

A PRACTICAL GUIDE TO THE LITIGATION READINESS OF ELECTRONICALLY STORED INFORMATION (ESI)

AXS-One White Paper prepared by Thomas Bookwalter, CEO FMDC





→ Copyrights

© 2007 AXS-One Inc. All rights reserved. AXS-One, the AXS-One logo, "Access Tomorrow Today," and AXSPoint are registered trademarks of, and AXS-One Compliance Platform, AXS-One Central, AXS-One Retention Manager, AXS-One Rapid-AXS, AXS-Link for Desktop, AXS-Link for SAP, AXS-Link for Lotus Notes, AXS-Link for Microsoft Exchange, AXS-One Data Archive Translator, AXS-Link for File System Archiving, AXS-Link for .PST Management, AXS-One Supervision, AXS-One Case Management, AXS-One Compliance Platform – Hosted Solution, "The Records Compliance Management Company" and AXS-Link are trademarks of, AXS-One Inc., in the U.S. All other company and product names are trademarks or registered trademarks of their respective companies.

AXS-One Inc.
301 Route 17 North
Rutherford, NJ 07070
(201) 935-3400
www.axsone.com



→ Contents

▶ Overview	4
▶ Section 1: Introduction	5
▶ Section 2: Overview of ESI Rules	8
▶ Section 3: Guidelines for Action	10
▶ Section 4: How Prepared Are You?	15
▶ Section 5: Conclusions	17
▶ Section 6: About AXS-One	18
▶ Section 7: More Information	19

OVERVIEW

On December 1st 2006, new rules for the preparation and discovery of electronic records in U.S. Federal courts - The Federal Rules of Civil Procedure (FRCP) were enacted. The rules will potentially affect every organization in the United States and beyond. An important change embodied throughout the FRCP is the recognition of “electronically stored information” (ESI) as a category of evidence equal to paper documents. The rules have significant impact on organizations’ electronic records management policies, which must now be considered from an IT as well as legal perspective.

This guide is divided into three major parts.

1. Introduction which highlights the complexity of the issues and summarizes the Guidelines for Action.
2. An Overview of ESI rules from various jurisdictions.
3. A discussion of the Guidelines for Actions that companies should consider and if applicable act upon.



→ 1. Introduction


The fundamental questions with respect to the changes in the courts regarding the handling of Electronically Stored Information are:

- ▶ What is the impact on companies of the recent rules respecting electronic evidence?
- ▶ What are the specific actions, if any, that would be both prudent and reasonable for companies to take now?

Federal court is not the only jurisdiction where ESI rules are being developed. All courts, at least in the U.S., are working to create a framework for handling ESI as evidence. The new FRCP rules are just one version of those rules. ESI rules and requirements affect any company that is in or anticipates litigation, state or federal, that will involve electronically stored information as evidence. In other words, this is an issue that impacts almost every company.

There is much more complexity to the courts' perspectives on ESI than first meets the eye. Much of the recent focus has concentrated on the changes to the FRCP. In addition to the work done by the Advisory Committee on Federal Rules (the group that authored the most recent changes to the FRCP), numerous other groups have been addressing the same issues for other courts for some time. These groups include:

- ▶ CCJ (Conference of Chief Justices – Working Group on Electronic Discovery)
- ▶ Federal District of Delaware – Default Standards for the Discovery of Electronic Evidence
- ▶ Ninth Federal Circuit
- ▶ Local districts in AR, CA, DE, FL, KS, MS, NJ, NY, PA, TX, WY
- ▶ Sedona Principles from the Sedona Conference
- ▶ ABA Civil Discovery Standards (29 and 31)
- ▶ Numerous State courts and legislations
- ▶ Foreign jurisdictions in the UK, Australia, France, Germany, Japan and many more



ESI Rules are indicative of a broader trend that acknowledges the importance of proper handling by companies of their ESI. The ESI Rules were developed specifically to address handling of ESI for litigation. Numerous regulators such as the SEC, HHS and others have also been creating rules as well. One thing is clear, ESI handling requirements are here to stay. Courts everywhere are addressing related issues every day. Companies will not be able to ignore the impact much longer without significantly increasing their risk and liability. Additionally, the longer they delay, the more likely costs will be staggering.

The implications of the rules surrounding ESI suggest several steps that companies should take to protect themselves in litigation. The following steps are prudent preparation for any company that regularly participates in litigation regardless of jurisdiction.

The guidelines fall into two broad categories:


1. Steps an organization should take to prepare itself and its people; and
2. Steps an organization should take to prepare its electronically stored information. The following guidelines will be explored more fully in the third part of this paper.

STEPS TO PREPARE THE COMPANY AND ITS PEOPLE

1. Keep key IT personnel well informed of ESI Rules in jurisdictions that affect the company.
2. Establish written policies and procedures for the handling of ESI and use documented practices that prove you consistently follow those policies.
3. Make IT development decisions that are mindful of the ESI Rules and their requirements.
4. Document current and past IT environments.
5. Know your data. At a minimum know the content categories of your ESI at each location.

STEPS TO PREPARE COMPANY INFORMATION

1. Create a central, searchable cross-platform archive.
2. Make sure that the archive has scalable search capabilities.
3. Make “accessible information” as accessible as possible.
4. Have well-established processes for effectively implementing selective preservation of ESI.

- 
5. Have audit logs of all interaction with archive records from creation to destruction for chain-of-custody documentation.




→ 2. Overview of the ESI Rules

ESI Rules are being developed in many different jurisdictions and further interpreted in case rulings. Debate continues on many of the issues as to what is the best approach. While there continues to be disagreement on the specifics, there is general agreement on the issues to be addressed including:

- ▶ Identification of ESI as a class of evidence separate from documents and things (FRCP 34(a))
- ▶ Disclosure or description of evidence before discovery (FRCP 16 and 26f)
- ▶ Pre-trial conferences to include ESI issues (FRCP 16, 26(f), 26(a), 26(e), 26, 29-37, Delaware Default Standards, CCJ-WGED, etc.). Issues addressed include:
 - ▶ Identity of custodians
 - ▶ Location and description of information
 - ▶ Description of supporting IT environment at the relevant time
 - ▶ Discovery timing
 - ▶ Claims of privilege
 - ▶ Scope and specificity of discovery requests
 - ▶ Form of production
 - ▶ Discovery of accessible and inaccessible information
 - ▶ Cost shifting
 - ▶ Claw back of mistakenly disclosed privileged information
 - ▶ Inadvertent destruction of relevant information in the normal course of business
 - ▶ Preservation requirements of relevant data
 - ▶ Identification of “e-discovery liaison”
- ▶ Sanctions (FRCP 16, and 37)

There is still considerable discussion about what is Electronically Stored Information. While the FRCP is somewhat vague on the definition of ESI, other groups have provided more detailed insight into the scope of ESI. The Electronic Discovery Working Group of the Conference of Chief Justices uses the following definition:

1(A) Electronically Stored Information is any information created, stored, or best utilized with computer technology of any type. It includes but is not limited to data; word-processing documents; spreadsheets; presentation documents; graphics; animations; images; e-mail and instant messages (including attachments); audio, video, and audiovisual recordings; voicemail



stored on databases; networks; computers and computer systems; servers; archives; backup or disaster recovery systems; discs, CDs, diskettes, drives, tapes, cartridges and other storage media; printers; the Internet; personal digital assistants; handheld wireless devices; cellular telephones; pagers; fax machines; and voicemail systems.

(B) Accessible information is electronically-stored information that is easily retrievable in the ordinary course of business. (Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information, Review Draft: September 2005)

The key point is that ESI covers all forms of electronically stored information on a wide variety of media and equipment. It is not limited to e-mail and Instant Messages. This means that in order to be most effective, archiving solutions need to be able to interface directly to an array of applications to gather and manage different file types, whether those files are attached to e-mails or not. Systems that are focused primarily or solely on e-mails will make it more difficult for companies to manage all of their discoverable information.

For several years companies have struggled with the importance of aligning their ESI practices with physical records management policies and practices or with litigation requirements in mind. The barriers to action have been varying combinations of:

- ▶ the belief that the rules do not apply to the company,
- ▶ the indifference of senior management to the related risks or
- ▶ the failure to articulate the ROI of investment in ESI management solutions.

Indifference to ESI requirements can be an expensive mistake. In two comparable recent cases one company spent over \$7,500,000 on ESI related litigation preparations. That is a staggering amount of money for any company. But when you consider that the second company spent over \$42,000,000 for essentially the same activities the hard dollar value of ESI preparation and litigation is not only clear but also financially justifiable.

While the demands of the ESI rules may be new to you or confusing, there are several basic steps to take in advance of litigation that will better prepare your company for matters dealing with ESI in litigation and help to reduce litigation related costs.

The ROI of these steps is very real. The result of taking these steps has favorable short- and long-term impact on the company's bottom line.




→ 3. The Guidelines for Action

The guidelines for actions that companies should consider and act upon if applicable to their situation are derived from the requirements outlined in the rules of the courts and other interested parties. The actions relate directly to requirements established in court rules or in court opinion in cases.

STEPS TO PREPARE THE COMPANY AND ITS PEOPLE

The preparation of ESI for litigation is not just a matter of preparing the ESI and its storage, management and access. It is also a matter of preparing the company and its people. There is a core group of people in Legal, IT and HR that should be fully aware of the requirements and have a shared vision of how to handle ESI. The following steps will help anticipate ESI related demands of litigation.

1. **Keep key Legal, IT and HR personnel well informed of ESI Rules.** It is acknowledged, and in some courts recommended, that IT personnel be an integral part of pre-trial discussions, depositions and possibly even witness stand testimony. In other courts it is required for a party's IT personnel to be involved in pre-trial discovery discussions. In some jurisdictions, the rules require the appointment of an "e-discovery liaison." In order for IT personnel to be most effective, they must not only be informed about the company's systems, past and present, they must also be informed about ESI Rules, company policies and procedures and how they all work together. The knowledge of ESI requirements will also influence their thinking about how they design and implement systems in the future to better protect the company and its information. According to the Fulbright & Jaworski 2006 Survey on Litigation Trends, the leading types of litigation continue to be focused on employment and contract matters. This means that in addition to IT and Legal, HR should be well informed of ESI rules and have a shared view with Legal and IT about how to handle ESI.
2. **Establish written policies and procedures for the handling of ESI and use documented practices that prove you consistently follow your policies.** The more consistent and the longer standing these policies, procedures and practices are, the stronger your arguments will be about the integrity of your electronically stored information and its management. Be sure that you do not limit yourself to dealing only with e-mail and Instant Messaging (IM). While important, e-mail and IM are not the only sources of potentially relevant information. The term "Electronically Stored Information" was intentionally chosen because of its inclusive characteristics. Policies should be reviewed regularly to ensure that they remain consistent with both regulatory requirements and with court rules. The policies should be maintained by legal, HR and IT.

- 
3. **IT development decisions should be mindful of the ESI Rules and their requirements.** Too many companies continue to keep a great distance between IT and legal. The vast majority of company records today are stored electronically and managed by IT. According to leading IT analysts Gartner, 90% of all business records are created electronically and only two thirds of those records are ever printed. Decisions about how that data is stored, what technology will support the management and the necessary functionality must reflect the legal and regulatory obligations of the company. IT decisions can no longer be made independent of input from the legal department.
 4. **Document current and past IT environments.** For the courts, the only relevant IT systems are those systems that existed at the time of the matter in question. In order to be responsive to this issue, describe the systems past and present, when they were in use and how they processed data at that time. Know how and where data was stored and what is needed to retrieve it today, if it still exists. The documentation should be able to describe those systems that were active at any point in time over the past several years. Current systems quite possibly did not even exist at that time. Earlier systems that generated the data may have been de-commissioned. The characteristics and limitation of the legacy systems and how they handled their data may significantly affect the accessibility of data relevant to the case. Given the rate of change in IT architecture, this could be a challenging task. For companies that are regularly in litigation, the payoff of documenting IT environments could be substantial. Instead of reconstructing a description for each new case, one central description with a time line can be quickly referenced. The potential savings are substantial. IT will save significant time and reduce resource demand. It will be particularly helpful in participating in the mandatory “meet and confer” conferences in each case.
 5. **Know your data. At a minimum know the content categories of your ESI at each location.** You will be required to provide this information for the data that is relevant to each case. One of the great challenges of ESI is the sheer volume of data. It is not just a matter looking for a “needle in a haystack.” It is more a matter of looking for many needles in many haystacks located in many fields! While you do not necessarily have to convert and process this data, knowing what data you have and where it is located will save the wasted effort of processing unrelated volumes of data just to confirm that it does not contain relevant information. This can be a huge savings.



STEPS TO PREPARE COMPANY ESI


ESI rules are about the use of Electronically Stored Information as evidence in litigation. In order for the information to be most useful, it must be managed for integrity and accessibility to facilitate document preparation and timely response. The more scattered the ESI is, the more difficult it is to respond accurately, effectively and economically. The following guidelines deal specifically with steps to take in handling ESI - improving the company's ability to better prepare its ESI for litigation.

An important issue for ESI is the treatment of "accessible" and "inaccessible" information. In the definition given above, accessible information is, "Electronically-Stored Information that is easily retrievable in the ordinary course of business." All companies have both accessible and inaccessible information. Often companies mistakenly make accessible information difficult and expensive to access. Doing so is counter-productive and overly costly.

1. **Create a central, searchable, cross-platform archive.** For most companies today, electronically stored information is spread across multiple locations - e-mail systems, database applications, shared file and collaboration systems, document management, scanning and imaging systems, on backup tapes, etc. In e-mail systems, employees with e-mails in .pst or .nsf files on their laptops or desktops are legitimately considered custodians of the data in their possession. Database administrators are the custodians of the data in their database applications. The wide, unknown and undocumented distribution of records characterized by this fragmented approach to information management is clearly not in the interest of the company. Companies in litigation are required to provide the names of the custodians of relevant data. With widespread employee .pst or .nsf files this is virtually impossible. The adverse potential of widespread .pst and .nsf files was dramatically illustrated in *Zubulake v. UBS Warburg*, where some, but not all, employees involved in the case deleted e-mails and then in deposition made claims of not being aware of the details of the situation. These depositions were later contradicted by the discovery of some of the deleted e-mails in other employees' desktop files. The outcome cost UBS over \$29 million. Having a half controlled data management environment is the same as having no control at all.

Other applications control their own records. Some maintain an archive of sorts within the applications themselves. This approach to an archive creates information silos (which require separate processing to access information) and increases the cost of discovery.

The solution is to create a cross-platform archive for records of all types that are to be archived. The archive system should be able to interface directly with the applications and not be limited to handling different file types only when they are attached to e-mail.




The archive must be able to gather and manage as many file types as possible - both directly from their original points of storage or their applications of creation - or when attached to e-mails or IMs.

2. **Make sure that the archive has scalable search capabilities.** Many companies that have purchased archive solutions in recent years tested the scalability of ingestion but not the scalability of access. Now that their archives have grown, they are encountering search problems with some searches requiring days to complete. Ensure that the archive retrieval characteristics are scalable and will be able to handle searches quickly and easily on your archive years from now. Also, make sure that this can be accomplished without deploying massive amounts of servers and storage.
3. **Make “accessible information” as accessible as possible.** Some portion of every company’s data is accessible for use in the normal course of business. As mentioned above in the CCJ-WGED Guidelines, this is the data that is considered accessible in litigation. It is in the best interest of your company to be able to access it quickly, easily and economically. Not only for the day-to-day operation of the business, but also for response to litigation discovery requests. This will reduce the need for .pst and .nsf files. For those .pst or .nsf files that are still needed, store them on shared storage under the control of the personnel that manage the ESI archive.

The easier the access to the data, the more useful the information becomes to you and the more time you will have to strategize about each case. You will need relevant information or descriptions of your information in several different instances. First, you will need it in the FRCP Rule 16 type pretrial conference where you are to describe your evidence in advance of any request for discovery. Second, you will need it in “meet and confer” conferences described in FRCP Rule 26 and in state rules as you discuss issues about delivery, format, accessibility and cost or burden of access. Thirdly, you will need it to be able to respond to discovery requests in a timely manner. Making or leaving ESI that is likely to be demanded in litigation hard to access only drives up your litigation costs and drives down company profits.

4. **Have well-established processes for effectively implementing preservation of ESI.** There are two aspects to this preservation requirement. The first is the preservation of information in advance of any litigation that is seen as being potentially relevant. Case law has long established that companies should preserve data that “they know or should have known would be relevant in the future.” There is an element of judgment in this aspect of preservation, in part because future relevance may not be clear at the time the records were created.

The second is information that is relevant to a case that is expected or has begun. It is very clear in the ESI Rules, that litigants are expected to take effective measures to preserve information



relevant to a case. While there is provision in the ESI rules for the inadvertent destruction of data in the normal course of business, companies that fail to take some action to segregate or “tag” records related to a case may be subject to sanctions. Already, companies have been heavily penalized in cases for failing to properly implement appropriate “litigation hold” procedures. Be sure that the archiving solutions you implement can easily place litigation holds on data and are able to place multiple holds on the same data for several different cases.

5. **Have audit logs of all interaction with archived ESI from creation to destruction.** Expect that the evidence that you bring to court will be challenged. One form of challenge will be to question your policies and procedures and your ability to prove that your practices follow your corporate policies. Another form of challenge will be to question whether you can prove that the records you have produced have not been altered. Audit logs that document every access to information in your archive from its inception to its destruction will be a significant aspect of your response to both of those challenges. They will provide “process chain-of-custody” proof about your handling of your ESI.




→ 4. How Prepared Are You?

Sometimes it is hard to determine where the risks are or whether new IT plans support or undermine the developing expectations with regard to ESI. The following are a number of questions about your current or planned policies and procedures and the related Data Loss Risk Exposure™. Review them and discuss them with both IT and legal.

GENERAL QUESTIONS

1. Do you have a structured archive with records management policies for the control of data?
2. Can the archive interface directly with a wide variety of different applications to capture records?
3. Can users delete records from the archive?
4. Has your backup system ever failed to restore backups?
5. Do you test your restore processes regularly?
6. Do you use backup tapes for long-term records retention?
7. Do users frequently ask that backup tapes be restored to recover information they need?
8. Do people keep critical business records on their laptops?
9. Is the data on laptops encrypted?
10. Are copies of these records in the archive?
11. Is there a formal well-documented, widely publicized process for informing employees about litigation holds?
12. Are there repeated litigation hold reminders?
13. Do litigation holds include instructions to IT storage management personnel?
14. In the event of a litigation hold order, can records (including records in the archive) be easily tagged for retention or segregated so that they will not be deleted in the normal course of business?



15. Is there some form of audit trail or audit log of activities against records, databases or mailstore?

E-MAIL RELATED QUESTIONS

1. Can users delete records before they reach the archive?
2. Do you place limits on individual users mailbox size?
3. Do users delete e-mails to make more room for new e-mails in their mailbox?
4. Do users move e-mails to .pst or .nsf files on their laptops or desktops?
5. Are e-mails retained in accordance with company policies and with regulatory requirements?
6. After employees have been informed of litigation hold orders, can they delete e-mails, records or working papers?



→ 5. Conclusions

The creation of rules to more effectively deal with ESI in litigation will have far reaching technological implications. Companies that are aware of the requirements are already rethinking their approach to the management of their electronically stored information. In the past, the primary concern regarding ESI was to ensure that it was available and that the systems used to manage ESI were always available to support the operation of the business. Once the information was no longer necessary to support the current day-to-day activities of the company, it was of less concern. When regulations required that records be retained, it was customary to just keep backup tapes a little longer.

With new ESI requirements, old records, those no longer needed for current business activities, have increased in importance. Issues of custodianship, discovery, duty to preserve, timely availability, inaccessibility, knowledge of location, categorization of content are all significant factors in the management of ESI.

Companies need to change their thinking about the scope and functionality of their IT infrastructure:

- ▶ How should data be retained?
- ▶ How long is it wise to keep data “accessible” from both a business and litigation perspective? Where should we keep the data?
- ▶ How do you provide employees with the appropriate levels of access to do their jobs, while ensuring that data is properly protected from deletion, alteration or private storage?

One implication is the need to implement a true enterprise-wide archive. Many companies have resisted doing this in the past. Those that already have an effective cross-platform archive are discovering that the archive provides a means of reducing costs, not only for IT but also for legal and general business operations. A well-designed archive can offer have widespread advantages to companies. The other implication is that legal professionals will need to take a more active roll in the design of systems and IT architecture and IT will need to be integrally involved in the creation of policies and procedures as they relate to ESI.

When it comes to ESI, there is little room for a “business as usual” approach, particularly for IT.

Companies that accept the challenges of the proper management of ESI will substantially reduce their litigation support and other costs. Companies that refuse to address these issues will find their IT operations disrupted, their costs skyrocketing and their ability to adequately protect themselves compromised.



→ 6. About AXS-One

AXS-One is a leading provider of high performance Records Compliance Management software solutions. Available as in-house installed software or hosted, the award winning AXS-One Compliance Platform™ is a secure, policy driven, high volume, archival, management and retrieval solution for electronic records, including e-mail, instant messages, images, output from ERP systems such as SAP, print streams and desktop documents. The archive ensures that all corporate records are retained and managed to address requirements for regulatory requirements, corporate governance, litigation readiness, e-discovery and broad risk management issues.

The AXS-One Compliance Platform efficiently combines disparate unstructured, semi-structured and structured data into a unified data archive structure, simplifying the manner in which companies in regulated and non-regulated industries retain, manage, search and retrieve records for legal discovery and broad compliance purposes. Data is stored and presented, with supporting contextual information, within a robust application framework. This framework includes user-specific Search technology, Supervision, Records Management and Legal Discovery that includes comprehensive legal holds capabilities.

The AXS-One Compliance Platform enables organizations to respond quickly and confidently to litigation preparation and electronic discovery orders while mitigating costs and risks. IT, Corporate Counsel and other authorized users can run case-related searches against all electronic records in the archive through a single web-based interface as well as manage the entire discovery process using integrated Case Management capabilities. To ensure organizations fulfill their “duty to preserve,” the results of searches can be placed on legal case hold, ensuring their normal retention and destruction cycles are automatically suspended until released by an authorized user. AXS-One solutions are capable of managing multiple litigation holds on the same data without creating multiple copies. AXS-One provides an auditable chain of custody for every record to demonstrate the integrity of the archive and the validity of the information used in evidence or in response to discovery. Active Case Management enables organizations to create manageable case files, which can be populated with data from the archive and, optionally, automatically updated with new data as it is ingested into the archive. Active Case Management enables organizations to pro-actively manage e-discovery requirements and ongoing investigations efficiently and securely.

AXS-One Inc.
301 Route 17 North
Rutherford, NJ 07070
(201) 935-3400
www.axsone.com



→ 7. More Information

For the latest information about our product and services, please go to our website at: www.axsone.com
or contact us at info@axsone.com.

United States / Headquarters

AXS-One Inc.
Meadows Office Complex
301 Route 17 North
Rutherford, NJ 07070
Phone: +201-935-3400
Fax: +201-939-6955

Australia

AXS-One Pty Ltd. Level 2, 201 Miller Street
North Sydney, NSW, Australia, 2060
PO Box 126,
North Sydney, NSW, Australia, 2060
Phone: +61-2-9922-6000
Fax: +61-2-9954-3130

Australia AXS-One Pty Ltd.

499 St Kilda Road
Melbourne, VIC, Australia, 3004
Phone: +61-3-9864-4100
Fax: +61-3-9820-1860

South Africa

AXS-One SA (Proprietary) Limited
Building No. 27 The Woodlands Office
Western Services Road
Woodmead, 2148 South Africa
Phone: +27-11-656-2850
Fax: +27-11-802-5020

Singapore

AXS-One Pte Ltd.
1 Phillip Street #12-02
Singapore 048692
Tel: +65-653-67808
Fax: +65-653-67303

Hong Kong

AXS-One Pte Ltd.
Level 25, Bank of China Tower
1 Garden Road, Central
Hong Kong S.A.R., PRC
Phone: +852-2251-8970
Fax: +852-2251-8971

Taiwan

AXS-One Pte Ltd.
17F, No. 167, Tun Hwa North Road
Taipei, Taiwan, 105
Phone: +886-2-2547-7000
Fax: +886-2-2717-2199

United Kingdom

AXS-One Europe Ltd.
54 Clarendon Road
Watford, Herts, WD17 1DU
Phone: +44-8707-460-464
Fax: +44-8707-460-484

United Kingdom

AXS-One UK Sales and Marketing
73 Watling Street
London, EC4M 9BJ
Tel: +44-20-7152-1114
Fax: +44-20-7152-1101

AXS-One Inc.
301 Route 17 North
Rutherford, NJ 07070
(201) 935-3400
www.axsone.com