigation hold processes for e-mail and other ESI. Good litigation hold processes tend to be automated, able to be initiated across large groups of individuals, and are scalable in the event that the litigation hold persists for months or in some cases, years. IT can help Legal tremendously in this area.

*Educate Legal on archival capabilities* – Legal departments know what they need,

but they don't know how these needs can be accomplished through technology. They sometimes really have no idea how to make this happen. IT has an important role in educating Legal on archival technology capabilities. This will help Legal develop policies and processes for electronic documents that can be implemented through technology.

*Find and retrieve documents in native format* – Increasingly, IT departments will be required to discover and retrieve documents in their native format. IT can lead this effort by developing archival processes that store documents in their native formats.

*Create and Update an ESI Survey Data Map* – Increasingly important for meeting the “Meet and Confer” provision of the Federal Rules of Civil Procedure, IT can help Legal by developing a detailed ESI Data Survey Map. This is a map that outlines what types of ESI are located where throughout an enterprise. An up-to-date ESI Data Survey Map is an important tool for helping *reduce* the scope of discovery.

*Partner with Legal in creating a document retention policy* – A good document retention policy ensures compliance with regulations, reduces risk in litigation, is consistent with end-user work habits – and perhaps most important – can be faithfully followed. This requires IT working with Legal to develop policies that can be implemented with technology.

*Disable PST files and other forms of underground archival* – PST files and other types of user-controlled archival represent both a risk and burden for organizations during discovery. IT can help Legal by ensuring that this type of underground archival is minimized. The emerging best practice is to disallow creation and use of PST files, and instead archive e-mail and implement IT-controlled repositories such as archive systems.

*Create process for deleting older e-mail and files that are not under hold or needed for compliance or business processes* - Just as companies want to be careful about deleting email and other types of ESI too early, likewise they want to avoid accumulating all old e-mail and files forever. IT can help Legal by developing ongoing processes for identifying and deleting old, non-litigation hold impacted, unneeded e-mail and files.

In following these best practices, IT will move away from a reactive state into a state of litigation readiness.

### **About Contoural, Inc.**

Contoural is a leading independent provider of business and technology consulting services focused on litigation readiness, compliance, information and records management, and data-storage strategy. Contoural helps clients address the business requirements emerging around data. For example, electronic discovery rules—under the new Federal Rules of Civil Procedure—now require US companies entering litigation to know what electronically stored information they have, where it is stored, and how quickly they can retrieve it. Similar issues and requirements affect business records in many countries worldwide.

Similarly, legal and regulatory compliance requirements under emerging privacy laws are motivating enterprises to take a closer look at the integrity and security of electronic document files and other digital data. Contoural helps clients understand the business requirements for managing records, and then assists clients to align these business needs with their IT strategies and storage spending. These services bridge the gap between applications and data storage.

Contoural services include:

- Records-retention policy development
- Litigation hold process development
- Litigation-discovery process improvement
- ESI Survey Data Map development
- Data classification and storage strategy
- Data archiving solution design and program management

With these services, Contoural helps enterprises ensure compliance and reduce risks, while also achieving litigation readiness and reducing costs.

Contoural, Inc.  
1935 Landings Drive  
Mountain View, CA 94043  
650-390-0800  
[www.Contoural.com](http://www.Contoural.com)  
[info@contoural.com](mailto:info@contoural.com)