eData Outside Litigation: Prelitigation Risk Management

by

Stephanie A. Blair

Prelitigation planning has become irreplaceable in this age of eDiscovery. Although much of the focus, and the angst, related to eData has centered on eDiscovery and the eye-popping verdicts resulting from missteps and omissions, organizations can do much to reduce those risks with careful planning.

Organizations can substantially limit risks with a robust records-retention and eDiscovery-readiness plan.

Among other benefits, a records-retention and eDiscovery plan can:

1. Reduce storage costs
2. Reduce litigation risk
3. Reduce the cost of discovery
4. Enforce corporate compliance
5. Provide business continuity
6. Ease organization, storage, and retrieval of business records
7. Defensibly dispose of expired records

In addition, when failure to produce records in litigation is the result of a comprehensive, consistently enforced records-retention program, that program becomes a defense to claims of spoliation. *See Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005); *Park v. City of Chicago*, 297 F.3d 606 (7th Cir. 2002); *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988); *cf. Testa v. Wal-Mart Stores, Inc.*, 144 F.3d 173 (1st Cir. 1998).

However, despite these obvious benefits, a third of U.S. companies do not have records-retention policies that address the retention, storage, and disposal of electronically stored information (ESI).[1] As a result, most U.S. organizations are likely to be massively over-retaining records for no legitimate business or legal reason. By most accounts, more than 95% of the

[1] *See* 2007 *Cohasset ARMA AIIM Electronic Records Management Survey*, available from the authors at www.arma.org.

information retained by U.S. companies should be destroyed but is not.[2] Given the volume and risk involved, records-retention and eDiscovery readiness are worthy investments of time and resources that can yield a significant return.

2.1 Regulatory and Other Legal Requirements: Considering the Legal and Regulatory Landscape

A critical step in drafting a records-retention policy and schedule is identifying the applicable legal requirements concerning the retention and destruction of information. An organization must consider the externally mandated laws and regulations that govern it (e.g., from the IRS, SEC, DOD, DOL/EEOC, EPA), as well as its duties to preserve data relevant to actual or reasonably anticipated litigation. *See, e.g., Rambus, Inc. v. Infineon Techs. AG*, 220 F.R.D. 264, 286 (E.D. Va. 2004) (valid records-retention/destruction programs need to be put on hold where litigation is "reasonably foreseeable"); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (obligation to preserve arises when party knows or should have known that evidence is relevant to current or anticipated litigation).

FAQs:

What is a records-retention policy?

A records-retention policy is a document describing the principles and practices implemented to manage documents and data that constitute an organization's "business records."

What is a records-retention schedule?

A records-retention schedule is a taxonomy listing the "business records" of the organization and the length of time the organization will store each record type.

Can't organizations just use an "off the shelf" policy?

No. Organizations differ widely on the "business records" they maintain and on the legal, regulatory, industry, and business retention obligations with which they must comply. A policy and schedule should be custom designed for each specific organization.

For organizations with international operations or data, determining all applicable legal requirements can be very complicated.

For example, Article 8 of the Charter of Fundamental Rights of the European Union (2000/C364/01) recognizes that every person has a right to the protection of personal data and that such data must be processed fairly and for specified purposes, and on the basis of the consent of the person or some other legitimate lawful basis. This right includes the fundamental right to access personal data and to correct any mistakes within that data.

[2] Data is on file with the authors.

The legislation protecting individuals' rights in relation to personal data is mostly contained within Directive 95/46/EC on Data Protection, which seeks to harmonize the applicable national legislations of the member states. In the People's Republic of China, on the other hand, there is limited regulation on document retention in place, but it is generally understood that the civil law principle protecting the right to privacy also applies in relation to the protection of personal data.

Monitoring and Compliance Are Essential Components of a Retention Policy

Beyond the strict legal requirements, a reasonable policy can serve the legitimate information storage, access, and retention needs of an organization. A records-retention schedule should identify and prescribe time periods for the retention of information and records as appropriate for an organization's business needs and legal responsibilities. Such a schedule serves a legitimate business purpose, but is not designed to eliminate potential "smoking guns." *See Lewy*, 836 F.2d at 1112 (part three of a three-part test to evaluate the reasonableness of a defendant's document-retention policy addresses whether the policy was instituted in bad faith).

The mere existence of a written policy will not establish that document destruction was justified. Without a sound monitoring and compliance program, a records-management policy may be criticized as eliminating only "bad documents." *See Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 485 (S.D. Fla. 1984) (failure to implement the document-retention policy in a consistent manner was a significant factor in finding that the destruction of certain evidence relevant to legal proceedings could not be explained or excused as compliance with the policy).

An organization focused on eliminating "bad" documents not only risks accusations of bad faith (or worse), but also fails to recognize the value of contextual documents in mitigating the so-called "bad" documents and potentially exonerating the organization from allegations of misconduct or wrongdoing. *See Arthur Andersen LLP v. United States*, 374 F.3d 281, 297 (5th Cir. 2004) ("There is nothing improper about following a document retention policy when there is no threat of an official investigation, even though one purpose of such a policy may be to withhold documents from unknown, future litigation. A company's sudden instruction to institute or energize a lazy document retention policy when it sees the investigators around the corner, on the other hand, is more easily viewed as improper."), *rev'd on other grounds*, 544 U.S. 696 (2005).

The consequences for ill-conceived records-retention policies that merely serve as vehicles to "cleanse" files in advance of anticipated litigation or investigation can be severe. For example, in civil litigation, records-retention programs that focus on eliminating "bad documents" may be criticized as illegitimate "document destruction" policies that may result in severe sanctions, including default judgment:

1. ***Rambus*, 220 F.R.D. at 286** (finding that the policy was implemented with the intent to destroy documents relevant to anticipated litigation)

2. ***Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73, 76-77 (D. Mass. 1976)** (default judgment affirmed against defendant who had adopted a records-management system designed to obstruct discovery)

3. ***Reingold v. Wet 'N Wild Nev., Inc.*, 944 P.2d 800, 802 (Nev. 1997)** (finding that a one-season retention policy for first aid logs at a water park was unreasonable as it was "deliberately designed to prevent production of records in any subsequent litigation"; remanding for a new trial and holding that an adverse inference instruction was appropriate in the circumstances), *overruled on other grounds*, 134 P.3d 103 (Nev.

2006)

A focus on concealment and damage control, as opposed to targeted retention based on operational, legal, or institutional value, may even result in criminal penalties. For example, sections 802 and 1102 of the Sarbanes-Oxley Act of 2002 provide for fines and/or up to 20 years' imprisonment for destroying or concealing documents or other evidence with the intent to impair their availability for use in a proceeding or with the intent to impede, obstruct, or influence federal investigations or bankruptcy proceedings.

2.2 Records-Retention Programs and Policies: What Records Belong in a Records-Retention Schedule?

The objective of any records-management program should be twofold:

- To reduce the overall cost of records retention and storage by destroying those records that have outlived their legal, regulatory, and business use; and

- To retain those records necessary to meet any legal and regulatory requirements of the business, and the continued operation of the business.

Implied within these objectives is the fundamental principle of eDiscovery—that a company should "know where its stuff is." If an organization has a good handle on the location, source, and content of its records collection, it should be well equipped to respond to requests for ESI in an efficient and defensible manner.

Development of a records-retention plan is the first and, to some degree, most important step an organization can take in developing an effective eDiscovery-response mechanism. A robust records-retention policy and schedule that are carefully crafted, effectively implemented, and faithfully followed will reduce the volume of records maintained by the organization.

Once an organization has mapped its records taxonomy and researched its retention obligations, it can then assess its current recordkeeping practices and begin to identify the technical and human resources needed to enhance its ability to store, access, and dispose of its records effectively and defensibly.

It is widely agreed that retention policies and schedules should be simple but comprehensive. They should address all types of documents, both physical and electronic (including email, data files, voicemail, etc.).

A sound policy will clearly and unambiguously articulate:

- The reasons for the policy

- The requirements of the policy (e.g., clearly defined categories of documents to be retained, retention requirements consisting of a retention schedule, and procedures for retention and destruction)

- The parties responsible for establishing program controls and providing active, ongoing management

- Safeguards to suspend records retention in the case of foreseeable, pending, or active litigation or government investigation

- The company's commitment to compliance with the policy

In this electronic age, special consideration must be given to electronic data files, email, and voicemail. Retention policies must be carefully coordinated with a company's IT personnel to reflect the company's particular IT infrastructure and capabilities.

Identifying the Universe of Documents: The Record Taxonomy

In order to identify the universe of documents to be included in a schedule, a company should understand the fundamental intent of the types of documentation it generates and receives so that it can establish a relevant retention schedule for both those records that must be retained and those that are destroyed.[3]

Typically, corporations opt to establish varying retention periods that will satisfy legal requirements concerning each category of documents, while at the same time trying to maintain a simplified process so that the program can be implemented without confusion. Establishing logically related but workable records groups according to the records' characteristics, such as functionality or the regulatory authority governing their retention, appears to be the best practice.

The best means to establish these records groups is to understand why and when company employees create documents and what type of documents they create, i.e., a record taxonomy. This taxonomy not only aids in establishing a proper retention schedule for all documents, but also identifies inconsistencies in practice in developing documents (both hard copy and electronic versions)—information that can also be used in addressing records-management system issues and in training employees to minimize practices that can result in significant variations in documents.

By understanding what documents are created within the various areas of the corporation, a company can then make a decision as to the type of retention schedule it wishes to implement, whether general or specific:

- **General schedule:** All documents within each records group are subject to the same retention schedule and guidelines (e.g., all company documents relating to tax issues will be disposed of within seven years of their creation), with different retention periods applying to different records groups, as appropriate. The retention period for each records group should reflect the longest minimum statute of limitations period applicable to a document within that group.

- **Specific schedule:** Document retention periods are tailored to meet the legal and operational retention requirements of different types of documents within each records group. This system is useful for companies whose various divisions create multiple documents under any one records group where the legally required retention periods vary.

[3] Of course, best practice also necessitates that a company review its litigation activity in recent years, and any action involving regulatory agencies that oversee its business, to ensure that it understands the compliance obligations associated with those matters.

Practice Note

- Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.
- Systematic deletion of electronic information is not synonymous with evidence spoliation.
- Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as email, instant messaging, text messaging, and voicemail.
- Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contains data retained for business-continuation or disaster-recovery purposes.
- Absent a legal requirement to the contrary, organizations may systematically destroy residual, shadowed, or deleted data.
- Absent a legal requirement to the contrary, organizations are not required to do so.

With an eye toward simplification, many companies opt for the general retention schedule. However, after analyzing its records inventory, each company must determine for itself which system will work more effectively while still complying with the relevant laws.

Overarching Principles

An effective records-retention plan will meet the following criteria:

- Designed to meet business needs and legal obligations
- Comprehensive, yet simple
- Addresses both electronic and paper data
- Clearly states rationale for policy
- Includes retention/destruction schedules
- Includes an exception for litigation holds
- Widely communicated
- Easily accessible
- Simple to follow

Also note that:

- The ideal schedule provides for the shortest retention periods legally and operationally possible.
- A cutting-edge policy is automated to take the guesswork and compliance out of

employees' hands.

Implementation:

- Designate a gatekeeper or records-management team
- Inventory business records by interviewing representatives of each business function and/or unit
- Identify records groups: Tax, HR, Finance, Accounting, Sales and Marketing, Corporate, and so forth

Compliance:

- An ignored policy is worse than no policy at all
- Develop a mechanism for auditing and compliance

Employee training is key, and should include:

- Litigation primer
- Best practices
- Records-retention program implementation

Employees should know:

- Importance of program
- Distinction between "business records" and "records of transitory value"
- How to store and discard business records in accordance with program

Consequences of failure to properly retain records:

- Sarbanes-Oxley Act of 2002
- Title 18 – Obstruction of Justice
- Civil penalties, including adverse inference

2.3 eData Policies

In addition to the records-retention policy and schedule, every organization should create eData policies related to the use of company information technology. Some fairly typical IT policies include email policies, Internet policies, and acceptable-use policies.

2.3.1 Email Policies

Few records-retention policies drafted prior to the year 2000 address the subject of email. Yet email presents the greatest management challenge, primarily due to the sheer volume of emails generated each day in U.S. businesses.

Many options exist for email policies, including:

- **Cap and Purge:** Puts a cap on the size of each user's mailbox and purges emails that have reached a certain age (typically 60 to 90 days).

- **Cap and Archive:** Puts a cap on the size of each user's mailbox and allows users to create local archives of emails they wish to save.

- **All-In Archive:** All incoming and outgoing email is stored indefinitely in an archive.
- **Selective Rule Archive:** Captures all email and uses sophisticated searches to automatically identify and classify business records, subject to retention obligations.
- **Selected Declared Archive:** Requires users to classify each email and store it in a designated archive location.
- **Role-Based Archive:** Captures email and applies retention periods based on the job classification of the sender or recipient.
- **Unlimited Email Server Storage:** Saves all email on the server indefinitely.

Each of these options has significant pros and cons related to cost, likelihood of compliance, and ease of access. No option is a perfect solution; the efficacy of each differs among organizations and their particular needs. A careful assessment of an organization's corporate structure, IT infrastructure, and litigation portfolio is necessary to select the best approach.

2.3.2 Acceptable-Use Policies

Acceptable-use policies are codes of conduct that describe both acceptable use of company computers and prohibited activities. Most relate to acceptable use of email and the Internet. Such policies have become increasingly necessary in recent years, due to the following trends in Internet use:

- 70% of Internet porn traffic occurs between the hours of 9 a.m. and 5 p.m.
- 30% to 40% of Internet activity in the workplace is not business related.
- 27% of Fortune 500 companies have drawn harassment claims stemming from employees' misuse of email and the Internet.
- Workers can waste up to a third of the workday on "cyberslacking"—surfing the Web for personal reasons or no reason at all.

A typical acceptable-use policy will include the following key features:

1. It will clearly state that all computers and related hardware (e.g., company-provided PDAs, cell phones, and portable media), along with the content on those devices, are the property of the company.
2. It will clearly state that such devices are provided to employees for business purposes only and should not be used for personal reasons.
3. It will clearly state that the company is entitled to and does monitor Internet and email usage. (Here the company must "put its money where its mouth is," and engage in some sort of compliance monitoring in order for this policy to afford the company protection from liability.)
4. It will clearly describe prohibited activities, including, but not limited to, solicitation; harassment; disclosure of confidential company information; illegal activities; the making of defamatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, obscene, or

otherwise disruptive statements; political activity; and any activity likely to disrupt company operations, including downloading prohibited content or virus-infected materials.

5. It will prohibit downloading software applications, including instant messengers, music-sharing tools, and other peer-to-peer applications.

6. It will clearly describe the repercussions for failure to comply.

As with records-retention policies, an acceptable-use policy is only as good as an organization's wherewithal to train its workforce and monitor compliance. Implementation that emphasizes training during the rollout of the policy is critical.

2.3.3 Other Technology Policies

Many companies and individuals are tech savvy or so-called "über users." When this is the case, acceptable-use policies should be expanded to include instant messaging (IM), VoIP (Internet-based telephony), blogging, text messaging, and so forth, to circumscribe use as appropriate to the needs of the organization. As illustrated by a recent case involving a supervisor's review of an employee's text messages, *any* acceptable-use policy must be consistently implemented in order to overcome an employee's expectation of privacy. *Quon v. Arch Wireless Operating Co.*, No. 07-55282, 2008 WL 2440559 (9th Cir. June 18, 2008) (employer's search of employee's text messages violated his Fourth Amendment right to privacy where employer had no specific policy regarding text messages on work-issued pagers, and employer's general computer- and email-monitoring policy was not consistently enforced with respect to the text messages).

A Note on Instant and Text Messaging

Researchers have found that IM is in use in more than 90% of U.S. companies.[4] Of those companies about 75% report that their IM activity is not controlled by the organization, but is downloaded by individual employees from Internet service providers such as AOL and Yahoo!. Similarly, text messages, even if generated on a company-issued phone, pager, or BlackBerry, are not retained by the company, if they are retained at all. Yet it is clear from a developing body of case law and commentary that IM and text messages, like email, constitute discoverable ESI. Companies must therefore assess the use and retention obligations of IM and text messages, and implement policies to establish greater control over these growing communication tools.

The key decision here for business: to IM/text or not to IM/text? If a company concludes that IM and text messaging enhance the productivity of its business, then it must enact policies and technology to manage and control their use. If these technologies do not enhance the business, then companies must enact policies and technologies to limit or prohibit their use for business purposes. Both options are common in today's business environment.

2.4 Technology Solutions

A host of technology solutions are available to ease implementation and compliance with an organization's records-retention program. Given the volume of data generated and received by

[4] *See Records Retention Rules and Best Practices Under Sarbanes-Oxley*, available at www.lighthousecs.com (last visited July 7, 2008).

organizations in the ordinary course of business,[5] technology tools to manage the flow, organization, and retention of eData are mission critical. Among the tools organizations should consider are:

1. **Email Management Solutions:** These tools capture, regulate, and archive email traffic according to rules defined by the organization to meet its operational and compliance needs. Many such tools come with robust search and retrieval capabilities, single-instance archiving, and litigation hold and eDiscovery functionality.

2. **eData Management Solutions:** These tools apply retention principles to user-generated files and a single archive for records storage and retrieval. Such tools offer an effective alternative to uncontrolled user data management, such as local archiving and subject-matter drives.

3. **Litigation-Hold Management:** These tools manage the litigation-hold process, including distribution of litigation-hold notices and compliance tracking.

4. **eDiscovery Management:** An array of tools are entering the market that are designed to assist organizations in searching, harvesting, culling, processing, and hosting data subject to eDiscovery.

The selection of technology solutions should first and foremost be a partnership between the organization's IT and legal teams. This multidimensional team should consider many factors, including the size of the organization's litigation portfolio, data volume, IT infrastructure, and other resources. Ultimately, to support the policies and protocols the organization establishes for records-retention policies, the technology must fit within the company's IT structure and enhance the end-user experience and thus compliance with retention obligations and business needs.

2.5 Litigation Readiness

As important as an effective records-management program is a thoughtful, repeatable eDiscovery response plan, i.e., a litigation-readiness plan. Such a plan identifies the processes and resources the organization will deploy to meet its discovery obligations when faced with threatened or actual litigation, government inquiry, or a subpoena. A litigation-readiness plan may have many components, including IT maps, data inventories, response protocols, forms, and templates. All are designed to meet enhanced discovery obligations imposed by the amended Federal Rules of Civil Procedure, state rules, and a growing body of case law.

A critical function of any effective records-management program is the orderly suspension of ordinary-course records disposal when certain records must be preserved due to anticipated or pending litigation or government inquiry. Developing a litigation-readiness plan expands upon the exception described in a records-retention policy and positions a company to meet the enhanced obligations imposed by the recently enacted amendments to the Federal Rules of Civil Procedure.

A litigation-readiness plan enables a company to:

[5] Email traffic is estimated to exceed 60 billion messages per day around the globe, not including spam. *See* www.prnewswire.com ("Email Usage to Exceed 60 Billion by 2006, According to IDC," Oct. 14, 2007).

- Effectively and efficiently respond to requests for ESI
- Avoid duplication of effort in multiple cases
- Promote the defensibility of the process
- Minimize business disruptions and related expenses
- Reduce the risk of inconsistent responses from case to case

The litigation-readiness plan identifies milestones, roles, and responsibilities in the litigation-response process. The plan further establishes standard protocols for data gathering, collection, preservation, and processing, in addition to data-production requirements. Deployment scenarios identifying resources that the company will deploy in defined classes of cases are an integral part of the plan. The plan also helps the company issue litigation-hold protocols, Rule 26(a) Initial Disclosures, and Form 35 Discovery Plans that are consistent across federal and state litigation, as well as in response to requests from federal and state regulatory agencies.

The Morgan Lewis eData team creates for its clients customized eDiscovery-readiness deliverables that include:

- An IT map
- A data inventory
- A litigation-readiness plan and checklist
- Modern records-retention policies, schedules, and practices
- Technology solutions recommended for optimized retention and litigation response
- A discovery checklist and litigation-hold template
- Employee training materials
- Regulatory and recordkeeping compliance
- Relevant forms and templates, from discovery plans to form disclosures

2.6 Training and Implementation

An essential component of any records-management program is the implementation phase. After the program is created, the focus should turn to implementation of the program, which should involve (a) preparation of training materials for implementation, enforcement, and compliance auditing of the program; (b) training of an internal records-management committee and/or manager; (c) internal publication of the program and training of company personnel; and (d) supervision and documentation of the first round of program enforcement.

In addition, organizations should investigate, analyze, pilot, and select technological solutions to automate and facilitate the records-management process.

Morgan Lewis is at the forefront of innovative workplace training programs and takes great pride in effectively educating personnel at all levels and in all departments.

We provide in-house legal departments with CLE-approved training that covers the latest developments in records retention, eDiscovery, and litigation holds.

For example, our courses for nonlegal personnel review best practices in drafting business communications that are effective yet do not unnecessarily expose companies to liability.

***Chasing Paper: Implementing Effective Records-Retention Policies*:** This program will train internal records-management and other relevant personnel on effectively implementing the company's updated records-retention policy and program, as well as current records-retention best practices. Trainers will use examples directly from the organization's own newly created retention schedule; hypothetical questions and scenarios designed to direct focus to and create awareness of common auditing, compliance, and destruction issues that may arise; documentation customized for the company; and forms created specifically to assist with the implementation and auditing of the retention schedule. As a result, at the end of this training, attendees have the know-how and tools needed for full-scale implementation and auditing of the schedule going forward.

***Think Before You Send: Savvy Business Communications*:** Designed for nonlawyers, this course is intended to prevent the creation of a damaging "smoking gun" document that can come back to haunt you in the course of discovery. It introduces the "Top 10 Best Practices for Savvy Business Communications," an easy-to-follow yet comprehensive set of practical suggestions, and illustrates their importance with a series of compelling real-world examples—many drawn from today's legal headlines. In the course of dissecting these case studies, participants will gain a detailed understanding of the risks of ill-considered communications, along with common-sense strategies for drafting communications that reduce risk without sacrificing effectiveness.

***Stop the Shredders: When and How to Draft a Litigation Hold*:** This CLE-approved course educates your legal department on the current state of the law regarding eDiscovery and records preservation, including the possibility of sanctions. It covers the events that can trigger a duty to preserve documents and reviews best practices for drafting and implementing a litigation hold, along with the strategic and legal issues involved.

Practice Note

- Companies should consider developing "trigger guidelines" that provide management with guidance and examples of situations that may trigger a duty to preserve. These guidelines can be included in an eDiscovery Readiness Plan (discussed in Section 2.5, "Litigation Readiness," above).
- Among other things, companies should examine the organization's litigation history, HR and ethics policies, and reporting obligations to identify those policies and procedures that could dovetail with "reasonable anticipation" of litigation. One example is the work-product doctrine.

Guarding Corporate Gold: Maximizing Privilege Protections for Corporate Communications: Corporations all too often receive a nasty shock when they learn that highly sensitive information—information they believed to be protected by privilege—must be produced in discovery because they had inadvertently waived privilege protections. This CLE-approved course will take your in-house counsel through a careful analysis of privilege—including attorney-client privilege, attorney work-product doctrine, and joint-defense privilege—and the ways in which corporations unwittingly lose privilege protections in the course of routine business transactions. It also offers practical suggestions for proactively managing communications in order to support a future claim of privilege during litigation or governmental investigation.

We are on the leading edge in terms of the substance of our training programs, and also in our delivery methods. We enjoy training people in a face-to-face environment. In circumstances in which face-to-face contact is not possible, we have experience in using webcast training sessions to achieve a company's goals. In these sessions, we create virtual "classrooms" that encourage participants to "raise their hands" to ask questions, permit trainees to test their new skills with polling questions, and use a "highlighter" to emphasize key concepts.

FAQ:

What is a legal hold?

A legal hold is the affirmative obligation to preserve records that might be relevant to actual or potential litigation, investigations, or other legal proceedings.

What triggers a legal hold?

A legal hold is triggered when it is known or reasonably should be known that certain records may constitute relevant evidence in actual or potential litigation, investigations, or other legal proceedings. *See, e.g.*, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (*Zubulake III*); *see also Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001) (citing *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998)).

When does an organization "reasonably anticipate" litigation?

Reasonable anticipation of litigation has been described as the moment when:

- It is more likely than not that litigation will ensue
- A credible threat of litigation exists

A party should examine the facts and circumstances, as well as its experience, in making this determination.

2.7 Auditing

Auditing and compliance are essential components of a retention program. A records-retention program must not only account for the externally mandated laws and regulations that govern the organization (e.g., IRS, SEC, DOD, DOL/EEOC, EPA, state Public Service Commissions) in order to ensure that documents are retained for the legally required amount of time. A records-retention program must also be "reasonable" in that it actively serves the legitimate information storage, access, and retention needs of the organization. Such a schedule serves a legitimate business purpose and is not designed to eliminate potential "smoking guns." Auditing and compliance are essential components that courts look to in order to determine whether a records-retention program is reasonably designed to meet the legitimate legal and business needs of the organization, or is merely a haphazard program that eliminates documents and data relevant to pending or anticipated litigation. Many options exist for conducting an effective audit. Two are described below.

Audit Options: Full Audit

Depending on the current state of a client's records-retention program, records inventory, and compliance history, a full audit of all records of a significant sampling of company personnel may be warranted. A full audit would entail interviews and inspections of employees across all locations, business units and functional areas. A full audit is a sensible approach when an organization has not previously implemented or enforced a records-retention policy, does not have internal resources to implement a new retention schedule for historical records, has "inherited" records from predecessor organizations, and/or has a volume of historical records that present additional challenges.

Audit Options: Selective Audit

The second option is to complete a selective audit, first using online questionnaires and certifications, then sampling for interviews and inspections of 1% to 5% of employees across the organization's locations, business units, and functional areas. A selective audit is a sensible approach for an organization that has historically engaged in some manner of records management and/or retains a manageable volume of records.

2.8 Records-Retention Schedule Refresh

Organizations are also encouraged to conduct a yearly "refresh" of the records-retention schedule to ensure that scheduled retention obligations are current with legal and regulatory requirements.

Stephanie A. "Tess" Blair is a partner in Morgan Lewis's Litigation Practice and leader of the firm's eData Practice.