



Goals of an Electronic Document Retention Program

June 1, 2006

Presented by:
Blake Marks-Dias



Trends That Make Sound Document Retention a High Priority

- ◆ Electronic documents make this a unique problem
 - ◆ At least 93% of all information is first generated in electronic form. 30% of that is never printed to hard copy.
 - ◆ Experts predict that in 10 years, the number of electronic documents on the planet will double every 60 minutes.
- ◆ Hefty sanctions for failing to preserve/produce electronic evidence. Zubulake.



Risks of Not Having a Policy/Not Following your Policy

- ◆ Andersen example (selective enforcement)
- ◆ Inability to retrieve and productively use business critical information on a daily or historic basis



Risks (cont.)

- ◆ Increase costs of doing business from inefficiencies related to disparate or inaccessible data
- ◆ Failure to comply with statutory or regulatory retention and destruction requirements
- ◆ Reduced ability to comply with court orders and other litigation-related imperatives requiring access to existing information
- ◆ Inability to respond promptly to government inquiries



Benefits of an Effective Document Management Policy

- ◆ Facilitating easier and more timely access to necessary information
- ◆ Controlling the creation and growth of information
- ◆ Reducing operating and storage costs
- ◆ Improving efficiency and productivity
- ◆ Incorporating information and records management technologies as they evolve



Benefits (cont.)

- ◆ Meeting statutory and regulatory guidelines
- ◆ Meeting litigation presentation obligations, which may be broader and more extensive than the organization's other records management obligations
- ◆ Protecting the integrity and availability of business critical information
- ◆ Preserving corporate history and memory, including evidence to support corporate governance and compliance initiatives



Goals

- ◆ Compliance with statutes, regulations and industry norms
- ◆ Ability to retrieve data efficiently
- ◆ Manage storage costs and information growth
- ◆ Ability to suspend destruction (“litigation hold”)



Mandatory Suspension of Document Retention Policy

- ◆ During government audits or investigations and pending or threatened litigation
- ◆ Morgan Stanley example
- ◆ New FRCP - - Safe harbor



Sample Document Retention Audit Program

Phase I: Identify potential sources of risk

- ◆ Industry-specific regulations
- ◆ Employment-related records
- ◆ Unnecessary and/or outdated backup tapes and archives
- ◆ E-mail proliferation
- ◆ Failure to follow written document retention policy
- ◆ Deletion of documents during government audit or pending or threatened litigation
- ◆ Goal: Identify key specific areas to review, based upon sources of risk



Sample Document Retention Audit Program (cont.)

Phase II: Investigation of current electronic document retention

- ◆ Map out current IT architecture
- ◆ Determine how paper and electronic documents are handled in key areas
- ◆ Analyze current procedure for instituting a “litigation hold” during government audit or pending or threatened litigation
- ◆ Compare company’s current practices to best practices for document retention and report to company on results



Sample Document Retention Audit Program (cont.)

Phase III: Develop appropriate document retention practices to minimize risk

- ◆ Develop appropriate retention and deletion periods, including procedure for a “litigation hold”
- ◆ Craft measures for ensuring compliance
- ◆ Develop adequate archive resources
- ◆ Limit number of backup tapes and store them in an easily retrievable format
- ◆ Software solutions for more convenient storage and deletion of electronic documents
- ◆ Train key personnel to enable self-policing



The Need to Identify Key Sources of Risk—The Sedona Conference's Checklist for Evaluating an Organization's IT Function:

1. All hardware used for organization-wide systems (*i.e.*, mainframes, mini computers, e-mail servers, file servers, fax servers, voice-mail servers?)
2. All operating systems (*e.g.*, Windows NT/2000/XP, Linux, Novell, Unix, proprietary?)
3. All desktop hardware and software, including:
 - a. office document programs (*e.g.*, word processing, spreadsheet programs)
 - b. internet browsers
 - c. electronic mail
 - d. calendar/scheduling
 - e. database management programs
 - f. industry-specific applications
 - g. finance or accounting systems
 - h. remote connection applications



The Need to Identify Key Sources of Risk—The Sedona Conference’s Checklist for Evaluating an Organization’s IT Function: (cont.)

4. All data storage locations available to users (e.g., local hard drives, network drive locations, removable media, third-party storage locations)
5. All portable hardware and software (e.g., notebook computers, PDA, etc.)
6. All “backup” systems (hardware and software)
 - a. For what purpose(s) does the organization keep backup media (e.g., tapes)? (Disaster recovery? To restore individual accounts? As a means to ensure records retention? Other?)
 - b. How often are backups made? Are they complete backups or incremental?
 - c. What is the length of retention of backup media?



The Need to Identify Key Sources of Risk—The Sedona Conference’s Checklist for Evaluating an Organization’s IT Function: (cont.)

- d. Does disposal occur immediately when the retention expires?
 - e. If a backup tape is simply released for reuse, is there a concern over the passage of time before reuse occurs?
 - f. Is the backup tape degaussed or otherwise erased as a whole, or simply released for reuse?
- 7. All electronic data archives
- 8. All network components and locations (e.g., routers, hubs, firewalls, etc.)
- 9. All data storage locations outside of the United States
- 10. All third parties involved in data collection or storage on behalf of the organization
- 11. If the organization uses file servers, how does the organization assure compliance with retention schedules for:
 - a. The records on the server?
 - b. Backup copies of the server?



The Need to Identify Key Sources of Risk—The Sedona Conference's Checklist for Evaluating an Organization's IT Function: (cont.)

12. Does the IT Function take ownership of records compliance on file servers, or is this left to the users or others?
13. Does the IT Function know all the servers?
14. Does the IT Function know what type of records are on each server?
15. If an employee places a record on a server (e.g., a word processing document) and forgets about it, how is compliance with retention policies achieved?
16. Is compliance with retention policies a mandatory deliverable for hardware and software?
17. What tools and automation are employed by the organization to manage documents in general and records in particular (for example, Accutrac, iManage, Hummingbird, IBM)



The Need to Identify Key Sources of Risk—The Sedona Conference's Checklist for Evaluating an Organization's IT Function: (cont.)

18. Does the organization have a formal electronic records management system?
19. Has the organization implemented formal technology standards for records management? (ISO 15489, DoD 5015.2, ISO 17799)
20. Does the organization employ automated assigning of metadata for content management or control issues to documents?
21. Does the organization use technology to filter outbound content for loss of intellectual property (for example, Sybari for filtering outbound e-mail and attachments)?
22. Does the organization deploy leveraged Digital Rights Management technology to enforce external parties' copyright and license conditions?



The Need to Identify Key Sources of Risk—The Sedona Conference's Checklist for Evaluating an Organization's IT Function: (cont.)

23. If a technology is adopted, and concerns regarding records management implications are identified later, what is the process to address those concerns?



Hypothetical: Foodie Corporation

- ◆ Sells gourmet stocks and sauces
- ◆ History of employment lawsuits from angry chefs
- ◆ No written e-mail policy
- ◆ Stores backup tapes indefinitely
- ◆ Subject to certain industry regulations



Hypothetical: Foodie Corporation

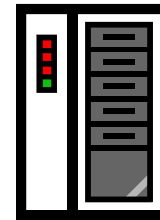
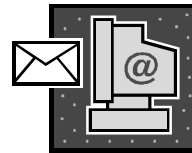
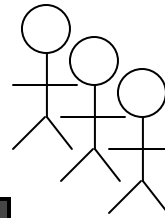
- ◆ Focus audit on:

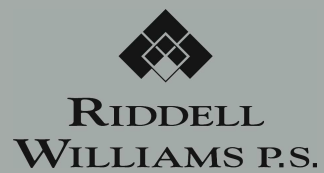
- ◆ Employment/HR documents

- ◆ E-mail policy

- ◆ Backup/archive policy

- ◆ Industry-related retention periods





Questions?

Please contact me any time with additional questions.

Blake Marks-Dias
Riddell Williams P.S.
1001 Fourth Avenue, Suite 4500
Seattle, WA 98154-1192
206.389.1575
bmarksdias@riddellwilliams.com