

## *e-Discovery*



Electronic discovery (e-Discovery) refers to “any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case”. This includes but is not limited to computer forensics, email archiving, online review, and proactive management.

The emergent e-Discovery field augments legal, constitutional, political, security, and personal privacy issues.

This toolkit provides guidance on the important decisions concerning archival, email management and retention, and litigation issues.



The ECM Association

1100 Wayne Avenue, Suite 1100  
Silver Spring, MD 20910  
Tel 301.587.8202 / 800.477.2446

[www.aiim.org](http://www.aiim.org)

# e-Discovery

## Table of Contents

<b>e-Discovery: Amendments to the Federal Rules of Civil Procedure (FRCP)</b> .....	<b>3</b>
<b>The Prospects for Uniform e-Discovery Rules (Or Lack Thereof) Among the States</b> .....	<b>4</b>
<b>What’s The Difference?</b> .....	<b>6</b>
<b>Email Management after the 2006 Amendments</b> .....	<b>9</b>
<b>Wherefore ROI?</b> .....	<b>11</b>
<b>FRCP: Discovery Obligations</b> .....	<b>14</b>
<b>New e-Discovery Rules: the Good, the Bad, and the Ugly</b> .....	<b>16</b>
<b>Staying Out of Court: Managing Email by Design</b> .....	<b>18</b>
<b>Retaining Websites</b> .....	<b>23</b>
<b>Records Management Goes Big Time</b> .....	<b>27</b>
<b>The Retention Game</b> .....	<b>32</b>
<b>Email Discovery: Tape Is Not Enough</b> .....	<b>35</b>
<b>Primer: Amendments to the Federal Rules of Civil Procedure</b> .....	<b>39</b>
<b>Industry Watch: Electronic Records Management: For Most, It’s Still “Waiting for Godot”</b> . . .	<b>46</b>

# e-Discovery: Amendments to the Federal Rules of Civil Procedure (FRCP)

Navigating the complex landscape of legal discovery can be intimidating and the landscape has changed once again with the amendments to the Federal Rules of Civil Procedure (FRCP), effective December 1, 2006. These amendments are a significant departure from applying traditional paper discovery rules to electronic discovery. The Supreme Court recognizes the importance of electronically stored information and the progressively prohibitive costs of document review and protection of privileged documents.

Electronic discovery (e-Discovery or ediscovery) refers to “any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case”. This includes but is not limited to computer forensics, email archiving, online review, and proactive management. The emergent e-Discovery field augments legal, constitutional, political, security, and personal privacy issues.

In regards to enterprise content management (ECM) and electronic records management (ERM), the two Rules to focus on are FRCP 26(b)(5) and FRCP 34(b). FRCP 26(b)(5) deals with General Provisions Governing Discovery; Duty of Disclosure; Discovery Scope and Limits; and Claims of Privilege or Protection of Trial Preparation Materials. FRCP 34(b) focuses on the Production of Documents, Electronically Stored Information, and Things. These amendments to the FRCP address a common corporate problem: the volume of electronically stored information and its maintenance. During an electronic discovery process, all types of data serve as evidence such as text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites, and computer programs. Because of lax corporate management, email is often the most valuable source of evidence in civil or criminal litigation.

A common, specialized form of e-Discovery is computer forensics (cyberforensics), which is “the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law”. Computer forensics executes a structured investigation while maintaining a documented chain of evidence to discover the contents of the hard drive of a specific computer. After physically isolating the computer, investigators make a digital copy of the hard drive and store the original computer in a secure facility. The cyberforensics team performs all investigation on the digital copy.

Current corporate operations are prone to the inadvertent production of privileged or work-product protected material. While this may create substantial risk, generally, it is cost prohibitive to conduct a comprehensive pre-production privilege review.

*Janelle Julien is associate editor of AIIM E-DOC Magazine (jjulien@aiim.org).*

# The Prospects for Uniform e-Discovery Rules (Or Lack Thereof) Among the States

The Federal e-Discovery Amendments of 2006, effective on December 1, 2006 (the “Federal Amendments”) provide “technologically neutral” rules for the discovery of electronically stored information in the federal courts. Attention has now shifted to rulemaking at the state level, where the volume of e-Discovery disputes is increasing and will continue to do so. States can withhold any explicit action, relying upon Federal court precedents and best practices, or they can choose from among at least four options.

## Mirroring the Federal Amendments

One obvious alternative is to adopt mirror images of the Federal Amendments, thus promoting uniformity within a state and, to the extent other states so act, across the country. However, it is no longer the case that changes to the Federal Rules is automatically copied by states.

As of April 2007, only eight states seem to be seriously considering adoption of discovery rule amendments drawing on the Federal Rules. Those states are Arizona, Indiana, Iowa, Kansas, Maryland, New Jersey (which adopted the Federal Amendments in total in September 2006), New Mexico, and Washington. The District of Columbia has appointed a Committee to study the issue, and the next six months to a year will undoubtedly see additional states join the ranks of those considering this approach.

## The “Uniform Rules”

For those states that will turn to the issue later, The National Conference of Commissioners on Uniform State Laws (“NCCUSL”) hopes that they will consider use of the “Uniform Rules Relating to the Discovery of Electronically Stored Information”. These draft “Uniform Rules”, whose final adoption is anticipated in August 2007, are closely modeled on the Federal Amendments but are positioned as standalone rules that are pithy and self-contained.

There are some minor substantive differences with the Federal Amendments. For example, mandatory discussion of e-Discovery topics is not tied to a court hearing or court order. This may be attractive to those states that have declined to adopt a counterpart to the federal “meet and confer” obligations.

## Texas Rule 196.4

Another approach to state e-Discovery rules is represented by Tex. Civ. P. Rule 196.4, which was enacted in 1999 by Texas and followed by Mississippi in 2003 and by Idaho in 2006. The Texas version of the rule requires a requesting party to identify information sought, and mandates payment by a requesting party of the expenses of any “extraordinary steps” required when production of electronic information not readily available to a party must be produced. Texas practitioners argue that this mandatory cost-shifting approach has reduced abusive and excessive discovery requests while providing adequate discovery.

Mississippi and Idaho followed the Texas structure but made the cost shifting a matter of discretion with the trial court.

## Guidelines for State Trial Courts

The Chief Justices of the various States have taken a different approach, acting through their Conference of Chief Justices (“CCJ”). Their “Guidelines for State Trial Courts on Discovery of Electronically Stored Information” were issued in August 2006 for use in states that have not adopted any e-Discovery rules. A copy of the Guidelines may be found on the National Center for State Courts website.

The Guidelines focus on what judges should do when facing an e-Discovery dispute rather than set forth rules governing party conduct. At least one reported decision (from North Carolina) has suggested that trial courts in that state should use Guidelines pending state rulemaking action.

### **Evaluation**

The inaction by states to date reflects, in part, a healthy skepticism over the need for explicit rules on e-Discovery and a desire to see how well the Federal Amendments work. However, based on preliminary reports, the emphasis on collaboration early in e-Discovery planning and the requirement that parties act in good faith is working quite well. In addition, the default standards on key topics and a more realistic approach to sanctions are promoting responsible internal training and process improvement. A focus on adopting these elements, therefore, whether as part of amendments to existing rules or as trial court guidelines, seems likely to best provide fair and effective state e-Discovery.

*Thomas Allman (tyallman@mayerbrownrowe.com) is Senior Counsel to Mayer Brown Rowe & Maw (Chicago), having served as Senior Vice President, General Counsel, and Chief Compliance Officer of BASF Corporation from 1993 to 2004. He currently co-chairs the e-Discovery Committee of the Lawyers for Civil Justice, serves on the Steering Committee of the Sedona Conference® (publishers of the Sedona Principles and the Sedona Guidelines), chairs the Sedona Subgroup on Email Management and writes and speaks widely on e-Discovery, corporate compliance and information management. Mr. Allman is active in ARMA, AIIM, ACC, and the ABA. He received his J.D. from Yale Law School.*

# What's The Difference?

*Is there a difference between document and records management?*

We all do it. In the daily rapport with our friends, colleagues, and in casual conversations at lunch, today's rapid-fire approach to sending and receiving information as quickly as our mouths or fingers can move leads to a tendency to overlook the choice of words we use. But of course we expect to be forgiven since everyone knows what we really meant anyway, right?

We also see it everyday in our field (whatever we are calling our field today), especially with all the attention placed on compliance and the importance of maintaining the records of our organizations. One example is the interchanging of the words records management and document management. They mean the same thing anyhow, right? Or do they?

## **Need Determines Viewpoint**

How often does the investigation into an electronic document management system (EDMS) within organizations start with a department or some other functional area saying they need to better manage the overload of paper, emails, and other electronic files followed by a call to IT because they know systems? This desire to better manage the documents within the office generally focuses on improving the storage, indexing/organization, and retrieval of those documents. Although the "reason" for the project to finally get rolling through added senior executive support may be due to higher needs such as regulatory requirements or improving overall organizational efficiency, the "What's-in-it-for-me?" factor typically revolves around users wanting to find things faster and clean up the clutter in their offices (i.e., get rid of the paper).

During these initial conversations, things like indexing, scanning, email storage, electronic file formats, and similar topics are the main points of discussion. At some point in the process, the records manager may (or may not) be invited to sit in on some vendor demonstrations. If compliance is one of the driving forces, many times a vendor may ask the organization to have the records manager sit in.

This is where the fun begins!

## **Understanding the Differences**

So, at this point in the process, the end users want to see how they will be able to find things faster and reduce the clutter in their area. IT wants to see how these systems fit into their infrastructure and what technical support may be required of them. Now a third perspective is thrown into the mix when the records manager is asked to provide input.

The records manager wants to know how the solution/process will address those things important to him or her such as identifying individual record series, record retention and destruction scheduling, determining the Office of Record (the official owner of the record), creating and maintaining an audit trail, reporting, policy development, procedures, and more. But none of this was discussed up to this point in the EDMS review process.

Generally, document management will focus on:

- Reducing the occurrences of lost and misfiled documents
- Providing faster location of and access to documents
- Reducing the amount of physical space used to store records (file cabinets, boxes, shelving, etc.)
- Better organization of existing records
- Improving general work process and organizational efficiency

Whereas records management generally includes the above, plus:

- Identifying what records exist (i.e., inventorying the records)
- Applying required retention periods to stored items
- Determining the owner of each record series
- Ensuring that a chain of custody and a proper audit trail both exist
- Assists in e-Discovery issues and applies legal holds to records when needed
- Adherence to defined policy and procedures for records regardless of the format (either electronic or hard copy)
- The concept of disposition—actually getting rid of documents (This also helps in the eventual migration of information to a new system since there will be less data to migrate, which will occur but may not be until ten or more years down the road)
- Preservation of records throughout their lifecycle—some of which may be permanent and must be readable 100+ years into the future

### **Hindrance or Help?**

When the records manager is brought into the discussion, it may be viewed as an effort to stir up more dust thus clouding the solution seen by the department and/or IT. “Hey, we were moving right along with the project until they got involved. Now everything is slowing down.”

This is the point in the process where the records manager is asked to explain their proposed role and why the issues brought up are important. Often the terminology spouted by all parties is either foreign to the others or the same word is used, but they have far different meanings in each party’s respective role (see sidebar).

Let the stumbling begin....

Trying to reinforce the importance of records management in designing a new process or selecting an EDMS is usually what trips up the records manager because they can’t speak in IT terms. The end user of the system often has not given much thought to records management in the past, so they may see it as not as important to them—at least not at the present time.

No matter what subject matter you are talking about, if you don’t put it into a context in which the receiver understands, then you may as well be speaking in Swahili. The end user just wants to move forward with the technology since it sounds so simple (just a few clicks is all it takes—that’s how the vendor presented it) and it may sound like the records manager is talking about things that are not that important—or are they?

### **Know the Difference or Get What You Deserve**

If you don’t understand the differences between record management and document management, who knows what you’ll get—other than somebody or everybody being disappointed at some point in the future. There is significant risk to an organization for not applying basic record management guidelines when managing electronic records and/or the selection of an EDMS. Unfortunately, many of these risks will not

be realized until months or years later. Then it is too late. The damaging results can range from harm due to litigation and the e-Discovery process to significant lost productivity to a system not being used at all, because it doesn't meet user or organizational needs as originally thought (and wasting thousands or millions of dollars in labor and equipment costs).

Organizations need to have an integrated approach that addresses both document management and records management. Understanding how these terms differ will save organizations countless hours, money, and the embarrassment of not coming close to what turns out to be unrealistic expectations. Organizations must move towards an integrated information environment for both hard copy and electronic information.

An overarching issue for any project is the understanding and awareness of culture change and change management that needs to occur. As an organization moves forward with its strategic plan for records and information management, it is important that time is devoted to culture and change management to increase the likelihood of the project's overall acceptance by the end user as well as by senior management. And oh, by the way, what are we calling "our field" today?

*Stephen Goodfellow is president of Access Systems (www.accesskm.com), an independent consultancy in records management and process improvement. Steve is a frequent speaker, writer, as well as a consultant in electronic records management and can be reached at 315-682-1188 or at SteveG@AccessKM.com*

**SIDEBAR**

**Terminology**

Each of the following terms has a different meaning depending on the group that is using the term. The way record managers and IT professionals use these terms is vastly different and could lead to misunderstandings and confusion—all to the detriment of the organization and project(s) at hand.

Term	Viewpoint (what it means to each group)	
	Records Management	Information Technology
Archiving	To keep; information must be readable, no matter what changes occur 10-100+ years from now	To move; migrate data to off-line or near-line storage (tape, optical, low cost storage device, etc.)
Retention	Classify & store records according to a defined schedule which includes the potential disposal of a record.	Store in an electronic format and back up to another medium (i.e., tape). A destruction period is not explicitly defined.
File	A manila folder (or equivalent) that holds paper records; the act of properly placing a record into an appropriate container.	An electronic document.
Record	An official document of the organization (not every document is a record).	A field in a database.
Preservation	How will this record be accessed and viewed several decades into the future? Will all the components to read the data still be available (the media in which the data is stored; the device to read the media; the software that operates the device and reads the data). It is a Record Manager's job to think about preservation especially with records with a permanent retention.	Usually not addressed or a viewpoint of less than 10 years is taken due to the expected change in the systems used. But will all the data be able to be migrated to the new platform in the proper format successfully?
Office of Record	The one functional area of an organization deemed the party of responsibility for an individual record series.	Who created the data (but they may not be the ultimate owner of the information).

# Email Management after the 2006 Amendments

Both before and after the enactment of the 2006 Federal e-Discovery Amendments, a business or public entity not subjected to specific regulation on the topic has the responsibility and authority to determine how best to manage its email communications. Done correctly, the issue is not one of law, although legal and regulatory requirements set the stage and provide minimum requirements. A variety of legally defensible models exist, all of which are equally valid. Entities of comparable size have adopted radically different approaches with equal success based on the needs of the entity by reaching internal consensus among business and functional units, with legal, compliance, and IT advice.

Under the Amendments, the guiding principle is that information systems must be operated in good faith and that reasonable steps should be undertaken, when litigation is anticipated or begun, to preserve email relevant to the proceeding.

## Good Faith Alternatives

One enterprise, for example, may decide in good faith to focus on reducing the volume of email routinely stored on active and archival sources and to emphasize segregation of email whose content qualifies as records of business activity. Email containing only “transitory” information—of no lasting value—is to be quickly eliminated by user action, as enforced by automatic deletion after set times or “quotas” on the amount of storage space available to individual users. In a 2005 Industry Survey, over one-half of the respondents reported that they were “managing” email retention by limiting mailbox sizes. See *Electronic Communication Policies and Procedures: A 2005 Industry Study*, AIIM & Kahn Consulting, Inc.

Adequate alternative storage opportunities are necessary, however, since local storage may be discouraged. Users are often required to “classify” email, based on content, and then “drag and drop” the email into a networked file fitted with a predetermined retention duration based on a retention schedule.

Yet another enterprise, also acting in good faith, may prefer to empower users by retaining email without requiring early classification decisions. Entities following this approach typically move email from active servers to lower cost (“tiered”) storage that offer capacities such as de-duplication of messages and attachments in order to reduce storage costs. One variation favored by entities with a compliance focus is to capture all incoming and outgoing email into a “vault” or “safe” where the user cannot change or delete the information but can access it for individual use.

Entities adopting this model see the costs of over-retention as balanced by the increased productivity of users with access to information, regardless of its perceived age or value. Some have also utilized this feature to implement litigation holds involving ongoing claims where compliance concerns exist about the ability to adequately retain the information needed.

## Integration of Document Management

An important feature of any email strategy is to provide realistic options for retention of electronic “records” as the entity defines those terms. A “print and file” approach is legally defensible as a strategy (paper has a longer and more predictable retention capability than almost any electronic media) but in the main, document management systems which integrate email with other forms of electronic information, are increasingly useful for this purpose. The toughest issue is to reliably assure movement of individual email into those systems.

### Legal Holds and Backups

Any email strategy will ultimately be judged on the effectiveness of the “litigation hold” process that kicks in once litigation is foreseen or commenced. Many entities are adding resources and making advance provisions for interruptions of otherwise routine operations that may be needed to assure continued availability of email.

For example, while appropriate use of disaster recovery systems (and use of recycling of media created) is unaffected by the Amendments, it is important to remember that email on backup media is discoverable and preservation of the media (interruption of recycling) will be necessary in direct proportion to the degree to which unique information is available only on that media. Moreover, identification of the existence of potentially relevant unsearched media will have to be disclosed at an appropriate time.

*Thomas Allman (tyallman@mayerbrownrowe.com) is Senior Counsel to Mayer Brown Rowe & Maw (Chicago), having served as Senior Vice President, General Counsel, and Chief Compliance Officer of BASF Corporation from 1993 to 2004. He currently co-chairs the e-Discovery Committee of the Lawyers for Civil Justice, serves on the Steering Committee of the Sedona Conference® (publishers of the Sedona Principles and the Sedona Guidelines), chairs the Sedona Subgroup on Email Management and writes and speaks widely on e-Discovery, corporate compliance and information management. Mr. Allman is active in ARMA, AIIM, ACC, and the ABA. He received his J.D. from Yale Law School.*

# Wherefore ROI?

*Do ECM projects still require ROI (return on investment) justification?*

In today's acronym-laden electronic content management world, an old three-letter standby is being put through its paces. For years, return on investment (ROI) has been the calling card of ECM initiatives and projects worldwide. Depending on the size and scope of a project, staff and consultants have been known to crank through myriad ROI calculations, each designed to show just how much a targeted department might save by addressing its content management needs. Management or board approval often rested on a specific number or date at which an ECM investment would either pay for itself or at least stop costing the company more money.

Today, many of those calculations are changing. Increasingly, enterprises of all sizes and structures are looking at ECM with a new eye towards benefits that go beyond dollars-and-cents ROI. Business drivers have changed, pushing content management to the forefront of many enterprise-wide strategic initiatives. Technology has also streaked ahead, meaning ROI calculated this year might not hold up three years hence. Perhaps most importantly, the very nature of business has changed, with electronic content inhabiting an ever-more centralized role in the enterprise. The result of these and other factors is that while ECM initiatives today continue to be strengthened with strong ROI, many are being approved as much for their qualitative as their quantitative promise.

One of the bigger drivers behind increased attention to electronic content management is the growth of content itself, not only in pure volume but also in importance within the organization. A recent IDC survey found that 76 percent of respondents said they have a need to develop content once and reuse it many times after that. More than half—58 percent—said they need well tagged content in order to improve how they manage and deliver information, and 48 percent cited a need to combine and analyze content from many different sources.

Moreover, the explosion of technology pushes old content to the periphery even as it generates more content to take its place. Distributed servers, Web farms, and multinational corporations are among the factors that have created a far-flung (though content-centric world) whose parameters continue to expand. Toss in the multifarious ways in which content is now used, along with legions of new content users (customers, business partners) and the pressing need for effective content management can hardly be ignored.

Thus, ECM project approval need no longer rely on ROI alone. That said, just as Mark Twain famously quipped regarding mistaken reports of his corporal demise, reports of ROI's death have probably been "greatly exaggerated". You still may need ROI, but the best ROI appears to come packaged with other key ECM rationales.

## **Other Rationales**

One of the other key rationales is legal and regulatory compliance. "On the legal and discovery side, you have to implement systems like managing email, getting rid of shared drives, and anything else to reduce frivolous lawsuits and avoid fines," says Dan Elam, vice president of ECM consultancy eVisory. As a pure ROI calculation, Elam notes, putting a number to a potential legal judgment (which is never actually paid, since the system has prevented the lawsuit) falls short. At the same time, it is just that sort of non-standard return—the avoidance of a potential multimillion dollar discovery bill or legal judgment—that can sway a board or executive to develop more effective ECM.

Another persuasive argument is that good content management is simply good business. “You may want to ask yourself, does it make us more competitive? Does it make us more innovative?” notes Carl Frappaolo, executive vice president of Perot Systems Innovation Lab (formerly Delphi Group). Frappaolo talks about doing a “thorough needs assessment” rather than a financially focused ROI calculation. Included in that needs assessment, he says, are things such as whether not having effective content management is costing the company the salaries and/or benefits of temp employees brought in to search through and manage content, or increased storage costs due to excessive data duplication. “One of the questions you want to get at,” Frappaolo says, “is not the current cost for maintaining your records, but what is the cost of not maintaining your records?”

Another cost that doesn’t always fit neatly into a standard ROI calculation is the cost of recovering from a loss of data, be it due to human error or natural or man-made disaster. “How do you come up with numbers that are representative of what the risk might be?” asks Russ Edelman, president of Corridor Consulting. In one case, Edelman says, his group calculated the estimated cost to rebuild systems and software, as well as to replace people who may have been affected by the disaster, but the numbers added up so quickly that executives had a hard time taking them seriously. Better than trying to attach a large number to a disaster, he counsels, ECM professionals should stress the amount of work it would take to recover the lost data, and the almost certain loss of continuity and efficiency that might result.

Traditional ROI calculations may also be off the mark, Edelman adds, if they ignore or underreport the true cost of ownership of systems and data. He cites the example of a recent ROI study that focused on the cost of new software and projected reductions in staff time, but completely ignored the cost of (and benefits to) re-engineering systems and processes as well as training costs for the new system. “In order to be effective, ROI has to begin with the entire total cost of ownership,” Edelman says. “The good news is end-users and decision-makers are getting savvier to this, that ROI may not represent all factors.”

While ROI may be getting something of a bad rap as a gauge for enterprise-wide ECM deployments, though, it remains a decent driver for smaller scale, department-level initiatives. “If you want to implement accounts payable, you need to show you can save money,” comments Elam, who argues that the validity of ROI grows in an inverse relationship with the cost as well as scope of an ECM initiative. Smaller, targeted, less expensive initiatives such as an OCR claims processing system, in other words, might present attractive ROI numbers and a short payback period, while the returns on larger initiatives prove harder to quantify.

This fits into what Mike Alsup, president of ECM integrator Gimmel Group, says about trying to peg absolute and accurate cost figures to the implementation of an ECM project. “The problem with an investment ROI analysis is that, except at a departmental level, the hard ROI depends on heroic assumptions,” Alsup says. “For example, if you save 10,000 people one hour per day, can you really eliminate the jobs of 1,200 people? Probably not.” Alsup advocates for “justification” as the new rationale for ECM. Justification, he says, takes into account not only investment ROI but also the costs and risks of litigation, the need for regulatory compliance, disaster recovery costs, the use of ECM as a business enabler, and the need for ECM to enable accurate and complete records management in today’s enterprise.

“ROI has always been really important, and it is just in the last two or three years it has become less important in a way,” Alsup notes. “What has really happened is that ECM became more important to the entire organization primarily because of non-ROI justification, things like compliance, records management, and e-Discovery.”

## Moving from ROI to VOI

For the acronym lover in all of us—good news. Not only can ROI continue to be used as one of a quiver full of arrows for ECM justification, enter a new acronym—VOI, for “value on investment”—to take its place.

“People misunderstand how to apply ROI in relation to ECM,” states Toby Bell, research director at Gartner. “If I ask the business side or the CFO, they’ll say ECM equals cost, and BPM (business process management) equals ROI.” Bell argues that executives who view ECM in this way ignore or shortchange the “horizontal” value of good ECM—consistent, accurate data and content that can be used to create “vertical” applications and solutions that can be sold to customers or business partners. Gartner even offers another acronym—CEVAs, which stands for “content enabled vertical applications.” Bell cites examples such as loan origination and claims processing, whose very existence, much less ROI value, can be traced to the good horizontal-scale value of efficiently and accurately managed content.

“The real value of ECM is when it starts to intersect with BPM,” concurs Craig Rhinehart, vice president for compliance markets and products for FileNet. “Take the example of insurance claims processing. There is not a lot of value in storing a repository. The real value comes from the routing of information throughout a large distributed organization, in a common workflow with common business steps.”

All of which leads back to the idea that ECM professionals will win converts by preaching the benefits of ECM as both a holistic and complementary technology to aid the entire ECM-challenged enterprise. An even stronger argument may be made that ECM is really a core competency or simply the “cost of doing business” in today’s content-centric, electronically enabled world. As such, ECM’s ROI—or VOI—becomes self-evident.

“Executives and CFOs really want to hear how is it helping, not just ‘what’s the return if we do this,’” says Frappaolo. “Good CFOs will really want to understand why it is helping, do we need to retrain, is our culture or are our processes changing for the better? It is not just a focus on the numbers but on the overall how and why.”

“You can spend a lot of time coming up with all kinds of calculations,” Edelman concludes. “If we have 150,000 people worldwide who spend 5 percent of their time looking for content, and if we know the average salary of the individuals we can come up with some kind of number. There’s a good chance executives will look at that and just laugh. You are trying too hard to sell the ROI. Some of this is much more intangible. What you want is for people to start to say we are doing this because we believe in the concept, rather than here is mathematically how it is all going to work.”

*James Dukart is a freelance writer based in Minnesota. He can be reached at [jdukart@thewriteplanet.com](mailto:jdukart@thewriteplanet.com).*

# FRCP: Discovery Obligations

The 2006 Amendments to the Federal Rules (FRCP), which came into effect on December 1, will have important consequences for the way an enterprise manages its electronic information. Rules 16, 26, and 34 reflect a new paradigm of issue resolution based on early discussion of key issues. Parties and their counsel are expected to candidly assess and then disclose details about relevant “sources” of potentially discoverable information, including those sources that they do not intend to search and may or may not preserve. These discussions place a premium on adequate preparation and, in turn, should help induce parties to better integrate their internal technical and legal expertise. It will also require counsel to make an effort to understand how information is actually used by their clients.

## Early Disclosure Discussions Required

From the point of view of those of us who are members of the Sedona Conference© this approach is the key to resolving the difficult issues of e-Discovery. The major problem we have identified with current practice has been the postponement of disputes until it is almost too late to make anything other than a binary choice between sanctions and non-sanctions. However, it will not be easy to reach a uniform level of performance, and some of the learning curve experiences will not be very pretty. The degree and formality of disclosure will properly vary in direct proportion to the complexity and needs of the case. Patience on the part of the courts and a certain level of mutual trust among contesting parties will be necessary to make the paradigm work.

Two of the topics for early discussion under Rule 26(f) involve information in both documentary form and electronic form. First, parties must discuss the preservation steps they have already undertaken or contemplate taking. Preservation obligations generally arise as a matter of substantive common law. They are “triggered” by the filing of litigation or its anticipation and can apply to any form of potentially discoverable information, no matter how difficult it may be to locate and preserve. The goal of Rule 26(f) is for the parties to discuss and resolve any preservation concerns early to avoid post-production disputes. Rule 37(f) suggests that careful attention must be paid to balancing perceived preservation needs against the legitimate needs to maintain the use of information systems that recycle or overwrite electronic information. Thus, instead of a sole focus on document “retention” policies which winnow out of valuable business information (with destruction of the balance), entities must balance competing needs through exercising reasonability and good faith.

If parties cannot agree on preservation steps, either one may seek a formal court order. Stipulated preservation orders can serve a useful purpose by establishing a baseline set of compliant activities where they are feasible. The Committee Note to Rule 26(f) discourages the use of ex parte preservation orders (i.e., orders issued without prior notice to the opposing counsel) and also discourages premature requests for preservation orders absent adequate discussion.

The second topic for early discussion involving all forms of information (both electronic and hardcopy) is any voluntary accommodations the parties might reach regarding non-waiver of privilege or work-product protection in the course of discovery. Rule 26(b)(5)(B) adds a process for asserting such a privilege after production but the Committee Notes to Rules 16 and 26 implicitly suggest that parties should also consider entering into voluntary agreements, which can be included in the scheduling order, which may, at least as between the parties, help establish the substantive effect of such inadvertent production.

The parties to litigation are also obligated by Rule 26(f) to discuss the form or forms of production (and, by inference, the form of preservation) of electronically stored information. The Advisory Committee ducked the issue of the need for metadata and embedded data, unlike the Sedona Principles, which take the position that metadata need not be produced unless a clear need exists. Best practices increasingly point towards maintaining (preserving) ESI in native format until that decision can be reached.

### **Reasonable Document Production Only**

Finally, the 2006 Amendments also explicitly mirror the practice in the electronic world to the common practice in document production. In the latter case, parties determine the scope of what they will search for purposes of production and object to those demands they consider unreasonable. Under Rule 26(b)(92)(B), directed solely at information in electronically stored form, a party need make its initial production only from those sources which it identifies as not reasonably accessible because of undue burden of cost. A court may, upon request of the other party, order production from such sources if it disagrees with its non-accessibility or if it determines that good cause, measured by the need of the case and balanced by proportionality concerns, justifies such production. In doing so, a court may order some form of cost shifting, although the Committee Notes clarify that a requesting party cannot simply “purchase” discovery from sources that are not otherwise discoverable.

This standard of limited production will, many hope, encourage parties to seek to confine their demands for e-Discovery to readily accessible sources, or, in the words of the Sedona Principles, from those “active” sources that are established and used in the ordinary course of business and from which information may be readily retrieved.

*Thomas Allman (tyallman@mayerbrownrowe.com) is Senior Counsel to Mayer Brown Rowe & Maw (Chicago), having served as Senior Vice President, General Counsel, and Chief Compliance Officer of BASF Corporation from 1993 to 2004. He currently co-chairs the e-Discovery Committee of the Lawyers for Civil Justice, serves on the Steering Committee of the Sedona Conference® (publishers of the Sedona Principles and the Sedona Guidelines), chairs the Sedona Subgroup on Email Management and writes and speaks widely on e-Discovery, corporate compliance and information management. Mr. Allman is active in ARMA, AIIM, ACC, and the ABA. He received his J.D. from Yale Law School.*

# New e-Discovery Rules: the Good, the Bad, and the Ugly

It's that time of year again. Or rather, it's that "New Year" time of year again. And that means...Resolutions to Change. Or as the David Bowie song would say, it's time for "Ch-Ch-Ch-Ch-Changes."

I did a quick book search at Amazon.com on "change," which yielded 482,019 results. Just in the top twelve, we can find books on "Leading Change," on "Making the Most of Change," on "Strategic Organizational Change," on "Changes That Heal," and on "Changing Your Brain."

Sitting in my office, surrounded by more paper than is advisable for someone who is president of an association devoted to driving paper out of our processes, I am attracted by the title "Move Your Stuff, Change Your Life: How to Use Feng Shui to Get Love, Money, Respect and Happiness." Maybe if we could recast all this ECM stuff as "organizational Feng Shui," we might get more executive suite types to pay attention. I even note a book on "Leaving Microsoft to Change the World," but I'll leave that for another column.

The passing of the year marked a major change in the core set of assumptions governing how businesses and organizations conduct their activities. That change was the introduction of new Federal Rules of Civil Procedure (FRCP) on December 1, 2006. For those IT managers, records managers, and senior executives working to put some long-overdue rationality and structure and accountability into their information management systems, these changes may finally be the prod that moves organizations to action. A snapshot on some of the reaction to the new rules...

- "Companies not prepared for new e-Discovery rules." (*Computerworld*)
- "...new rules make it more important for companies to know what electronic information they have and where..." (*Business Week*)
- "U.S. businesses are going to have to change the way they handle electronically stored information..." (*eWeek*)
- "CIOs and their IT departments will find themselves on the firing line in most major business litigations." (*InfoWorld*)

The "good" news (and simultaneously the "bad" news!) about these changes is that, for the first time, a legal framework has been put in place governing electronically stored information (ESI) and e-Discovery. The reason that this framework is both good and bad news is that the "ugly" news in most organizations is the current state of information management. For the most part, organizations are ill-prepared for the changes that will be coming as a result of the changes in the Federal Rules of Civil Procedure.

A few highlights from AIIM's Industry Watch surveys about the state of information management preparedness in most organizations illustrate the challenges ahead (note: data below is for companies and organizations headquartered in the U.S.—although it should be noted that the new rules also have an impact on organizations headquartered outside the U.S. but doing business within the U.S.):

- 75 percent of end users describe their email management strategy as “not yet begun” or “much remains to be done.”
- 67 percent would “somewhat disagree” or “strongly disagree” with the statement, “There is widespread understanding in our organization of what electronic records are and how they should be retained.”
- 55 percent would “somewhat disagree” or “strongly disagree” with the statement, “In the event of a lawsuit, we have clear policies and procedures in place outlining what to do relative to electronic information.”
- Only 41 percent of organizations have a formal program in place to address litigation readiness and electronic information.

If Sarbanes-Oxley, HIPAA, SEC Rule 17, and the Morgan-Stanley decision weren't enough to convince organizations to get serious about effective management of electronically stored information, the new federal rules should be a wake-up call. It is now part of the expected cost of doing business that a company or organization has their information management systems under control. And not just public companies. Or health care providers. Or investment houses. Everyone.

*John Mancini is president of AIIM.*

*Note: Over the past 6 months, AIIM has done extensive surveys of the current state of information management in user organizations. Background on these and other AIIM Industry Watch surveys can be found at [www.aiim.org/industrywatch](http://www.aiim.org/industrywatch) or on the AIIM Industry Watch blog at [www.aiim.typepad.com](http://www.aiim.typepad.com).*

# Staying Out of Court: Managing Email by Design

*Harnessing ways to manage proliferating email to mitigate risk begins with records management. Setting and enforcing email policies as a larger set of RM policies are key.*

Email, one of the world's easiest, most commonplace business tools, comes at a high cost. As precedent-setting court cases on down to small court-skirmishes and email faux pas convey, when emails are not managed correctly, there is unnecessary exposure to lawsuits and scandal. Plus, a host of regulatory compliance issues lurk in the electronic ethers.

The trouble with managing emails escalates as email growth rates mushroom. Even estimating the number and volumes of emails sent annually is dizzying. By 2008, conservative estimates put the number of emails sent in the United States between seven and 10 billion according to research by Cohasset Associates, an information management consultancy, up from some 2.8 billion in 2005.

"Until Sarbanes-Oxley (SOX), email management did not get a lot of attention at the C level—or at the B level, meaning the board level," says Robert F. Williams, president of Cohasset Associates. "There's a pressing need for more information about managing email to bring about that awareness that you can't drive a car with three wheels very successfully."

If a leading industry survey conducted in 2005 is a good gauge, then businesses are in trouble. According to AIIM and ARMA International's bi-annual, joint survey conducted by Cohasset Associates to more than 2,000 records management professionals only about one-half of organizations surveyed reported having a retention policy for email. In addition, nearly one-third surveyed does not include e-records in their records management policies and procedures (the survey is available at [www.aiim.org/industrywatch](http://www.aiim.org/industrywatch)).

## Growing Threat

The exposure of risk if improperly saving and retaining emails or on the flipside, failing to properly archive and store emails at all, is mounting as lawsuit-happy disgruntled employees cry fowl and regulating agencies of all kinds force compliance. "The pain is getting more painful and the economic hardship is getting more and more onerous," says Randolph Kahn, Esq., founder of Kahn Consulting, a legal IT consultancy.

About 75 percent of business email is considered intellectual property and is discoverable, says David Campbell, product marketing manager for Enterprise Vault archiving solutions at Symantec, an enterprise security solutions provider. "There are any number of regulatory factors like HIPAA for health records, SOX for financial records and FERC on the energy side. You have to retain and hold email based on what industry you are in."

Campbell says email retention policies are getting more complex because of these and other business issues, making enforcement mandatory. "Different industries have different levels of comfort. If you are taking in customer emails with sensitive data, or invoicing and long tracking of support cases, you will want to retain a lot of customer email. But external email is just as important as the internal stuff running around. Some companies will save everything for ninety days and then purge everything out of the system."

In a case like that, the company had better be sure to have an archiving system with good records management policies. Why? As regulators say that email must be saved if it's involved in the business record, the courts are certainly driving the point home. In fact, in December 2006, a king of rulemaking—the Federal Rules of Civil Procedure—will broaden its definition of a document to incorporate emails, and even voice mails, stored in the computer. “Parties will be required to disclose, very early on in the discovery process, their computer systems and data, including email that relate to the litigation,” Williams says.

Email is thus discoverable but is difficult and costly at best to manage and retrieve.

So what to do about managing email to reduce legal and compliance risks? Here are some solutions.

### **Truly an RM Issue**

Above all, the managing of email is a records management issue, not an email issue, says Carl Frappaolo, executive vice president of the Delphi Group technology consultancy. “First and foremost, there needs to be a corporate policy that is clearly stated that dictates how email is to be handled. The policy needs to be enforced, uniformly,” Frappaolo says. “Then, it’s a matter of deciding how long an email needs to be retained, based on the records management policy.”

Frappaolo advises IT and records management departments not to go running off and set their own email policy but to keep it broad around business records. “It’s the content/subject matter, business issue, customer, and such that matters,” he says. “The retention policy for email will likely be the same as a written letter, contract, etc. It is based on the content and nature of the communication, not the type of media.”

“Institutions have to decide who will retain business email communications so you are using your resources efficiently and not wasting effort,” Kahn says. This means determining how to retain the information and in what form. “You have to decide on technology and even storage locations so that you have access to the information, including locations so future litigants can have access to it. Build it with an eye towards expeditious and effective ways to retrieve the information in a cost effective manner.”

### **What To Save and How**

Technology comes to the rescue with tools like filters to head off unwanted junk mail. Broader solutions such as records management/ enterprise content management software may or may not have email archiving and management capabilities. In many cases, individual email management and even compliance management point solutions can be integrated with these broader solutions.

Perhaps one of the stickiest areas is setting criteria for saved versus non-saved emails. This falls under a company’s definitions for business records and business emails. “Our favorite definition is a business email is any email that has ongoing business, legal, compliance, or historical value and that has evidence of its business or business activities,” Kahn says, noting emphasis on “ongoing value.” He gives the example of company email about a budget meeting on Friday. “After Friday, its value to the institution is marginal. It should go away. It is not the kind of thing the institution should retain and use resources to manage.”

Kahn emphasizes the definition of a business email also requires a particular kind of value—legal, compliance, business, historical—certain kinds of value that are important. “You need to be clued into what that value is and make sure we are maintaining all of that in accordance with company policies.”

Don't simply take a snapshot of all inbound emails, says Bill Forquer, executive vice president at Open Text, an ECM solutions provider, citing the additional risk and excessive costs firms put themselves under when they use backup systems as archive. "You have to properly classify emails in the context of a records strategy. Otherwise you are creating liability for yourself by holding onto something that could be expired."

Once an organization is confident that they are saving the right emails, Frappaolo says, "These emails should be automatically moved to a storage device and protected. They should also be tagged with metadata information, or else discovery and recall becomes a real problem." As Forquer emphasizes, the ever-changing winds of the business and regulatory environments compel firms to create agile records management and archiving systems that do a good job of indexing documents for swift retrieval.

Based on the industry an enterprise competes in, Forquer says, the enterprise needs to review its regulatory responsibilities, determine policies and procedures appropriate for its business and industry, and then tell how it's going to execute it. He gives the example of SOX requirements for publicly held companies that require firms to explicitly set business processes around external financial reporting. "The result is that companies need to maintain the appropriate business records and processes associated with that reporting for seven years," he says.

### **Policymaking at the Top**

Priscilla Emery, president of e-Enterprise Advisors, an ECM consultancy, emphasizes setting policies from the top down. "Policies around managing email in general need to be set from as high up in the company as possible and need to be implemented using records management techniques."

With email management a critical but contentious subset of records management, Emery notes, "Depending on the size of the company, it often takes a village of participants to set policy. Likely, this is records management and IT people together, and they should be getting guidance from legal, financial and audit, and others with vested interests in the outcome."

### **Policing the System**

Another area that companies grapple with is setting and enforcing email usage guidelines. Inappropriate use of email networks, sending improper or proprietary information, can get a company or an employee into trouble but employers are legally responsible for an employee's bad act. Emery says a records management policy for email dovetails with other critical email issues like anti-spam filtering and the lawful monitoring of employee email and Internet use by the employer.

"You have to keep what you have to keep, but if someone is doing something stupid, it's up to the company to make sure the person is fired or appropriately disciplined," Emery says. She advises firms of any size to set guidelines around proper email etiquette and usage and to regularly communicate guidelines to employees, while enforcing them.

Kahn agrees. "You need to develop clear policies to tell employees what to do, what not to do, and how to do it. Tell them what a business email is. Have clear policies to tell them what is and what a record is not."

Setting records management policies and guidelines around emails is one thing, but enforcing them is another. Kahn says this demonstration can include ongoing training for employees, ongoing review of the information that has already been kept, and keeping abreast of legal and regulatory developments. Training can go far to head off problems before they occur, especially if the employee knows the implications of their actions. To this end, Kahn's firm offers a training program called Keeping Good

Company. “We use it to tell employees the importance of good records management, good email management. The average employee is the foot soldier on the front line of effective information management for the company so it’s important to train them.”

### **Managing It**

Forquer of Open Text says enterprises need an integrated approach to email archiving with other records management practices. “Use a series of automated capabilities set by the end user. That’s where you start to filter down the information you really need to retain, set retention times, and follow through with the destruction of documents as appropriate to the policies that are in place, following compliance with regulations.”

Like Open Text, user-driven classification is an element of Symantec’s solutions. “You can archive specific folders. We also have flexible rules-driven classification. You can save content very easily based on the metadata. Rules are based off of the senders, the recipients, the subject line, or so forth,” Campbell says.

Forquer says flexibility in content management systems are key to adapt to changing regulatory and business environments. Solutions by Open Text and other ECM vendors help enterprises to integrate with other enterprise solutions to form repositories of searchable files, such as by department or subject. Therefore, content systems can pull from programs like Microsoft Exchange for email or Microsoft SharePoint for documents. “The onus is on providers like us to move into these primary computing environments to ultimately effect records management policy within those systems,” Forquer says.

“Search and retrieval is where the rubber meets the road,” Campbell says. These systems need to be based on archival systems, not daily backup. They also need to avoid redundancy with elements such as single instancing that only saves one copy of a large PowerPoint presentation that went to forty people in the company. “You can archive this of course on your own hard drive or a network drive. Single instancing means we are only going to archive one copy of that PowerPoint, even though the metadata will show who else received it.”

As these ideas illustrate, incorporating email management, archiving, and searching into the broader context of enterprise content and records management will only improve a firm’s business processes while keeping them out of court.

*Marcia Jedd is president of MJ & Associates ([www.marciajedd.com](http://www.marciajedd.com)), a marketing communications and research consultancy in Minneapolis.*

**SIDEBAR****Managing Email Done Right**

The consequences of ignoring email management are mounting. But now that the world is waking up to the fact that electronic information constitutes a business document or record, here are some email retention and management best practices from Cohasset Associates' white paper, *Making the Case for Email Archiving and Litigation Readiness* (July 2006):

1. Retain electronic information – as long as it's needed for legal and ongoing business reasons and in a manner that allows for efficient search and retrieval.
2. OK to destroy – after electronic information is no longer needed, destroy in accordance with the firm's records retention policies and practices.
3. Demonstrate actions taken – in the lifecycle management of the organization's e-records. Show actions were performed in accordance with policy and procedures.
4. Document audit trails of key activities performed, – including management oversight for who did what and when.
5. Provide assurances that the accuracy, reliability, and trustworthiness of records are preserved – e-records are managed over time and through any successive technology upgrades or migrations.

# Retaining Websites

*Websites can be subject to e-Discovery and contain records too. Don't forget to include them in your records and retention management program.*

While records and retention management is increasingly touted as a critical technology for compliance teams, legal personnel, and records managers, a critical audience is often overlooked: individuals responsible for managing company websites. Websites frequently contain content—such as news releases, policies, procedures, and videos—that can be considered “discoverable items” during audit or litigation processes, or may need to be managed as records. Consequently, it is imperative for organizations to institute consistent and comprehensive content retention and disposition processes for website content in order to help mitigate legal risks—particularly as the number of sites across organizations continues to grow.

While Web content management systems often provide basic content release and expiration capabilities, this functionality typically is not enough to support litigation and e-Discovery processes. Companies need records and retention management systems that apply uniform retention schedules and policies across all website content to ensure information that's no longer useful or required is systematically destroyed. This process can decrease litigation risks and discovery costs by reducing the amount of website content that must be audited and reviewed. A records and retention management system also enables organizations to freeze website content during litigation, making certain users do not delete information subject to discovery.

Furthermore, by adding retention management functionality to websites, organizations can generate significant business benefits beyond supporting e-Discovery and records management. For example, by facilitating the planned and automated disposition of website content, retention management systems can reduce “content clutter” on websites and decrease information technology (IT) storage costs related to site content.

## Managing Risk on Websites

Information found on an organization's website during discovery processes may cause damage to the business. Alternatively, an organization may be subject to litigation if it is unable to verify what information was on a website at a given point in time—for instance, if a customer insists the product they purchased does not function as specified on the vendor's website.

Similarly, a company may not be able to produce records that document accountability and stewardship of materials available on a site, calling into question an organization's credibility. Poorly managing website content can also make it impossible for organizations to detect fraud, false statements, and other illegal behavior occurring on its sites—further compounding the website risk management challenge.

As discussed earlier, general website content (not only official records) can be considered discoverable items during litigation, meaning retention and disposition policies should be applied across individual content items on a website. Some organizations' risk management policies may apply to the entire website itself. In these cases, companies must be able to take and store snapshots of their websites, or “roll back” to what a website looked like on a specific day.

### Instituting a Website Risk Management Policy

Developing and instituting a website risk management policy can help organizations determine how to best implement and utilize a records management system for websites. Abiding by such policies can mitigate many risks and decrease the likelihood of litigation caused by erratic disposition of website content.

Generally, when it comes to evaluating website risks, organizations should discuss and define known threats and vulnerabilities, assess their potential impact, and determine what actions need to be taken to control each risk in the most economical way. Some questions to ask are:

1. How does my organization use its websites? Are they internal or external-facing sites? What is the business purpose of each site? Is the website the primary or single method of communicating to your employees, partners or customers? Answering these questions will give you a better understanding of your website audiences, the type of content on your sites, and potential threats.
2. How often do the sites and specific portions of the sites change or get updated? Once a week? Daily? Upon refresh of the browser? How often does the actual website change through rebranding or a site redesign? How are you recording that change? Does that change impact any of your risks? Answers to these questions will give you a better understanding of how many revisions each item on your website contains. This information can help you decide if rollback functionality to recreate a site is a good option. It also helps determine how resource-intensive and potentially costly (from a content storage perspective) website snapshots might be for each of your sites.
3. Is the information on the sites unique, or is it readily available in other organizational records? Begin by identifying whether or not you have any items on your websites that must be managed as records according to industry regulations or company policies. Then, determine if that content (or a copy of it) is managed as the official record anywhere else within the organization. If the content on the website is the only version available, then that item needs to be managed as the official record.
4. What is the level of risk (legal, fiscal, or administrative) of the websites or portions of the sites if content is lost or unavailable? For example, if you make manufacturing or drawing information available to your suppliers or manufacturing partners on an extranet site, do you have any contractual obligations to make this content available at all times online? Is there any risk of a future lawsuit if you are unable to reproduce what you offered on your site at a given point in time? What are the administrative costs of manually finding and delivering current and previous drawings to partners if the content is lost or unavailable on the site?
5. Does content on my sites provide evidence of contractual or other legal relationships? For example, do you store customer contracts, product warranties, or support escalation policies on any of your websites? Will the contents of these documents conflict with other printed material within the organization? Identifying these content items during your website evaluation can help you target which items require immediate attention when creating and defining your retention and disposition policies.

### Retention Management Benefits beyond Mitigating Risk

In addition to supporting content management initiatives that help mitigate risk, a records and retention management framework for websites can generate other business and operational benefits.

*Increase user efficiency:* Retention management reduces “content clutter” by eliminating website information that is under-utilized or outdated. Too much “clutter” on a website can be costly; employees may spend too much time trying to find correct information on an intranet, or customers may give up searching for answers online—increasing the number of calls to a customer support center. Typically, a Web content management system offers basic content release and expiration capabilities. However, with these systems, content contributors usually determine content expiration on an inconsistent, ad-hoc basis. Records and retention management systems can leverage a combination of metadata and usage

analytics to generate “smarter” disposition schedules that can be systematically and consistently applied across all website content. By removing unnecessary information, companies can optimize Web content searches and improve user efficiency.

*Improve quality of website content:* After several years of website usage and employee turnover, many internal and external websites are plagued with out-of-date or inaccurate information. Users begin to distrust the content, and poor decisions are based on incorrect information. Automated retention schedules can better ensure fresh, current, and relevant website content.

*Reduce storage costs:* Storage and maintenance costs for the ever-growing volume of Web content continue to add up. Why pay for additional hardware or waste time, dollars, and resources backing up and maintaining systems for content that is not even used? Retention management enables companies to reduce IT storage costs by offering a systematic way to archive old content and eliminate irrelevant information.

*Optimize website performance:* Retention management enables organizations to automatically move under-utilized, or infrequently accessed, content to an “archive” server. That way, bandwidth and resources can be focused on popular content, such as videos, to ensure optimal performance.

*Minimize potential costs of discovery:* The cost for e-Discovery during litigation can be outrageous—sometimes totaling millions of dollars to produce one document in question. For example, in the *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.* (205 F.R.D. 421 S.D.N.Y 2002) case, the litigant estimated it would take approximately \$10 million to produce a single requested document. Some companies settle legal cases simply because it’s cheaper than going through e-Discovery processes.

The less information available to sift through on a website can help minimize costs when discovery requests are made. Retention management provides organizations with a systematic, policy driven, and legally defensible approach to control how long information is retained based on usage, relevance, age, and state (such as a legal or audit hold). This capability is becoming increasingly important, as there are a growing number of instances where website content is used in legal discovery processes.

For example, in the *Beck v. Atlantic Coast PLC*, 868 A.2d 840 (Del. Ch. Feb. 11, 2005) case, the failure to produce an entire Web page constituted sanctionable conduct. More information about this case, can be found at <http://www.ediscoverylaw.com>.

### **Leveraging a Records and Retention Management Framework for Websites**

A records and retention management framework can support and automate the steps companies should take to mitigate risk on their websites. Websites typically are made up of many pieces of content. Using a records management system, organizations can apply retention and disposition schedules to any or all content items on the website—whether they are considered company records or simply general website content. Companies can use the system to apply different schedules to various content items based on the content author, type of content, which website it belongs to, access history, etc.

More rigorous website risk management policies require that organizations be able to recreate exactly what a website looked like on a specific date—which is when website snapshots and rollback functionality may come into play. In this case, organizations should leverage a system’s revision management capabilities for individual website parts as well as for the website itself. While many systems enable users to roll back items to return the website to a previous state, others allow users to utilize revision control and rollback functionality to recreate a website at a specific moment in time in another reference (or non-production) system.

Snapshot functionality enables organizations to capture a website at a specific moment in time to store in an archive, repository, or records management system for future reference. Storage costs, as well as the amount of dynamic content available on a site, need to be considered when planning rollback versus snapshot capabilities.

### **Website Risks Continue to Evolve**

More and more website content is subject to litigation and audit scrutiny, making it increasingly important for companies to have a robust retention management framework in place that can help mitigate the risks associated with these activities.

Looking ahead, companies may also need to evaluate their technologies for accurately recording website usage. Recently, the U.S. Department of Justice subpoenaed records from several search engine companies, including Yahoo!, AOL, and Google, detailing the online searches conducted during a specified period.

This case signals a new dimension of law enforcement. While communications and Web use is routinely subpoenaed when a crime is suspected—typically a single user's laptop is confiscated and his or her email exchanges are obtained—there now is a possibility that one day companies will need to verify or defend in court the website usage of its customers, employees, and partners. For example, what users saw on a website, search terms used, whether or not they downloaded or contributed data, and so forth.

Many Web analysis, reporting, and content management tools offer the functionality needed to track this information. Various departments within an organization may already capture this data for other business purposes. Companies should be aware if they are tracking this information in-house today in case it is needed for litigation. They eventually may need to ensure this technology is in place, along with a comprehensive records and retention management system, to minimize as much as possible the risks associated with its websites.

*Todd Price is vice president of product management and product marketing for Stellent, Inc. ([www.stellent.com](http://www.stellent.com)), a provider of content management solutions. He is responsible for driving the strategy and development of Stellent's Universal Records Management & Universal Content Management solutions to ensure that the company successfully anticipates and meets customers' needs.*

# Records Management Goes Big Time

*Sheer proliferation of information, media formats, and compliance issues raise the profile and need for records management.*

In the old days, records management was relatively straightforward, relegated to hardcopy paper records and photographs. Over the decades, microfiche gave way to audiovisual mediums and a plethora of electronic formats, making the role of the records manager overwhelming. “Records managers are responsible for the lifecycle of records and information from birth to death,” explains Virginia Jones, certified records manager (CRM), and records manager with the information technology division of Newport News Department of Public Utilities.

In the old days, managing records and documents was often relegated to a few employees, scattered across departments. Now, increased regulation and a fiercely competitive business environment have raised the records management (RM) bar to a strategic one that begs implementation enterprise-wide in order to meet regulations or deliver stakeholder value. According to the Association of Records Managers and Administrators (ARMA), a record is information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business. But it’s not so cut and dried, say records management experts, who suggest enterprises around the globe are grappling with even defining what constitutes a “record” let alone its effective management.

“The biggest controversy right now in enterprise content management (ECM) and RM is the definition of what constitutes a record,” Jones says. While records and information management professionals might agree that a document is any recorded information, such as a draft, manuscript, electronic document, and the like, these things may not be considered a record. “All records are documents but not all documents are records,” she adds. Jones illustrates the point with a collaborative workflow solution that produces a series of document versions. “The collaborative material may not become a record until all parties agree on it.”

“There’s always been a large debate in the RM community as to what a record is and when it becomes a formal business record that has to be placed under a strong RM program,” says Bill Neale, records management subject-matter expert with FileNet Corp. He says compliance and legal issues have introduced chief financial officer and legal department involvement in the role of determining and selecting ECM and RM solutions as well as forming RM policy. “Each company has to evaluate their business process, the regulatory environment, the business issues and auditing issues, in determining what they really need to keep as a formal business record.

Certainly, not all content is a formal business record,” he says. “A record is many pieces of information which together form a record of an event or transaction,” says Alan Pelz-Sharpe, principal consultant with the management consulting division of Wipro Technologies. He says twenty to thirty years ago, a records manager primarily managed paper, but recently text messaging and all other electronic mediums have called for a “whole rethink” to RM. “We do have to be a little bit careful: ECM is part of RM, but database vendors play a role. A lot of data in databases isn’t included in the ECM vendor’s visions, and equally, these aren’t often included in RM practices.” He notes large vendors like IBM and Oracle are addressing this with their own solutions. Microsoft’s SharePoint is another solution.

J. Timothy Sprehe, president of Sprehe Information Management Associates, Inc., a records management consultancy, gives the example of a large credit card company implementing an ECM system to include RM. “The firm sees RM clearly from the risk management perspective but also as a

knowledge management tool to mine the database for customer information and for customer relations. That's not possible with paper records." For example, with a robust ECM system and with RM capability, the company can maintain official customer records according to a records retention and disposition schedule it previously established on an automatic basis. Benefits include mining the system for customer-specific information to create marketing offers or keeping meticulous track of customer contact.

To date, similar examples of savvy RM-ECM are hard to find, often relegated to world-class enterprises. Complicating the matter are the huge volumes of documentation flowing through organizations today. "Before one decides what you can and can't say is a record, you have to get the volumes under control first," Alan Pelz-Sharpe cautions. He says for the most part, government agencies and other highly regulated industries, like heavy engineering and pharmaceuticals, have done a good job at RM. Now, regulations and business pressure are causing other industries to take a hard look at RM.

To be sure, regulations are forcing the issue. Data privacy mandates such as the financial services modernization act (Gramm-Leach-Bliley) and corporate governance issues like the Sarbanes-Oxley Act of 2002 requiring tightened financial record keeping for publicly held companies and HIPAA (Health Insurance Portability and Accountability Act) shine a spotlight on RM. "People found out they had a terrible mess of their records. The initial work triggered by Sarbanes-Oxley and other regulations have caused organizations to get some control," Pelz-Sharpe says.

### **RM Decision-Makers at Odds**

"RM systems don't create records, they merely receive and manage records," Sprehe says, "So it's important that any RM system be integrated with any document, imaging, email, or correspondence management system. Very quickly you get to ECM." What constitutes a record is usually obvious, he says, although the role of who makes the decision surrounding records has certainly broadened with the proliferation of electronic records.

Sprehe performs significant consulting for the government agencies in executing their RM plans. "In the federal government there's a major disconnect between the RM and IT communities. They use the same terms but mean different things when it comes to RM," he says, noting historically, chief information officers haven't considered RM a priority and RM managers haven't been the most IT-savvy of individuals. Sprehe says only recently has each area acquired deeper knowledge of the other's area. "It's a slow process." He notes enterprises typically don't employ qualified records managers to help define the business rules around managing documents and records.

ECM solutions providers can help. Using the scaleable P8 architecture with a specific RM application, FileNet has an eye on business processes when it implements a solution. FileNet uses the ISO 15489 standard for records management in developing solutions. "Our methodology follows that right down the line in that standard. We provide services around developing the records program for clients," Neale says. So FileNet can assist with decisions around business processes which determine what makes a record or companies can make their own decisions around RM. "Regardless of the software used, a firm has to have well-documented policies with their (document) classification plans and retention schedules before you build the records program."

Neale says many electronic RM systems put the burden on the user to define what constitutes a record. "The means the user needs to understand the software, and how to categorize a document at the file plan level." But all too often, he says, users can't or won't take the effort to go to that level of detail. As a result, Neale says, "You have to automate those decisions and let technology take that burden off the end user. There's tremendous productivity gain on the worker's side and RM side when you do that." (See sidebar)

Sprehe agrees, “One of the problems with a lot of software vendors offerings at the moment is solutions don’t delegate this work out. At the end of the day, employees aren’t going to flag records. Even in automatic solutions, how good it is and defining what records are can be subjective.”

It’s clear enterprises go about the arduous task of RM in different ways, muddled by an avalanche of document management solutions. According to a report by U.K.-based consulting firm, firms either adopt a single electronic document and records management (dubbed EDRM) strategy while others take a holistic approach to information management, using an ECM solution. Another consultancy, CMS Watch, says ECM vendors are continuing to hone their RM offerings, albeit via specific applications which aren’t really used enterprise-wide.

### **Reliant Energy Gets Power from Sarbanes Solution**

One such company taking the holistic tact is Reliant Energy, a Houston, Texas-based electricity provider serving nearly two million customers. It used Stellent’s Universal Content Management system and made the transition last year to Stellent’s Sarbanes-Oxley solution, which rides on the architecture of the content management system. The move has made all the difference in increased productivity and data entry errors, says Courtney Herbert, manager of internal controls effectiveness for Reliant’s audit department. “We had a successful attestation last year with Sarbanes-Oxley. This year it’s going very well,” he says.

Herbert notes some 110 processes across more than 60 workgroups must be documented in its audit process to meet the stringent requirements of Sarbanes’ Section 404 for process, control, and documentation. Before moving to the Stellent solution, the audit department had to corral 110 Excel spreadsheets, other online solutions, and a lot of corresponding paper files. “We had a lot of issues around the integrity of the data we were trying to report on. Once we implemented the Stellent solution, all the information is captured in a central location,” he says. Many headaches have been saved in the area of testing the company’s financial controls. “We’re able to run quick reports and utilize that information to make our processes more efficient.”

One great result of the Stellent’s Sarbanes application is that all financial documents required for compliance, if not already available electronically, are scanned into the system. All documents are converted to PDF format; many are used as supporting attachments. “The ability to scan in documents and the data repository aspects of the content management system is extremely important,” Herbert says.

Another outgrowth of the automated Sarbanes solution at Reliant is outside auditor’s time is greatly reduced because the audit department now handles the detailed testing process, instead of the each business area’s process owners. So instead of scores of employees working on the tedious testing and control area, Herbert says about the equivalent of ten audit employees work to fulfill this Sarbanes requirement about four to five months each year.

### **Better Water Works with RM**

Virginia Jones of the Newport News Department of Public Utilities was hired on in 1993 to manage the water provider’s jumble of records spread over several facilities, some dating back to 1890. She characterizes the process as an evolution in establishing a solid RM policy and realigning business processes around RM and the utility’s online systems. Currently, the utility uses a proprietary customer information system it created and is working toward migrating to an off-the-shelf system within the next 18 months, necessitating changes in its RM policies.

Jones uses the example of a customer moving away. Under the new system, the customer's record will be maintained in the system for one year before its automatic movement to an archival section of the system for another two years before being purged into a delete basket of sorts before being deleted. Redundancy in data entry is avoided in perennial sections of records such as site information. Next up, Jones says, the utility will move to a new asset management system, and similarly redefine any corresponding business rules and RM policies. Finally, Jones says, the utility is planning to move to an electronic document management system in 2007. "We've had a solid records information management foundation over the last decade so we've been able to more easily transition to these systems," Jones says.

### **Too Many Documents Saved, or Not Enough?**

"RM has received a lot more attention in recent years first of all because of these scandals like Enron, WorldCom, and Arthur Andersen," Sprehe says. "CEOs can now go to jail if the records have been tampered with. Plus, people don't recognize that being a packrat can be a liability," Sprehe says. Indeed, long-time retention of documents like emails may have contributed to the downfalls of executives in some of the more recent big-business prosecutions. For the typical worker, saving too much information on the desktop is a common pitfall or savior depending on how you look at it. It can be a positive when searching for information on your desktop, for instance. Especially at larger enterprises, ECM solutions swoop in to copy documents or an entire desktop back to the central server.

RM experts say some of the trouble around events like lawsuits can be avoided when documents are destroyed according to document retention schedules. Jones says many firms retain documents that surface in lawsuits because of lack of reasonable RM policies, including failure to set or adhere to a disposition schedule. But destroying records after the fact can raise a red flag. "Companies have gotten into trouble because they continued to destroy records after they were part of a lawsuit," she says.

### **Leveraging RM**

The lure of managing risk attracts enterprises to RM, Sprehe says. "The first tendency to view RM is as risk management, but you're only motivated so long as a risk is perceived. Smarter enterprises are recognizing the need to capture e-records as soon as they're created," he says. He argues in favor of enterprises taking on vigorous RM as an offensive philosophy in the form of electronic RM and in the broader context of ECM, thus giving the enterprise instant access to current and authoritative institutional memory. "Then, the records repository becomes the most valuable institutional memory that the enterprise has, so the uses of records in day-to-day business operations, once recognized, become extremely valuable."

*Marcia Jedd is president of MJ & Associates ([www.marciajedd.com](http://www.marciajedd.com)), a marketing communications and research consultancy in Minneapolis.*

## SIDEBAR

### Benefits to Good Records Management

“Managing information is a growing issue, and RM is a subset of it. The cost of managing information is just crazy so there are hard benefits to be had with RM,” says Alan Pelz-Sharpe, principal consultant with Wipro Technologies’ management consulting division. He says establishing a proper RM policy will bring about enterprise efficiency gains. “It might not be the objective of RM, but people are often surprised it brings about hard benefits.” Bill Neale, records management expert with FileNet Corporation, agrees. “When combining RM with business process management, there can be tremendous savings such as leveraging steps in a workflow application or in metadata searches to find documents.”

Here are a few benefits to RM:

- Reduced data storage costs
- Proficiency gains on the network
- Improved employee productivity
- Reduced litigation costs

### RM at the Desktop

Enterprises are saddled with a slew of compliance and corporate governance issues. Making life a little easier for end users while adhering to records management (RM) policies is the point behind a solution by Trusted Edge, Inc., a provider of retention management and compliance software. “Traditional RM solutions require users to both classify and publish to the RM repository as a discretionary event. We make it a non-discretionary event with the RM Edge solution,” says Michael Beck, CEO of Trusted Edge. RM Edge goes beyond the border of document repositories to the desktop where 80 percent or more of corporate business records reside, thus improving retention scope and efficiency.

RM Edge captures information created at the desktop level by requiring its classification as a record and its capture. “It’s no longer contingent on user discretion,” Beck says. When the end of the life of the document is reached according to RM schedules, RM Edge reaches out to the desktop to delete files. The solution allows for creation of a metadata repository to even include items and documents that weren’t promoted to a RM repository. It allows the customer to set their own rules and retention schedules around these miscellaneous desktop items. “Nobody wants to save the company picnic memo and it’s a concern (from the data storage perspective) when it goes to thousands of mailboxes, so the system can delete those things on schedule after their useful life,” Beck notes.

Trusted Edge’s customers are primarily those competing in highly regulated environments like financial services and life sciences firms. In the case of a brokerage firm with international clients, the solution works to capture every document and email created by customer account number to form extensive customer records. These records are created and managed according to the brokerage firm’s RM policies, with the capability to capture documents deleted at the desktop level.

Solutions by Trusted Edge assist customers in “e-Discovery” quests, commonplace when a lawsuit or compliance issue arise. “The software supports enterprise-wide retention policies for desktop documents and emails while helping customers protect their valuable intellectual property,” Beck concludes.

# The Retention Game

*How do you make sure that emails are captured properly to both mitigate risk as well as keep them available to find again?*

Email is critical for modern business, but retention policies are sorely lacking. Email generates large volumes of storage: Microsoft Exchange processes billions of email messages (plus attachments) daily through corporate email servers, which are growing at a rate of 35 percent per year. To mitigate risk, organizations must manage email archives to avoid serious accountability, storage, litigation, and regulatory liabilities from today's era of regulations—Sarbanes-Oxley Act (SOX), the Health Insurance Portability Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), to name a few.

## Why Email Retention?

Without an effective email retention plan, it is time-consuming and expensive to search and restore email databases. Litigation is also an important aspect: organizations have lost lawsuits by keeping too much or too little information. According to "WhatIs.com," electronic discovery (also called e-Discovery) refers to "any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. e-Discovery can be carried out offline on a particular computer or it can be done in a network. Court ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-Discovery."

According to e-Discovery expert Elizabeth Charnock of Cataphora, "Having a well-defined email retention policy that is consistently executed is next to impossible to challenge in the event of any kind of litigation. If a company deletes all emails from its mail servers automatically on the last day of each month, anyone showing up with a subpoena for electronic data on the first of the month is then out of luck, at least with respect to items that existed only on such servers."

Lifecycle management of emails can mitigate some of this risk. With archiving, fixed durations are attached to individual emails, allowing continued access to the email for substantial periods. Email is then "aged out" (deleted) periodically as the associated period expires, a result permitted by and consistent with legal and records management doctrine. Archiving is an attractive option since it postpones any necessity to decide whether individual email must enter a more formal records management system.

Conversely, companies are reluctant to delete messages and opt to retain all of their emails, which affect storage purchases and management. Storage hardware is relatively cheap, so initial purchases account for only 20 percent of storage-related expenditures. However, managing these emails is another story: email administration consumes up to 43 percent of IT support costs.

## Solving the Problem

How do you solve the problem of only retaining the right emails in your RM system so that you can delete the rest to decrease your risk exposure?

Kris Brown, senior sales engineer at TOWER Software Pty Ltd, believes that although a complex problem, it can be broken into two main schools of thought—automatic and manual. The automatic methodology implies that technology is employed to read and categorize email based on rules and content, including sender and receiver. Obvious benefits include no user interaction and guaranteed compliance to the rules set out in the technology solution. Not so obvious problems with this solution include cost to implement custom rules for every organization, as well as having to do all the upfront work of determining the type of emails that an organization creates. In addition, there is the big issue of relying on a machine to determine

what a record is. “No current system (despite claims of vendors) is 100 percent accurate 100 percent of the time, and hence you are looking at emails (potentially thousands) that don’t fit into the categories or the machine misfiles,” says Brown.

Brown also recommends a second approach, which uses an organization’s workforce. “An organization has thousands of mini-records managers readily available,” Brown says. “Employees know their workspace and its inputs and outputs. They have intrinsic knowledge of a work process that no machine can replicate. So, the other approach is to utilize this knowledge by allowing the users to catalog the emails. It doesn’t have to be as hard as it first seems, most users already create pseudo filing systems with a series of folders in their inbox, and unless forced to delete, tend to keep everything forever.” End users can use the same skill of filing emails they deem important to catalog the organization’s email records. An obvious flaw to this approach is it requires the user to do something, and make a decision. However, if they do make a decision, it will be far more accurate than a machine.

There is no single answer. Each organization is different. If your main objective is to decrease your risk, then human intervention is needed, as this is much more accurate than any set of blanket rules. Automatic categorization can’t reduce the risk as much as having the sender/receiver of the email make a business decision at the time of creation to catalog the email.

For some organizations, email archiving, is a viable solution, which involves the transfer of email from primary storage to secondary, near-line or off-line storage, usually with continued user access and robust retrieval capabilities. According to Thomas Allman, Senior Counsel at Mayer, Brown, Rowe & Maw LLP, when configured to allow continued and productive use of email, email archiving produces minimal interference with familiar business processes and can be integrated with existing applications.

Allman believes a possible solution for email retention is an integrated approach for an enterprise that combines selected attributes that are most important to it. Any solution should be carefully implemented in stages, after a full understanding of the characteristics of the specific vendor applications selected. First, an organization could prioritize its most likely sources of valuable email and treat them differently (i.e., email generated or received by specific groups of users, such as executives, or types of functions, such as human resources, could be captured and retained for a fixed period before deletion). Second, this selective archiving could be augmented by enabling users to declare as “records,” based on content, individual email for transfer to the custody and control of the traditional records management system (if any) in place for that division or function. Third, as a general default, all email generated by or received by users not captured by the focused categories could be separately archived for shorter periods, with automatic deletion available unless the email is designated by users for transfer in accordance with the individualized approach described above.

Another concern is saving the right emails and whose responsibility it is to double-check the email retention policy. Brown acknowledges that any system without checks and balances is flawed. Reporting on the information that is categorized, whether done automatically or manually, will give an idea of compliance and accuracy. However, unless there is some enforcement of the rules, then the rules themselves are weak. There also has to be a point where the organization accepts some risk. If an email is deleted incorrectly, it has to be let go. “Keeping everything forever simply increases the risk to an organization, which is far greater than accepting a level of loss. A strong policy around this can also help an organization deflect some of the risk, ensuring that employees are held accountable for their actions,” Brown says.

Recommended practices for email retention include:

- Assessing your email records situation
- Generating intelligent business policies
- Communicating the policies to all end-users
- Using email management applications to archive, manage, audit, restore, and delete emails
- Instituting effective back-up and restore procedures
- Initially capturing and storing all email, IM, and attachments
- Basing retrieval capabilities on primary index values such as unique message ID, date, from, to, subject line, and combinations
- Providing full-text search capabilities against message text as well as attachments
- Scheduling deletions according to compliance timelines
- Preserving regulated data on non-rewritable, non-erasable formats (an important provision of the SEC regulations)
- Automatically verifying the quality and accuracy of the archiving process
- Offering full audit capability of the email archives

Understandably, management of email is the largest risk to organizations and it calls for solutions that are more comprehensive, which will take considerable time and cost to implement. However, by actively managing message stores throughout their lifecycle, organizations can establish email retention policies that will protect corporate intellectual property, increase information retrieval speed, and reduce expensive email server overload. Allman says, “Any solution adopted will be a compromise between competing policy considerations and its effectiveness will be dependent upon the solution of a variety of key technical issues.”

*Janelle Julien is associate editor of AIIM E-DOC Magazine (jjulien@aiim.org).*

## **SIDEBAR**

Primary regulatory body or regulation that applies to email retention

- Banking: FDIC, OCC (Office of the Comptroller of the Currency)
- Telecommunications: Title 47, Part 42
- Pharmaceutical: FDA—Title 21, Part 11
- Healthcare: HIPAA (Health Insurance Portability and Accountability Act)
- Defense: DOD—5015.2 standard
- Brokerage firms: SEC—Rule 17a-3 and 17a-4
- General business: Sarbanes-Oxley Act

# Email Discovery: Tape Is Not Enough

*If you're backing up your email to tape, that's not enough to keep you out of trouble.*

While organizations strive to backup their electronic information, quick and efficient access to this content continues to be an afterthought. In particular, electronic message discovery has become a critical issue in today's corporate legal proceedings and compliance investigations, often becoming a costly issue.

According to the Gartner Group, the amount of business-critical data now stored in email is as high as 60 percent. In addition, the National Archives and Records Administration cites email discovery as the fastest growing area of discovery in litigation. Companies are often faced with court orders to produce old emails. These companies must go through an extensive and time-consuming process to determine if a specific email has been completely purged from existence, and then take the necessary steps to locate and produce the message(s) in question.

Litigation discovery is a critical component of the legal process. With the tremendous growth in all forms of electronic data, emails, instant messages (IM), and Word documents are now admissible in court. Therefore, companies must be able to quickly and easily search massive electronic storage archives to locate specified documents or emails.

Chicago law firm Vedder Price Kaufman & Kammholz has stated that traditional e-Discovery methodologies for restoring email can cost about \$2 per message, which includes the attorney review costs. In a recent example, Philip Morris USA was hit with \$2.75 million in sanctions, or \$250,000 per employee, when it failed to preserve court-required emails for 11 employees. If an organization stays mired in the traditional methodologies of email storage and e-Discovery processing, it will be stuck addressing e-Discovery from a reactive stance and quite literally paying the price for so doing.

Email's larger role in litigation studies have shown that email is by far the most prevalent business record in the corporate environment. Therefore, it is no surprise that the discovery of email is a central strategy of modern-day regulatory investigation and litigation. The reasons behind this trend are all in the numbers:

1. Email is a business record critical to daily corporate activity.
  - 52 billion emails sent each day by 2006 (The Radicati Group, Inc.).
  - 2.2 billion IMs sent each day (IDC).
  - 15.8 MB of email sent/received per user each day by 2008 (The Radicati Group, Inc.).
2. Email has become the de facto repository of corporate digital assets.
  - 93 percent of all documents produced since 1999 were created in digital form.
  - 70 percent of electronic data is never produced to hard copy.
  - 70 percent of companies' digital assets are contained in email.

3. Email may contain information on business matters, status reports, inventory lists, minutes of meetings, drafts of documents, business strategies, or other important business decisions, and litigants, both regulatory and civil, are increasingly aware of the legal value of email and aggressively pursuing it as a central investigation and litigation strategy in discovery.
- In 2004, one in five U.S. companies had an employee's emails subpoenaed in the course of a lawsuit or regulatory investigation (*Time Magazine*, 9/20/2004).
  - According to Osterman Research, nearly three out of four enterprises have faced a requirement during the past three years to search through backup tapes to recover old emails in response to a request from the legal department, human resources department, or some other entity within the enterprise.
  - 95 percent of AIIM survey respondents believe the process by which electronic records are managed will be important to future litigation.

### **Tape Backup is Good Enough, Right?**

It is commonplace in today's companies for there to be a disaster recovery plan in place, and for the central cog of this plan to be creation and maintenance of tape backups for the various IT systems, email being at the top of the list. A backup tape of an email system is a copy of messages on the system taken over some regular interval of time—typically a 30, 60, or 90-day snapshot—which is then stored away. In the event of a catastrophic failure of the email systems, the backup tapes are pulled and their data “snapshots” used to replicate the system before the failure. The replication is not going to be 100 percent duplication of the pre-failure environment, but it will get a company back up and running with a good percentage of its most critical messaging data.

Companies need to ensure that not only the text of emails is retained, but that attachments are also stored in the same searchable archive. A number of email management solutions today can capture attachments and make them searchable and retrievable through powerful discovery tools.

In the arena of disaster recovery, tape backup is a viable and satisfactory solution. In the arena of electronic discovery, however, this is not so viable and not so satisfactory a solution. The discovery process is essentially comprised of four components: (1) evidence collection, (2) evidence processing, (3) evidence review, and (4) evidence production.

**Evidence collection** is the process of identifying relevant backup tapes, restoring those tapes, de-duping those tapes (i.e., removing duplicate messages) and identifying relevant and responsive messages by searching the message files for particular keywords. Easy process? Well, are the relevant tapes collected in a single onsite location readily accessible to the e-Discovery team, or as is the more commonplace scenario, are those tapes dispersed over multiple satellite office locations or otherwise offsite with a third-party tape storage vendor? Also, undertaking such an activity requires the identification of personnel to undertake the task. Which critical IT staff are you going to pull off their normal IT duties to devote to this immediate endeavor?

**Evidence processing** is the process of extracting metadata from the email files. Intricacies involved in this process—is this data being properly restored with the messages restored from tape? Is the metadata's integrity being maintained through the restoration process, or has the storage or restoration process itself worked to alter that metadata in legally significant ways?

**Evidence review** entails the design and development of a review database, the hosting of that database, and, typically, the legal review of documents by outside counsel. Depending on the number of employees subject to a discovery request and the associated volume of email data to be reviewed,

database design and development work can become quite substantial and costly, with the basic rule of thumb being the more people subject to discovery the greater this cost. And the greater the volume of data to be reviewed, the more hours of outside counsel review required at hourly billable rates that can readily average more than \$300.

**Evidence production** is creating output of messages deemed to be responsive to the discovery request, typically in PST, PDF, or TIFF format, and if used in litigation, with Bates numbering.

Perhaps there is no better real-world illustration of the pain points involved in conducting e-Discovery from tape than the Wyeth experience during part of its Phen-Fen case. In the Phen-Fen case against Wyeth's sister company and A.H. Robins Inc., the plaintiff sought relevant email messages from an identified list of key employees. Wyeth's tape backup systems, however, couldn't easily isolate messages for the desired employees without incurring significant cost associated with restoring tape data for discovery, i.e.:

- Recreating storage environment for tape restoration, including securing the appropriate tape drives and storage software
- File de-duping and keyword search consulting to cull down data
- Designing and developing a Web database for outside counsel to review data
- Monthly hosting of the review database
- Producing data to the other side in PST, PDF, or TIFF format plus Bates numbering

End result: Wyeth settled with the plaintiff rather than pay estimated e-Discovery costs of up to \$1.7 million.

In addition, questions surrounding restoration and retrieval capabilities are just part of the e-Discovery analysis. For instance, a requesting litigant or regulator has a right to the "best evidence" on the matters requested, and where email and e-file data is involved, this means data whose metadata and secure storage can be established/authenticated. There are also issues regarding the duty to preserve data from future destruction upon notice or anticipation of possible litigation.

There is also the matter of employees saving their business-critical email data locally to their desktop or laptop machine, or to some other storage device like CD or DVD. Osterman Research has found that 77 percent of email users store data locally and that 29 percent of these "local stores" are not captured in the tape backup process. To locate this data in e-Discovery requires the hiring of forensic experts who must go to individual employees and scrub their laptops and hard drives, and/or copy their CDs and DVDs to collect this non-backed up data.

The moral of this story: if backup tape is your primary means of storing email data, your pain points when faced with discovery will be substantial.

### **So, If Not Tape, Then What?**

Today's e-Discovery marketplace is developing new software tools and applications that allow organizations to get away from e-Discovery of backup tapes. One such fast growing solution is email archiving. An email archive is a single repository of corporate email data stored not on backup tape, but on new quick retrieval online storage systems installed within the enterprise environment.

With data collected in a single location, retrieving and reviewing this data becomes a much more straightforward process. Whether employees have stored email data to their local computers in many ways becomes a non-issue since all email traffic is being captured in the archive upon receipt or release from

the enterprise. The producing party can show that mail captured in the archive is duplicative of data stored to the desktop. If questions about mail alteration or authenticity arise, then, “yes,” a requesting party may still have legitimate argument for seeking email off desktops, but as in all discovery processes, courts are balancing the need for production in terms of potential value/relevance to case versus the burden of production. A responding party is in good position to argue desktop retrieval is unnecessary and unduly burdensome when the archive system is capturing all email traffic.

Many of the new archiving solutions feature powerful Web-based search and retrieval tools that allow a responding party to quickly locate the most potentially relevant email data using criteria like time and date of the message, senders, or recipients, and keywords of central importance to the factual allegations of a case or regulatory investigation. This is often a search and retrieval exercise that can be undertaken by a company’s own internal legal staff, by its outside law firm, or a combination of both.

Finally, these new email-archiving solutions provide companies with the ability to convert responsive email data to a variety of output formats—PST, PDF, TIFF, CD, DVD, print—which can be conveniently shared with internal personnel, or outside regulators or opposing litigants. Many of these solutions have the ability to keep detailed logs of the searches run and the data retrieved, and to generate useful audit reports of these logs.

While electronic discovery processes and technologies continue to evolve, one thing is clear-taking a proactive approach to email archiving and discovery is one of the best ways to protect an organization from hefty legal fines and astronomical discovery costs. Since most companies will inevitably be involved in a lawsuit at some point in their existence, now is the time to implement an electronic content management strategy that will prepare them for the legal discovery process.

*Brian E. Seward, Esq., (bseward@ilumin.com) is a Senior Legal Consultant for iLumin Software Services, Inc, a provider of email management solutions. Prior to joining iLumin, Mr. Seward practiced law for thirteen years in Washington, D.C. and New York City. He is a senior member of the iLumin Electronic Discovery and Data Migration services practice, advising on matters of product development and market strategy.*

# Primer: Amendments to the Federal Rules of Civil Procedure

The Federal Rules of Civil Procedure (FRCP) govern civil procedure in the United States district courts. New amendments to the Federal Rules of Civil Procedure address the discovery of electronically stored information. On April 12, 2006, the Supreme Court of the United States approved and forwarded these amendments to Congress, and take effect on December 1, 2006. Certain revisions to the Federal Rules of Civil Procedure address the preservation and discovery of data in electronic media, also known as e-Discovery.

The amendments will revamp existing discovery rules in order to better accommodate discovery directed at information generated by computers, and will affect Rules 16(b), 26(a), 26(b)(2), 26(b)(5), 26(f), 33, 34(a), 34(b), 37(f) and 45, as well as Form 35.

When it comes to FRCP preparation, ask these questions:

- What is an e-Discovery request?
- What are the true costs to produce electronically stored information?
- How can your organization prepare for discussions on electronic discovery prior to a pre-trial conference?
- How do you identify all potentially relevant sources of information?
- What are the different issues concerning discovery of electronically stored information from the conventional discovery of paper records?

This **AIIM Primer** on the **Federal Rules of Civil Procedure** will help you and your organization prepare to respond to e-Discovery requests for information.

## What is it?

---

The Federal Rules of Civil Procedure (FRCP) govern court procedures for civil suits in the United States district courts. Circulated by the United States Supreme Court according to the Rules Enabling Act, the FRCP is then approved by the United States Congress. Supreme Court modifications to the rules are based on recommendations from the Judicial Conference of the United States, the federal judiciary's internal policy-making body.

The Judicial Conference of the United States authorizes its Committee on Rules of Practice and Procedure to appoint an Advisory Committee on the Rules of Civil Procedure, which monitors the effectiveness of the Rules of Civil Procedure and makes recommendations for proposed amendments.

The U.S. district judge has the ultimate authority in courtroom legal procedure, and has a role in advancing common law practice and establishing new positions. When making decisions, the district court judge applies the substantive laws of the state. Federal courts must apply the substantive law of the states as rules of decision in cases where state law is in question. However, the federal courts usually use the FRCP as their rules of procedure. States make their own rules that apply in their own courts, but most states have adopted rules based on the FRCP.

Established in 1938, the rules replaced the earlier Field Code and common law pleadings. Significant revisions were made in 1948, 1963, 1966, 1970, 1980, 1983, 1987, 1993, and 2000. The 2006 revisions

provide practical changes in discovery rules that will make it easier for courts and litigating parties to manage electronic records.

The Field Code and common law pleading was more formal, traditional, and particular in its phrases and requirements. An intermediate step between common law and modern rules, New York attorney David Dudley Field created the Field Code. Adopted in 1848-50, Field's code merged law and equity proceedings. By contrast, the FRCP is based on a notice pleading, which is less formal, created and modified by legal experts, and not as technical in requirements. For example, in a notice pleading, the same plaintiff-bringing suit would not face dismissal for lack of the exact legal term, providing the claim itself was legally actionable. This change gives "notice" of your grievances, and reserves the details for when the case progresses. Actual law and not the exact construction of pleas is the primary focus.

Another system used by a minority of states (e.g., California) is Code Pleading, which is older than notice pleading and based on legislative statute. Code Pleading bridges the gap between obsolete common law pleading and modern notice pleading by placing additional burdens on a party to plea the "ultimate facts" of their case. On the contrary, notice pleading only requires a "short and plain statement" showing that the pleader is entitled to relief. The only exception is when a plaintiff alleges fraud; the plaintiff must plead the facts of the alleged fraud with particularity. (FRCP 8(a)(2)).

## Categories and Rules

Comprised of 11 different categories and 86 different rule sets, the following table outlines the Federal Rules of Civil Procedure:

Category	Category Description	Rules in Category	General Content in Category
I	Scope	1 and 2	Category I describes the purpose of the rules and their role in governing civil action in federal district courts.
II	Commencement of civil suits	3 to 6	Category II contains the rules that provide for the commencement of a civil suit, including the filing, summons, and service of process (legal notice).
III	Pleadings and motions	7 to 16	Category III provides for civil suit pleadings, motions, and defenses and counterclaims. The "complaint" is the plaintiff's pleading. The "answer" is the defendant's pleading.
IV	Parties	17 to 25	Category IV describes the capacities in which a party or parties can be sued. It maintains the provisions describing the mechanisms for the filing of countersuits, joinder claims, class action lawsuits, and other actions.
V	Discovery	26 to 37	Category V contains the rules governing discovery (e-Discovery included). In general, the discovery rules help ensure that neither party is subjected to surprises at trial. In many states discovery can occur only through formal request. In contrast, the FRCP requires parties to divulge certain information without a formal discovery request.

VI	Trial	38 to 53	Category VI provides for the plaintiff's right to a trial by jury or by the court. Additionally, this category contains the rules that describe how cases are assigned for trial, how actions are dismissed, and how subpoenas are handled. On December 1, 2006, FRCP 45 (subpoenas) will be amended to conform with the e-Discovery rules.
VII	Judgment	54 to 63	Category VII maintains the provisions governing legal judgment and costs. "Judgment" is the decree and any other order from which an appeal lies. Category VII judgment rules maintain provisions for establishing new trials, amending judgments, and the enforcement of judgments.
VIII	Provisional and final remedies and special proceedings	64 to 71	Category VIII contains the series of rules that provide for the final provision or remedy of a case. The rules covered in this category include seizure of property, injunctions, offers of judgment, and execution of judgments.
IX	Special proceedings	72 to 76	Category IX contains the rules governing special civil action proceedings, such as condemnation of real and personal property, magistrate judges, and pretrial orders.
X	District courts and clerks	77 to 80	Category X provides direction concerning the business and operations of the district courts. The rules covered in this category include hours of operation, filing of pleadings and orders, trials and hearings, orders in chambers, procedures for books and records maintained by the clerk, the role of stenographers, and transcripts as evidence.
XI	General provisions	81 to 86	Category XI explains to which proceedings the rules apply (United States district courts vs. state courts) and provides direction on their general applicability, jurisdiction and venue, local rules applications, and judges directives.

After years of applying traditional paper discovery rules to electronic discovery, on April 12, 2006, the Supreme Court of the United States approved several proposed amendments to the Federal Rules of Civil Procedure to accommodate the modern practice of discovery of electronically stored information. The goal of the amendments is to recognize the importance of electronically stored information and to respond to the increasingly prohibitive costs of document review and protection of privileged documents. These amendments reinforce the importance of litigants thinking about electronic discovery.

## Amendments

*Amendments to the Federal Rules of Civil Procedure include, according to the Advisory Committee Notes:*

- **Rule 16 — Pretrial Conferences; Scheduling; Management:** New subsections 16(b)(5) and 16(b)(6) provide that the scheduling order may address "disclosure or discovery of electronically stored information" and any agreements "for asserting claims of privilege or of protection as trial-preparation material after production."

- **Rule 26 — General Provisions Governing Discovery; Duty of Disclosure:** Subsection 26(a)(1)(B) is amended to substitute “electronically stored information” for “data compilations” as a category of the required initial disclosures. Subsection 26(b)(2)(B) is added to excuse a party from providing discovery of electronically stored information that is “not reasonably accessible because of undue burden or cost,” but the burden remains on the producing party to make the required showing. Subsection 26(b)(5)(B) is added, providing a procedure for a party to maintain “a claim of privilege or of protection as trial-preparation material” concerning any discovery, even after it is produced. As the Advisory Committee Notes clarify, “Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production,” but rather it “provides a procedure for addressing these issues.” Finally, similar to new Rules 16(b)(5) and 16(b)(6), new subsections 26(f)(3) and 26(f)(4) are added to make sure the Rule 26(f) conference includes a discussion of any issues relating to “disclosure or discovery of electronically stored information,” and “claims of privilege or of protection as trial-preparation material.” Form 35 (Report of Parties’ Planning Meeting) is revised to reflect the changes to Rule 26(f).
- **Rule 33 — Interrogatories to Parties:** Rule 33(d) is amended to specify that electronically stored information may qualify as appropriate business records from which an answer to an interrogatory may be derived or ascertained.
- **Rule 34 — Production of Documents, Electronically Stored Information, and Things:** Rule 34(a) is amended to reference electronically stored information, and Rule 34(b) is amended to supply a procedure for specifying and objecting to the form in which electronic information is to be produced. Under new subsections 34(b)(ii) and 34(b)(iii), the default form for producing electronically stored information is that “in which it is ordinarily maintained [or] reasonably usable,” and “a party need not produce the same electronically stored information in more than one form”.
- **Rule 37 — Failure to Make Disclosure or Cooperate in Discovery; Sanctions:** New subsection 37(f) is added which states, “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system.” The Advisory Committee Notes explain that the premise for this amendment is that ordinary computer use necessarily involves routine alteration and deletion of information for reasons unrelated to litigation.
- **Rule 45 — Subpoena:** Rule 45 is amended to incorporate the changes to Rule 26(b) and Rule 34 as applied to the production of documents by third parties pursuant to a subpoena.
- **Proposed Rule of Evidence 502 — Attorney-Client Privilege and Work Product:** Waiver By Disclosure: The Advisory Committee on Evidence Rules has proposed a new Rule 502 that would formalize a “subject matter” waiver of the attorney-client or work product privileges through voluntary disclosure, with an important exception for “inadvertent” disclosure. Specifically, upon a voluntary disclosure of privileged or work product information, Rule 502(a) would further require production of “undisclosed information concerning the same subject matter if that undisclosed information ought in fairness to be considered with the disclosed information.” Rule 502(b), however, would provide an exception where “the disclosure is inadvertent . . . and if the holder of the privilege or work product protection took reasonable precautions to prevent disclosure and took reasonably prompt measures, once the holder knew or should have known of the disclosure, to rectify the error, including (if applicable) following the procedures in Fed. R. Civ. P. 26(b)(5)(B).” The Committee Notes explain that the new Rule 502 would resolve disputes over the effect of inadvertent disclosure and selective waiver of privileged or work product information, and responds to the prohibitive litigation cost of reviewing and protecting privileged or work product material, particularly in cases involving electronic discovery.
- **Local e-Discovery Rules:** Several local jurisdictions have already amended their court rules to reflect the importance of discovery of electronic data. A summary of the applicable local rules can be provided upon request.

- **Citation of Unpublished Opinions:** The Supreme Court also approved new Federal Rule of Appellate Procedure 32.1, which will allow litigants to cite any “federal judicial opinion, order, judgment, or other written disposition” issued on or after January 1, 2007, even if it has been given an “unpublished” or similar designation. The effect of the new rule, as stated in the Committee Note, is that “a court of appeals may not prohibit a party from citing an unpublished opinion of a federal court for its persuasive value or for any other reason.”

## e-Discovery

---

Rules 26 and 34 of the Federal Rules of Civil Procedure specifically cover discovery and disclosure of information that is relevant to civil suits.

Discovery is the part of the litigation process in which opposing parties exchange relevant information and testimony. This process helps both sides understand the facts and evidence before the commencement of a trial.

Electronic discovery (e-Discovery or ediscovery) refers to “any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case”. This includes but is not limited to computer forensics, email archiving, online review, and proactive management. The emergent e-Discovery field augments legal, constitutional, political, security, and personal privacy issues.

*FRCP 26(b)(5)* deals with General Provisions Governing Discovery; Duty of Disclosure; Discovery Scope and Limits; and Claims of Privilege or Protection of Trial Preparation Materials. *FRCP 34(b)* focuses on the Production of Documents, Electronically Stored Information, and Things. These amendments to the FRCP address a common corporate problem: the volume of electronically stored information and its maintenance. During an electronic discovery process, all types of data serve as evidence such as text, images, calendar files, databases, spreadsheets, audio files, animation, websites, and computer programs. Because of lax corporate management, email is often the most valuable source of evidence in civil or criminal litigation.

A common, specialized form of e-Discovery is computer forensics (cyberforensics), which is “the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law”. Computer forensics executes a structured investigation while maintaining a documented chain of evidence to discover the contents of the hard drive of a specific computer. After physically isolating the computer, investigators make a digital copy of the hard drive and store the original computer in a secure facility. The cyberforensics team performs all investigation on the digital copy.

Under these amendments, corporations must proactively manage the electronic discovery process to avoid sanctions, unfavorable rulings, and a loss of public trust. Corporations must be prepared for early discussions on electronic discovery with all departments. Topics should include the form of production of electronically stored information and the preservation of information. Records management and IT departments must have made available all relevant electronically stored information for attorney review.

## The Sedona Guidelines: Best Practice Guidelines for Managing Information

---

The Sedona Conference is a 501(c)(3) research and educational institute consisting of academics, industry experts, lawyers, and judges dedicated to the advancement of law and policy in the areas of antitrust law, intellectual property rights, and litigation.

The following guidelines are recommended best practices from the Sedona Conference:

1. An organization should have reasonable policies and procedures for managing its information and records.
2. An organization's information and records management policies and procedures should be realistic, practical, and tailored to the circumstances of the organization.
3. An organization need not retain all electronic information ever generated or received.
4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval, and ultimate disposition or destruction of information and records.
5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation, or audit.

## Guidelines for the Federal Rules of Civil Procedure Preparation

---

1. Map out all places where electronic information is stored. Locate any data source including deleted data, data on systems no longer in use, data in remote or third-party locations, copies of production data used in demos, test systems, etc.
2. Update your records retention policy to include all electronic information. Corporate retention policies should be applied to email and other electronic records.
3. Ensure your litigation hold policy fully covers all electronic information including backup tapes. Make sure your litigation hold policy document includes rules for all relevant electronic records, such as email, electronic documents, scanned documents, and backup tapes.
4. Establish systems that simplify identification, retrieval, and production of potentially relevant data. Purchase software that provides Online Risk Management and Web Application Security.
5. Establish a Plan of Action. Evaluate how you can organize your data storage to proactively prepare for electronic discovery requests.

## Sources

---

1. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
[http://www.foley.com/files/tbl\\_s31Publications/FileUpload137/3345/IP%20Lit%20Alert%20amendments%20to%20ediscovery.pdf](http://www.foley.com/files/tbl_s31Publications/FileUpload137/3345/IP%20Lit%20Alert%20amendments%20to%20ediscovery.pdf)
2. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
[http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_032032.hcsp?dDocName=bok1\\_032032](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032032.hcsp?dDocName=bok1_032032)
3. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
<http://www.s-ox.com/News/detail.cfm?articleID=1917>
4. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
[http://www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf)

5. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
<http://www.uscourts.gov/rules/Reports/ST09-2005.pdf#page=110>
6. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
<http://www.h2law.com/CM/BreakingLegalNews/BreakingLegalNews297.asp>
7. "New Federal Rules to Civil Procedure (FRCP) Rules 26 and 34":  
<http://www.legalpub.com/publications/The%20New%20E-Discovery%20Rules.htm>
8. "e-Discovery": [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci1150017,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150017,00.html)
9. "e-Discovery": <http://en.wikipedia.org/wiki/E-Discovery>
10. "Computer Forensics": [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci1007675,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1007675,00.html)
11. "New E-Discovery Rules & The Attorney-Client Privilege: A Middle Ground for Waiver?" by Julie Anne Halter, Preston Gates & Ellis LLP <http://www.prestongates.com/westlaw/HalterCLN.pdf>
12. "Amendments to the Federal Rules of Civil Procedure":  
[http://www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf)
13. "Federal Rules of Civil Procedure" by Judi Hasson:  
[http://en.wikipedia.org/wiki/Federal\\_Rules\\_of\\_Civil\\_Procedure](http://en.wikipedia.org/wiki/Federal_Rules_of_Civil_Procedure)
14. "Interview of Judge Shira A. Scheindlin." The Sedona Conference, 2004.  
<http://www.thesedonaconference.org/dltForm?did=ScheindlinInterview.pdf>
15. Baldwin-Stried, Kim. "E-Discovery and HIM: How Amendments to the Federal Rules of Civil Procedure Will Affect HIM Professionals." *Journal of AHIMA* 77, no.9 (October 2006): 58-60ff.
16. AHIMA e-Discovery e-HIM Workgroup. "The New Electronic Discovery Civil Rule." *Journal of AHIMA* 77, no. 8 (2006): 68A-H.
17. US Courts. "Summary of the Report of the Judicial Conference Committee in Rules of Practice and Procedure." September 2005, [www.uscourts.gov/rules](http://www.uscourts.gov/rules).
18. Federal Rules of Civil Procedure, 2005.  
<http://judiciary.house.gov/media/pdfs/printers/109th/civil2005.pdf>
19. "The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age," September 2005, [www.thesedonaconference.org](http://www.thesedonaconference.org)
20. Ronan, Timothy G. "A Primer on the Pitfalls of Failing to Preserve Electronic Evidence." *Connecticut Lawyer*, May 2004. [www.pullcom.com/docs/ElectronicEvidence\\_TGR\\_May04.pdf](http://www.pullcom.com/docs/ElectronicEvidence_TGR_May04.pdf)

*Janelle Julien is associate editor of AIIM E-DOC Magazine ([jjulien@aiim.org](mailto:jjulien@aiim.org)).*

# Industry Watch: Electronic Records Management: For Most, It's Still "Waiting for Godot"

## KEY FINDINGS

---

### Managing Electronic Information Still #2 Priority in Most Organizations (vs. Paper)

In general, end users believe they have done a reasonable job of putting in place formal programs to manage paper-based information. When it comes to electronic information, in general organizations report far less structure.

### Many Records Management Programs Just Cover the Tip of the Iceberg

As the survey pushed participants for more granularity with regards to their records and information management program, it became apparent that many end users have yet to address important elements in a truly comprehensive program.

### Organizations—Especially Medium Sized Ones—Are Vulnerable to New e-Discovery Rules

There are some aspects of the new e-Discovery rules announced December 1, 2006 (such as the safe harbor for inadvertent deletions) that are positive, given the extremely ambiguous legal environment that exists for "electronically-stored information" (the term used in the new rules). However, as is evident from the results of this survey (and other AIIM industry Watch surveys), the expectation that the new rules create—that organizations have control over their electronically-stored information—is problematic at best for most organizations.

### In Searching for an Electronic Records Solution, Organizations Stress the Basics

The decision to implement an electronic records management solution hinges on three primary drivers: "improve efficiency and productivity", "compliance", and "risk management/business continuity". It is surprising that even in a survey specifically focused on records management, and with a sample dominated by "document management specialists", the "productivity" and "efficiency" benefits of RM technologies are understood and valued.

### RM Outsource Opportunities Exist, Especially as RM Requirements Grow More Complex

As organizations struggle with the complexity of records management requirements, they are increasingly realizing that an outsourced solution is at least something that should be considered. The reason for the shift is the increasing risks of "doing it wrong", and the increasing complexity of "doing it right".








## ABOUT THE SURVEY

---








This survey was delivered via an online survey instrument ([www.zoomerang.com](http://www.zoomerang.com)) during the 4th quarter of 2006. A total of 821 end users participated in the survey. The participants reflect a broad sample of

organizations in terms of size, with 17% drawn from small organizations (less than 100 employees), 26% from mid-sized organizations (100-1,000 employees), and the remainder from large and very large organizations (more than 1,000 employees).








The results reported in the survey highlight the major findings from the survey. A complete question set, along with breakouts of the data by company and organization size, can be found in the appendix.

Approximately how many employees are there in your ORGANIZATION as a whole?			
1 to 100		141	17%
101 to 500		112	14%
501 to 1,000		102	12%
1,001 to 5,000		174	21%
5,001 to 10,000		81	10%
10,001 to 50,000		139	17%
Over 50,000		72	9%
<b>Total</b>		821	100%

There was heavy participation in the survey by those that could be considered “closest to the action” in their organizations with regards to document and records management. Over half of those participating described themselves as “document management specialists”. This category includes, but is not limited to, those who are records managers within their organizations. The percentage of document “specialists” in this survey is higher than is typical for other AIIM surveys.

Pick the choice that best describes your role within your organization:			
President or CEO		46	6%
Line-of-business or process owner		114	14%
Document management specialist		447	56%
CIO, IT executive or IT manager		149	19%
CFO or finance executive		12	2%
Legal counsel		12	2%
Security manager or executive		17	2%
<b>Total</b>		797	100%

Almost 60% of the respondents were from the U.S., followed by the United Kingdom (14%), Canada (13%), rest of Europe (6%). End users from 49 countries participated in the survey.

In which country are you located?			
Australia		17	2%
Brazil		5	1%
Canada		103	13%
France		3	0%
Germany		6	1%
United Kingdom		115	14%
United States		488	59%
Other, please specify		85	10%
<b>Total</b>		<b>822</b>	<b>100%</b>

A significant number of participants (26%) were from government at all levels, followed by financial services, including banking, finance, insurance (13%), utilities, oil and gas (8%), professional services/consultants (8%), manufacturing and engineering (6%), and education (6%).

In which industry sector does your organization operate ?			
Banking & Finance		71	9%
Insurance		37	4%
Chemicals & Pharmaceuticals		38	5%
Construction & Building		4	0%
Consultant		63	8%
Education		48	6%
Govt & Pub Serv – Federal or National		72	9%
Govt & Pub Serv – Provincial or State		54	7%
Govt & Pub Ser – Local, County, or Town		99	12%
Healthcare		27	3%
IT – NOT in the ECM industry – HARDWARE		5	1%
IT – NOT in the ECM industry – SW or SERV		18	2%
IT – a provider of ECM products and services		0	0%
Legal		23	3%
Manufacturing & Engineering		52	6%
Non-profit		18	2%
Retail		4	0%
Telecommunications & Media		18	2%
Transportation & Distribution		13	2%
Utilities, Oil & Gas		65	8%
Wholesale		1	0%
Other, please specify		94	11%
<b>Total</b>		<b>823</b>	<b>100%</b>

**Managing Electronic Information Still #2 Priority in Most Organizations (vs. Paper)**

Throughout the survey, we were specific in identifying whether the question related to the management of INFORMATION or RECORDS or both. Participants were asked to interpret the term INFORMATION management as referring to the general use and management of information of all types (paper, structured electronic information, unstructured electronic information). Participants were asked to interpret the term RECORDS MANAGEMENT as referring to the subset of information that is expressly classified and retained as official organizational documentation.

In general, end users believe they have done a reasonable job of putting in place formal programs to manage paper-based information. Over 60% of end users report they have formal programs in place to manage paper-based records, the security and privacy of paper-based information, compliance, and disaster recovery.

Please indicate if your organization has formal programs (in other words, specific programs that include designated employees, policies, procedures, and information technology) that address the following topics relative to PAPER-BASED information:

Top number is the count of respondents selecting the option. Bottom % is percent of total respondents selecting the option.	YES	NO	Not sure
Classification of information as records	605 74%	176 21%	38 5%
Information Security	637 78%	119 15%	61 7%
Data Privacy	616 76%	118 14%	80 10%
Disaster Recovery/Business Continuation	557 68%	185 23%	75 9%
Database Management	518 64%	176 22%	116 14%
Risk management	470 58%	199 25%	140 17%
Litigation Readiness	355 44%	251 31%	202 25%
Regulatory Compliance	560 69%	150 18%	104 13%

When it comes to electronic information, in general organizations report far less structure. Those reporting formal programs for managing the electronic information needed for regulatory compliance were 12 percentage points less than for paper-based information, and 17 percentage points lower when dealing with the classification of electronic records vs. paper records.

Please indicate if your organization has formal programs (in other words, specific programs that include designated employees, policies, procedures, and information technology) that address the following topics relative to ELECTRONIC information:

Top number is the count of respondents selecting the option. Bottom % is percent of total respondents selecting the option.	YES	NO	Not sure
Classification of information as records	466 57%	303 37%	48 6%
Information Security	686 84%	88 11%	43 5%
Data Privacy	624 76%	123 15%	69 8%
Disaster Recovery/Business Continuation	631 77%	120 15%	66 8%
Database Management	573 71%	133 16%	103 13%
Risk management	424 53%	217 27%	165 20%
Litigation Readiness	292 36%	309 38%	206 26%
Regulatory Compliance	463 57%	213 26%	135 17%

The data suggests that organizations of all sizes are relatively mature in paper-based records management. Except for the smallest organizations (less than 100 employees), typically 75-80% of survey participants report a formal program for paper-based records management. There is a significant drop-off when the focus shifts to electronic records. Typically only 55-60% report a formal program to manage electronic records; among organizations with 5,000-10,000 employees, the percentage drops to less than half, 48%.

	% with a records management program—PAPER	% with a records management program—ELECTRONIC
State and local government	77%	57%
Financial services	79%	57%
Manufacturing and engineering	71%	54%
Utilities, oil, and gas	83%	63%

The most significant weakness in the management of paper-based information relates to litigation readiness (also a significant weakness on the electronic side). Given the recent changes in discovery and e-Discovery rules (new changes in Federal Rules of Civil Procedure announced December 1) this weakness in managing both paper and electronic information will become more of a strain in the months ahead for many organizations.

Mid-sized organizations are particularly vulnerable in this regard. The percentages that report specific programs relative to litigation readiness are as follows:

	% with a litigation readiness program—PAPER	% with a litigation readiness program—ELECTRONIC
101-500 employees	39%	27%
501-1,000 employees	40%	34%
1,001 to 5,000 employees	42%	37%

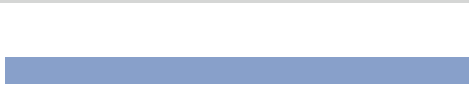








**Many Records Management Programs Just Cover the Tip of the Iceberg**

---

As the survey pushed participants for more granularity with regards to their records and information management program, it became apparent that many end users have yet to address important elements in a truly comprehensive program.

Over 70% of formal programs include such basic elements as retention, appropriate use of email, and ownership of information assets. This is consistent with past AIM surveys. However, as more complicated issues are addressed—i.e., confidentiality, extension of policies down the supply chain, and control of remote information—the percentage of end users typically reporting a formal program drops by 40-50%.

Indicate if your organization has specific policies or procedures that address the following issues. (Check all that apply.)

Ownership of records and information, i.e., who owns the information created and received by an organization.		547	69%
Employee privacy at work, i.e., the employer's right to monitor and review employee email.		611	77%
Records retention and/or classification		620	79%
Email usage: e.g., business vs. non-business communications, storage, purge, archival		563	71%
Classification or coding of information, i.e., as confidential, vital, or trade secrets.		389	49%
Transmission of confidential or trade secret information.		414	52%
The applicability of your organization's information management policies to third parties, such as contractors.		410	52%
The applicability of your organization's records management policies to third parties, such as contractors.		346	44%
Rules for telecommuters, mobile workers, and "road warriors" using notebook computers and other devices outside the office.		392	50%

Significant gaps with regards to the more complicated issues associated with information management are particularly evident in looking at organizational size. For example, only 41% of mid-sized organizations (101-500 employees) report policies and procedures related to transmission of confidential data, 34 points lower than that reported by the largest organizations (over 50,000 employees). The same carries through to extending information management policies through the supply chain and to applying information management policies to remote workers (both are 27 points lower for those with 101-500 employees).

The surface nature of many programs is evident from a few somewhat basic questions related to executive communications, policy statements, and training. These are core indicators relative to the seriousness of a program, and one would expect to generate a much higher positive response.

For example, barely 60% of user organizations report receiving an executive communication over the past 18 months about records and information management issues. Only 47% have a statement outlining a



records or information management policy in employee manuals. Only four in ten end user organizations provide training programs for employees on records and information management.

Again, mid-sized organizations have gaps in their programs, exposing their organizations to significant risk.



	Statement about RM in employee manual? % YES	Employer takes RM seriously?
% STRONGLY AGREE		
101-500 employees	42%	28%
501-1,000 employees	48%	30%
1,001 to 5,000 employees	43%	24%
Over 50,000 employees	65%	50%

A few comments from participants are illustrative of the challenge of matching actions to intent in many organizations:

- Executives don't view "records issues" as worthy of their direct attention.
- We have just a broad statement that records management is important. There was no action to substantiate the statement.
- Records and information management is still the last thing on their minds.
- The policy is vague and not easily found—most employees don't know where to find it and it leaves RIM up to the business units.
- Records management is not even mentioned in new employee orientation.
- It is my opinion that Records are a very low priority here.

Has an executive communicated with you via an internal memo, email message, or presentation about records and information management issues in the past 18 months?			
Yes		492	61%
No		320	39%
<b>Total</b>		813	100%

Is there a statement from your CEO or other high-level executive regarding the importance of records and information management that is a standard part of your employee manual, records management manual, or other policy or procedure that is provided to all employees?			
Yes		387	47%
No		428	53%
<b>Total</b>		817	100%

Does your organization regularly deliver training for employees on records and information management issues?			
Yes		338	41%
No		479	59%
<b>Total</b>		817	100%

This gap between actions and intentions is reflected in other questions as well. 75% of end users “strongly” or “somewhat” agree with the statement, “My organization takes records and information management issues seriously.” When enforcement of policies is considered, though, the gaps in programs emerge. Only 39% “strongly” or “somewhat” agree that “records and information management directives are consistently enforced.”

A look at the vertical breakouts highlights the lack of rigor that characterizes many records and information management programs. For example, only 5% of state and local officials would agree that their organizations are serious about records and information management.



	“Takes records and information management seriously” STRONGLY AGREE	“Records and information management directives consistently enforced” STRONGLY AGREE
State and local government	27%	5%
Financial services	44%	18%
Manufacturing and engineering	27%	10%
Utilities, oil, and gas	40%	11%

**Organizations—Especially Medium Sized Ones—Are Vulnerable to New e-Discovery Rules**

There are some aspects of the new e-Discovery rules announced December 1, 2006 (such as the safe harbor for inadvertent deletions) that are positive, given the extremely ambiguous legal environment that exists for “electronically-stored information” (the term used in the new rules).

However, as is evident from the results of this survey (and other AIIM Industry Watch surveys), the expectation that the new rules create—that organizations have control over their electronically-stored information—is problematic at best for most organizations.

This is particularly clear in the context of e-Discovery. Barely half of those participating in the survey responded positively to the question, “Does your organization have a formal process for ensuring that all information potentially relevant to pending or current lawsuits, audits, and/or investigations?”

Does your organization have a formal process for ensuring that all information potentially relevant to pending or current lawsuits, audits, and/or investigations is preserved? Such processes are often called “Records Hold,” “Legal Hold,” or “Disposal Suspension.”			
Yes		428	53%
No		380	47%
<b>Total</b>		814	100%

The “good news” about the new Federal Rules for Civil Procedure are that they finally establish a framework for the management of electronically stored information. The “bad news” is that organizations are expected to measure themselves against this framework.

This is an area in which the largest companies have at least tried to make headway. In response to the question of whether a formal process exists relative to “Records Holds” or “Legal Holds”, 84% of the largest organizations in the survey (over 50,000 employees) responded “YES”. For most organizations with 101 to 5,000 employees, though, typically less than half have such procedures.

Medium-sized organizations in particular seem to have engaged in wishful thinking or rationalization over the past five years as it increasingly became apparent that the bar was rising in terms of managing electronic information. Many organizations reacted to Sarbanes-Oxley by concluding, “It doesn’t relate to us. We’re not a public company.” The same logic seems true in the reactions to the information management requirements of HIPAA. Or countless other compliance and regulatory requirements related to information management.

Organizations will not be able to escape the expectations associated with the new Federal Rules of Evidence and e-Discovery. They apply to organizations of all sizes and in all segments.

Once again, the comments are illustrative of the challenge facing many organizations:

- We have an informal policy that the RM Clerk will be notified so these documents can be labeled and stored in a vault. As it is informal, it is not always followed.
- As with all questions of policy - the policies are on paper, but compliance by employees is not enforced. No mechanism exists for enforcement except in the occasional case of an audit or a call for information from a higher command.
- Paper is nailed down. Electronic is still being refined.
- This is an area of risk that has been identified to management, however no steps to formalize a process/policy have been initiated at this time.
- We have procedures for communicating Legal Holds; however, no procedures in place to ensure compliance. No training offered as of yet, but that is something we will be addressing.
- We used to, but there has been so much turnover in our Law department that our Litigation Hold process got lost somewhere along the line!
- One of our biggest current gaps.









State and local governments appear to be quite unprepared to the new world of e-Discovery, with less than half of those surveyed reporting a formal policy to handle “Legal Holds” and “Records Holds”.

	“Formal process for legal holds or records holds?”
State and local government	45%
Financial services	69%
Manufacturing and engineering	65%
Utilities, oil, and gas	58%

**In Searching for an Electronic Records Solution, Organizations Stress the Basics**

The decision to implement an electronic records management solution hinges on three primary drivers: “improve efficiency and productivity”, “compliance”, and “risk management/business continuity”. It is surprising that even in a survey specifically focused on records management, and with a sample dominated by “document management specialists”, the “productivity” and “efficiency” benefits of RM technologies are understood and valued. Past AIIM surveys focused on capture and ECM have reached similar conclusions. It is important that suppliers and resellers demonstrate not only the compliance and risk reduction benefits of an electronic records management solution, but also the major efficiencies gained from a deployment.

Think about the reasons why you might implement electronic records management technologies in your organization. Please check the TWO that are the MOST important (please check only TWO).

Compliance		401	50%
Leadership, competitive advantage		50	6%
Improve efficiency and productivity		480	60%
Risk management/Business continuity		297	37%
Better customer service		144	18%
Reduce costs		147	18%
Faster turnaround, improved response		121	15%
Increased profits, better performance		51	6%

There is significant variation in how vertical segments view these market drivers. Those in the public sector—perhaps because of the close link between these systems and their ability to satisfy constituent demands—clearly understand the link between effective records management and efficiency and customer service. State and local employees are clearly on the front lines when it comes to the customer impact of their records management system choices. The drivers for the private sector respondents were significantly more focused on avoiding risk than improving service.

	Manuf	Util	Finance	S&L Govt
Compliance	67%	62%	59%	40%
Leadership, competitive advantage	4%	6%	4%	2%
Improve efficiency and productivity	67%	61%	50%	72%
Risk management/Business continuity	35%	45%	50%	24%
Better customer service	2%	8%	13%	34%
Reduce costs	18%	14%	21%	17%
Faster turnaround, improved response	8%	8%	7%	24%
Increased profits, better performance	12%	8%	3%	3%

Consistent with past AIIM surveys, when it comes to making the final decision about an electronic records management solution, RM staff are often “influencers” rather than “deciders”.

Who in your organization has THE MOST IMPORTANT role in determining whether or not to implement an electronic records management solution? (Select one.)			
Legal		99	13%
Information Technology		187	24%
Tax/Audit		9	1%
Records Management		178	23%
Operations/Administration		141	18%
Compliance/Risk		60	8%
Line of Business		74	9%
Finance		35	4%
<b>Total</b>		<b>783</b>	<b>100%</b>

The intersection between Legal, IT, and RM is clearly critical to development of an effective solution. The relatively even split between these functions when forced to choose “THE MOST IMPORTANT” can be viewed as a reflection of the importance of this intersection.

	Legal	IT	RM	Ops/Admin
101-500 employees	10%	18%	32%	24%
501-1,000 employees	13%	33%	27%	12%
1,001-5,000 employees	10%	25%	23%	17%
5,001-10,000 employees	15%	28%	25%	15%
10,001-50,000 employees	21%	27%	15%	14%
Over 50,000 employees	17%	23%	26%	4%

In thinking about a records management solution, the first priority for most organizations is getting “the basics” in order. For example, the following factors are “extremely important” in considering a records management solution:

- 85% Easing the capture, preservation, and sharing of electronic information.
- 56% Easing the capture, preservation, and sharing of hardcopy information.
- 67% Providing the foundation for rapidly deploying consistent RM practices, policies, and procedures across business units.
- 67% Enhancing accountability, avoiding risks, and improving access to information for discovery and litigation support.
- 67% Reducing time and labor needed to reconstruct information in the event of disaster or loss.
- 64% Enabling compliance through RM best practices.
- 57% Controlling email.

In terms of matching these priorities to budget allocations, end users are very consistent. For example, 42% of end users say they have “already allocated” budget to address the priority of “easing the capture, preservation and sharing of electronic information”, and another 28% have budget allocated in the next budget cycle. The 70% who have already allocated budget or have it planned for the next cycle for easing the capture, preservation, and sharing of electronic information was the highest of all the challenges under consideration by end users.





**RM Outsource Opportunities Exist, Especially as RM Requirements Grow More Complex**

As organizations struggle with the complexity of records management requirements, they are increasingly realizing that an outsourced solution is at least something that should be considered. Among those surveyed, 30% indicate that they would be “likely” or “very likely” to consider an outsourced RM solution.

This 30% that would consider an outsourced RM is likely higher than it might have been as recently as five years ago. The reason for the shift is the increasing risks of “doing it wrong”, and the increasing complexity of “doing it right”. This combination in other IT areas often represents an ideal opening for an outsourced solution. The percentage that would consider an outsourced solution—as well as the percentage that would “never” consider an outsourced solution—is consistent across organization size. There is some variation across major vertical industries in terms of their willingness to consider an outsourced solution.

	% “very likely” or “likely” to consider an outsourced RM solution	% that would “never” consider an outsourced RM solution
State and local government	32%	15%
Financial services	33%	12%
Manufacturing and engineering	34%	16%
Utilities, oil, and gas	19%	17%

In considering an outsourced solution, the MOST important consideration is accessing the information (69% ranking “extremely important”), followed by mitigating compliance risks (56%) and cost reduction (48%). There is a great deal of variation in these results by organization size. For example, “mitigating compliance risks” was significantly more important for the larger organizations in the sample, while mid-sized organizations place a higher premium on information access.

In thinking about an electronic records management solution for your organization, how likely overall would you be to consider an outsourced solution?			
Very likely		90	11%
Likely		152	19%
Not likely		442	56%
Never		110	14%
<b>Total</b>		<b>794</b>	<b>100%</b>

Security (84%), lack of control and flexibility (71%), and concern about communications with the outsource partner (61%) are the top three obstacles that end-users see in implementing an outsourced RM solution.

What are (or would be) the primary obstacles in your organization to implementing an outsourced electronic records management solution? (Select all those that apply.)			
Concern about communication effectiveness between organization and outsource partner.		463	61%
Uncertainty about how to measure performance.		261	34%
Concern about security issues.		639	84%
Concern about compliance issues.		427	56%
Lack of internal experience in managing outsourced relationships.		237	31%
Opposition from the IT department.		230	30%
Opposition from the records management staff.		215	28%
Lack of control and flexibility.		545	71%

There is a good deal of overlap in terms of the perceived obstacles across vertical industries. In general, manufacturing and state and local government end users are less concerned about the compliance issues associated with an outsourced relationship. Manufacturing end users worry about having sufficient internal experience to effectively manage an outsourced relationship. And utilities voice relatively larger concerns than their peers about potential opposition from their RM staffs.

	Manuf	Util	Finance	S&L Govt
Concern about communication effectiveness between organization and outsource partner	69%	57%	61%	62%
Uncertainty about how to measure performance	35%	28%	32%	35%
Concern about security issues	81%	88%	83%	84%
Concern about compliance issues	58%	65%	71%	54%
Lack of internal experience in managing outsourced relationships	42%	30%	22%	30%
Opposition from the IT department	29%	37%	32%	35%
Opposition from the records management staff	27%	43%	28%	30%
Lack of control and flexibility	75%	73%	78%	77%

It is interesting that those who describe themselves as “document management specialists” see the great likelihood of internal opposition from IT (36%) and the RM staff (34%) as a potential obstacle to an outsourcing relationship. IT executives have a relatively high opinion of their ability to overcome internal opposition to outsourcing, with only 23% citing this as a potential obstacle.

68% of those responding do believe that there are certain types of documents that would NEVER be okay to outsource. The 385 comments made to this question provide insight into the concerns that end users have with particular types of documents. Some of the areas mentioned frequently in the comments were: 1) proprietary or trade secret information; 2) personnel and human resource information; 3) medical records; 4) confidential information; and 5) financial information.

*AIIM Industry Watch is published by AIIM.*