

Managing Electronic Records for Success in Litigation and Business

Breakfast Briefing – February 28, 2007

Presented by:

David Brenner

Tim Hogan

Blake Marks-Dias



Today's Briefing

- ◆ **Sources of E-Docs Risk**
 - David Brenner
- ◆ **Rule-Driven Changes in Litigation**
 - Blake Marks-Dias
- ◆ **Getting on Top of Your E-Docs**
 - Tim Hogan

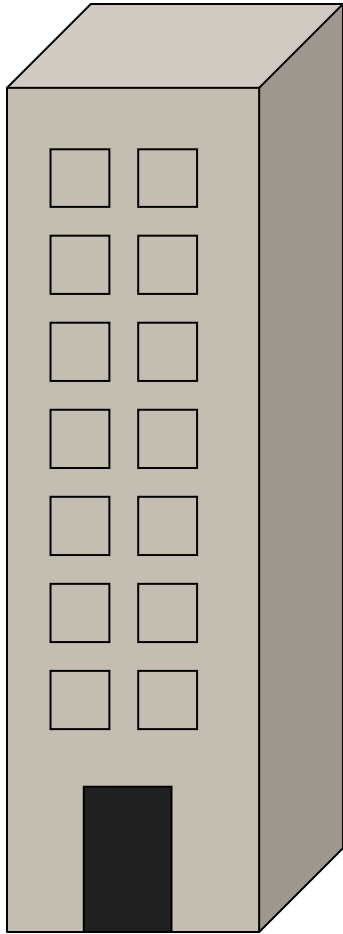


Sources of E-Docs Risk

David Brenner



Inc. Co. E-Docs Retention Goals



Inc. Co.

COMPLY with regulatory requirements

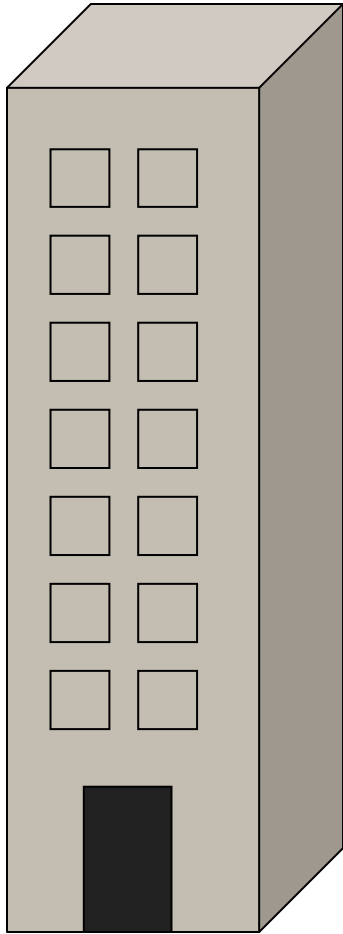
PROVE facts later

PRESERVE collective memory

ACCESS business critical information



Inc. Co. E-Docs Destruction Goals



Inc. Co.

ACCESS records easily and efficiently

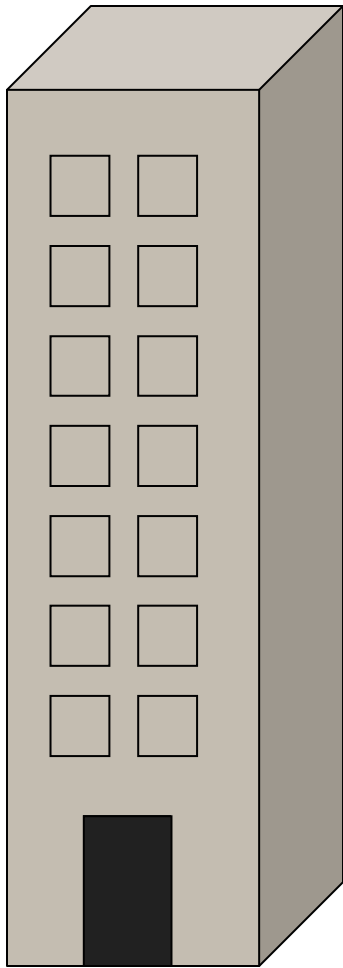
REDUCE operating and storage costs

INCREASE system efficiency

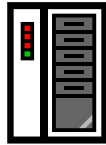
MINIMIZE misinterpretation, litigation costs



E-Docs Sources Risk



Inc. Co.



Systems Hardware & Software



Desktop Hardware & Software



Portable Hardware & Software



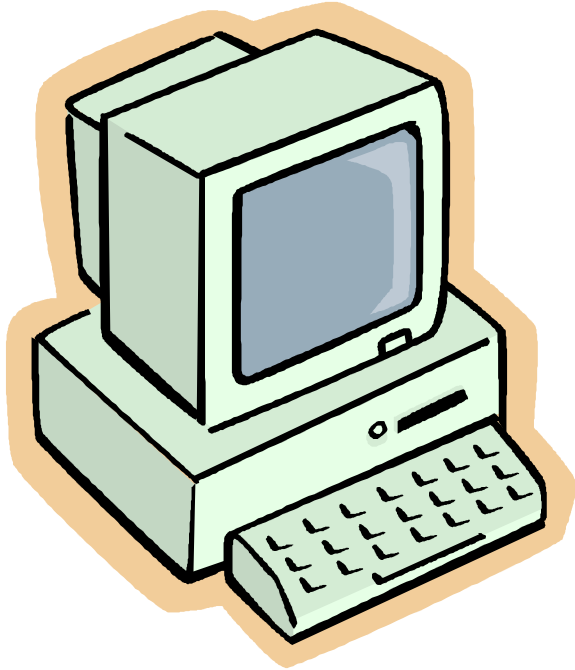
Removable Media



Backup Systems



E-Docs Sources Risk

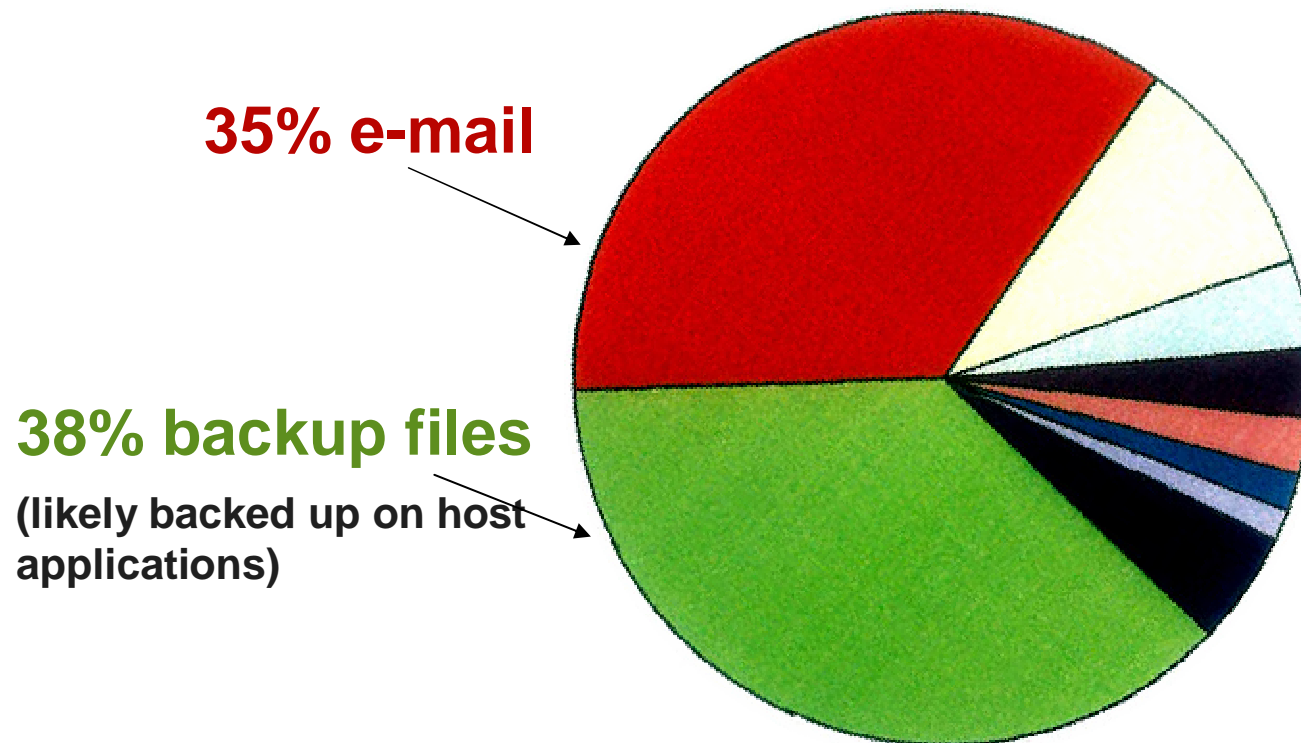


- ◆ Word processing programs
- ◆ E-mail
- ◆ Instant mail
- ◆ Calendar scheduling
- ◆ Database management
- ◆ Applications
- ◆ Internet browsers
- ◆ Financial / accounting



E-Docs Volume Risk

- ◆ Biopsy of selected employees' files
 - ◆ **2400** banker boxes of data stored by only **31** individuals – **over 6 Million pages!**
 - ◆ **22%** date back to year **2000 or earlier**

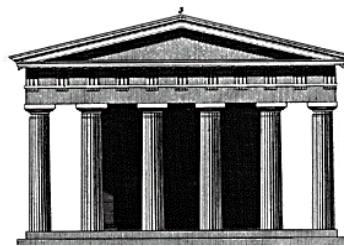




The E-Docs Risk Landscape



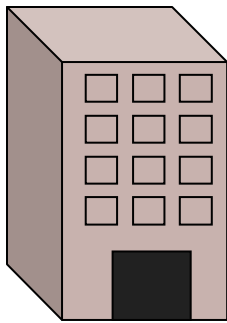
Government



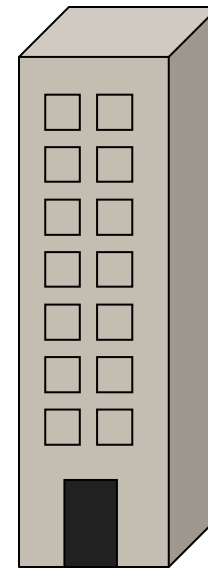
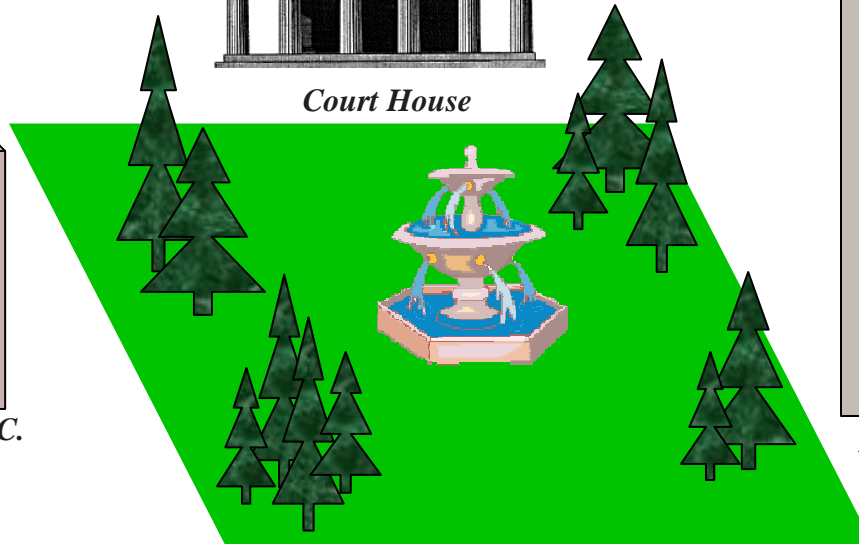
Court House



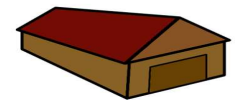
*Satellite operations,
partners
and joint ventures*



Lawyers, P.C.



Inc. Co.



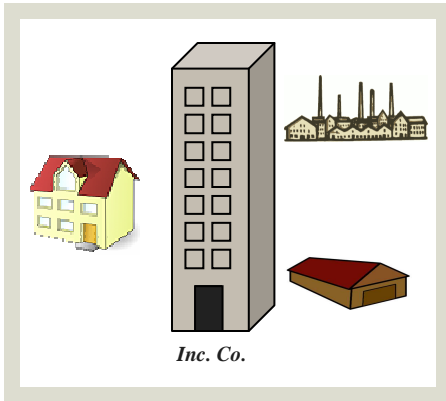
Third party storage

*Employee personal equipment,
home offices, PDA's*

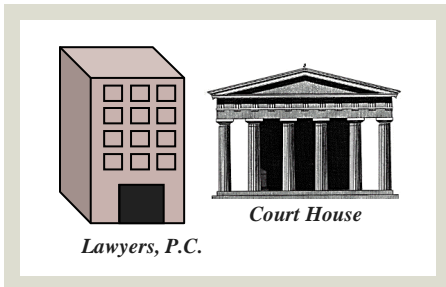




SUMMARY: Why Manage E-Doc Risk?



Accessing records to do business better



Cost-effectively maintaining and producing records to prove facts and win lawsuits



Complying with governmental regulations



Rule-Driven Changes in Litigation

Blake Marks-Dias



Why Is Electronic Evidence Important?

- ◆ The end of “electronic evidence lite”
 - ◆ “Mutual Assured Destruction”
 - ◆ Exceptions: employment and technology litigation
- ◆ Reasons for change
 - ◆ Electronic documents are the norm
 - ◆ Hefty sanctions (adverse inference) for failing to preserve/produce (Zubulake \$29 million; Morgan Stanley \$1.4 billion)
 - ◆ New litigation rules became effective December 1, 2006



Why Electronic Documents Are Different

- ◆ Volume, proliferation
- ◆ Dynamic, self-destructive
- ◆ Lack of standards
- ◆ Changing technology
- ◆ Harder to track
- ◆ Extraordinary cost



Electronic Evidence Discovery Issues

- ◆ Expense of accessing and manipulating records
- ◆ Inadvertent failure to produce
- ◆ Inadvertent production of privileged documents
- ◆ Inadvertent destruction
- ◆ Implementing effective “litigation holds”



The New Federal Rules: Five General Categories

1. Identifying electronic discovery issues early in the case
2. Electronically stored information that is not reasonably accessible
3. Protecting privilege and work-product
4. Discovery tools: interrogatories, requests for production, and subpoenas
5. Sanctions (and a safe harbor)



Identifying Electronic Discovery Issues Early in the Case

Rule 16: Court may include in initial scheduling order provisions for disclosure and discovery of electronic evidence, including agreements as to how privilege will be handled

Rule 26: Electronic evidence and related issues to be included in initial lay-down disclosures, initial party conference, and discovery plan

Rule 35: Electronic evidence issues to be discussed in initial report of parties' planning meeting



Electronically Stored Information That Is NOT Reasonably Accessible

- ◆ **Rule 26** on discovery limitations
 - ◆ A party need not provide discovery of electronically stored information from sources that the party identifies as ***not reasonably accessible because of undue burden or cost***
 - ◆ If other party moves to compel, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost
 - ◆ Court may nonetheless order discovery from such sources if the requesting party shows good cause, subject to specified conditions



Who Pays for the Production of Electronic Documents?

- ◆ **Traditional Analysis**: Presumption that responding party bears cost of complying with discovery requirements.
- ◆ **New Analysis**: Cost-shifting may be triggered when electronic discovery imposes an “undue burden or expense.” This turns primarily on whether the data is kept in an accessible or inaccessible format.



Who Pays for the Production of Electronic Documents? (cont.)

◆ Zubulake seven-factor cost allocation test:

1. Is request specifically tailored to discover relevant information ☐ *Most important*
2. Availability from other sources
3. Total cost of production, compared to amount at issue
4. Total cost of production, compared to parties' resources
5. Relative ability and incentive to control costs
6. Importance of the issues at stake in the litigation ☐ *Somewhat important*
7. Relative benefits to the parties of obtaining the information ☐ *Rarely important*



Cost Shifting Example

- ◆ Employment discrimination suit
- ◆ Potentially relevant evidence contained on backup tapes, including email
- ◆ Some of the data was moved from active data to backup tapes after the litigation was reasonably anticipated
- ◆ Who should pay for the expense of restoring and searching the backup tapes?



Cost Shifting Example (cont.)

- ◆ Applying Zubulake seven-factor cost shifting test, court ruled plaintiff must share 30% of the production costs. Quinby v. West LB, 2006 WL 2597900 (S.D.N.Y. Sept. 5, 2006).



Post-Production Privilege and Work Product Protection

- ◆ **Rule 26(b)(5)(B)**: Additional process for protecting inadvertently produced privileged material
 - ◆ Producer notifies recipient
 - ◆ Recipient returns or sequesters and may not use
 - ◆ Recipient may seek court review
 - ◆ Producer must preserve evidence until resolution



Discovery Tools: Interrogatories, Requests for Production, and Subpoenas

- ◆ **Rule 34**: States new requirements for how to produce electronic evidence:
 - (ii) default: must produce in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and
 - (iii) need not produce the same electronically stored information in more than one form.
- ◆ **Rule 45**: incorporates all of these changes into subpoenas to third parties



Sanctions (and a Safe Harbor)

- ◆ Duty to preserve all relevant evidence once litigation is reasonably anticipated.
- ◆ Therefore, a party must protect against routine alteration or destruction of relevant documents until the matter has been fully resolved.
- ◆ Guidance from Zubulake:
 - ◆ When litigation is “reasonably anticipated,” a party must suspend routine document retention and destruction policies and institute a “litigation hold.”
 - ◆ Hold applies to all “accessible” data and (perhaps) to “inaccessible” data of “key players.”¹

1. Zubulake v. UBS Warburg, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (“Zubulake IV”)



Counsel's Duty to Ensure Evidence Is Preserved

- ◆ **Attorneys may be sanctioned.** See Bradley v. Sunbeam Corp., 2003 U.S. Dist. LEXIS 14451, at *59 (N.D. W. Wa. Aug. 4, 2003) (fining attorney \$100,000)

“Sunbeam followed its document retention policy rather than honoring discovery requests and . . . Because of that, products were destroyed or not produced in blind adherence to its policy.”



Counsel's Duty to Ensure Evidence Is Preserved (cont.)

- ◆ Suggested steps from Zubulake V:
 - ◆ Issue and periodically re-issue litigation hold
 - ◆ Communicate directly with the “key players”
 - ◆ Instruct all employees to produce electronic copies of their relevant active files
 - ◆ Make sure that all backup media which the party is required to retain is identified and stored in a safe place. (Separate relevant backup tapes from others to prevent inadvertent recycling)



Spoliation Is a Sword That Cuts Both Ways

- ◆ Leon v. IDX Systems Corp., 2006 WL 26854512
(9th Cir. 2006)
- ◆ Plasse v. Tyco Elec. Corp., 2006 WL 2623441
(D. Mass. 2006)



Limits on Sanctions

Rule 37(f): Electronically stored information.

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 the routine, **good-faith** operation of an electronic information system.



Proposed Comment to Rule 37(f)

- ◆ Good faith may require that a party intervene to modify or suspend certain features of the routine operation of a computer system to prevent the loss of information, if that information is subject to a preservation obligation.
- ◆ Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.



Steps for an Effective Litigation Hold

- ◆ Send a written notice to all “key players” and persons holding documents relevant to the litigation
- ◆ Briefly describe litigation and importance in preserving all documents
- ◆ Instruct employees to refrain from deleting any relevant documents
- ◆ Suspend all “routine document destruction” such as automatic email deletions, etc.

- ◆ Written notice should include language along the lines of:

AS ONE OF THE POTENTIAL CUSTODIANS OF DOCUMENTS, YOU CANNOT FOLLOW YOUR NORMAL DOCUMENT RETENTION PRACTICES UNTIL FURTHER NOTICE. FOR EXAMPLE, YOU CANNOT AUTOMATICALLY DELETE E-MAIL OR RECYCLE DOCUMENTS RELATING TO [RELEVANT SUBJECTS] AS YOU MIGHT OTHERWISE DO IN THE ORDINARY COURSE OF YOUR EMPLOYMENT



Steps for an Effective Litigation Hold (cont.)

- ◆ Send periodic reminder notices
- ◆ Designate someone to be in charge of the litigation and hold and to act as a contact person to field any questions
- ◆ When in doubt, err on the side of preserving data
- ◆ Create a record of your efforts to preserve documents and to suspend routine deletion



Ways to Reduce Litigation-Driven Risks

1. Lighten the burden: eliminate legacy and unnecessary ESI (e.g., unnecessary backup tapes)
2. Create effective “litigation hold” process
3. If receiving discovery requests:
 - ◆ Predesignate/train IT system coordinator
 - ◆ Determine “accessible” vs. “inaccessible” data
 - ◆ Prepare IT personnel as 30(b)(6) witnesses
4. If requesting electronic evidence:
 - ◆ Learn about opposing party’s IT system to distinguish “accessible” from “inaccessible” requests and avoid cost allocation



Getting on Top of Your E-Docs

Tim Hogan



Addressing the Issues

- ◆ Without a **GAME PLAN** it's a broad and overwhelming topic
- ◆ Focusing on **RISKS** creates a manageable and practical path forward
- ◆ **END GAME** is adoption by the organization



How Things Go Wrong



- ◆ Senior Management not on board
- ◆ Policies / Procedures for electronic records not followed
- ◆ OVER-CREATION
- ◆ Poor Intra Company COMMUNICATION
- ◆ Faulty SYSTEM INTEGRATION
- ◆ INERTIA



Getting Started

- ◆ COMMUNICATION
 - ◆ The **Issue**
 - ◆ Organizational commitment
- ◆ KEY RISK areas identified



Simplify, Simplify, Simplify

- ◆ Data
- ◆ E-documents
- ◆ E-mail



Review and Assessment

- ◆ Protect Assessment from Discovery
- ◆ Analyze key risk areas –
 - ◆ Understand the systems and processes used in each key area
 - ◆ Specifics around the use, organization, storage and destruction of data, e-documents, and email
 - ◆ Use the assessment process to build support for the solution
 - ◆ Develop recommendations



Key Questions to Answer

- ◆ **Hard Copy Versus Electronic** - Are safeguards in place for electronic information comparable to the hard copy information? Do they work?
- ◆ **Version Control** – Does your software eliminate drafts and versions so that only the final version is accessible?
- ◆ **Retention Periods** – Is electronic information eliminated in a consistent fashion with hard copy information?



Key Questions to Answer (cont.)

- ◆ **E-Mail** – What rules do you have in place to protect against email proliferation?
 - ◆ Do your email software systems automatically delete messages if they are not stored after a fixed number of days?
 - ◆ What rules are in place covering the storage of emails?
 - ◆ Are there common protocols governing the organization of storage files for email?
 - ◆ How do retention/destruction rules get applied against individuals' stored email files?



Key Questions to Answer (cont.)

◆ **Effective Search Engines –**

- ◆ Can you effectively search across the company's various software systems to locate required information?
- ◆ Is there a common protocol for electronic information (e.g. author, topic, creation date, and retention period) allowing efficient and effective retrieval of information?

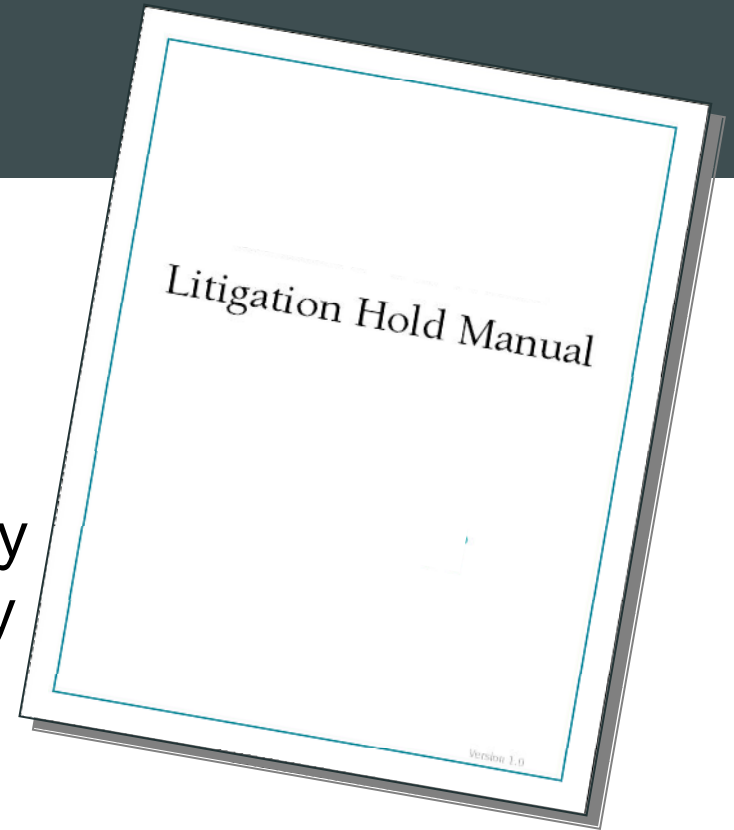
◆ **Persuasive Policy –**

- ◆ Are you able to persuasively document the measures taken to organize, locate, preserve and retrieve electronic information?



4 Steps to Reduce Risk

- ◆ Effective litigation hold process
- ◆ Design Simple Solutions
- ◆ Enterprise-wide integrated policy that can be used to **block** overly broad discovery in litigation and investigations
- ◆ Train and implement solutions





Legacy Issues

- ◆ Address legacy issues **after** the going forward solutions have been implemented
- ◆ Apply principles used for going forward solutions to address legacy issue
- ◆ Plan for monitoring and auditing to insure appropriate action is taken



Overview of Process

REVIEW & ASSESSMENT

- focus on key risk areas
- identify challenges
- develop recommendation

IDENTIFY & IMPLEMENT SOLUTIONS GOING FORWARD

Data

E-Docs

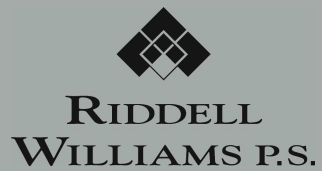
E-Mail

- communicate plan
- train
- monitor/audit

DEVELOP POLICY

- a *coordinated* approach integrated with hard copy retention
- a *flexible* approach recognizing needs of working groups

CLEAN UP LEGACY RECORDS



Questions?

Please contact us any time with additional questions.

David Brenner
206.389.1773
dbrenner@riddellwilliams.com

Tim Hogan
206.389.1782
thogan@riddellwilliams.com

Blake Marks-Dias
206.389.1575
bmarksdias@riddellwilliams.com