The impact of electronically stored information on corporate legal and compliance management:

An IBM point of view

By Barbara Churchill, Linda Clark, Jonathan Rosenoer and Fritz von Bulow, IBM Corporation

October 2006

Contents

Introduction

This paper presents an IBM point of view on the impact of electronically stored information (ESI)[1] on regulatory compliance and the process involved in legal "discovery," and the importance of managing ESI within the context of a corporate records management program. The magnitude and range of compliance risks associated with the management of ESI is driving IBM's investment in the development of more effective approaches and products designed to provide an integrated and leverageable platform to support regulatory compliance, legal discovery and life-cycle records management needs, as well as to provide cost savings and value creation. As regulators and courts increasingly recognize the enhanced and richer information value of electronic data compared with physical documents, companies should strengthen their ability to safeguard their rights and respond appropriately. Companies also need to recognize and avoid the implications posed by redundant and often duplicative siloed systems designed to address particular requirements (for example, Sarbanes-Oxly [SOX] Act compliance, electronic discovery, document retention management and so forth).[2]

This paper highlights some factors that can influence a company's ability to maintain and manage ESI in a manner that effectively supports corporate compliance and records management objectives as well as the electronic discovery process. It also describes key system and process attributes that are helpful to support these efforts. Topics that are of particular interest for electronic discovery and records management, such as treatment of e-mail and metadata, are explored to aid strategic and tactical planning activities for responsible executives.

E-mail as a source of discoverable documents: the need for an electronic discovery process and records management enabled by technology

Managing the discovery and production of ESI can best be approached as an integrated end-to-end process. Although e-mail is one of the top requests in regulatory investigation and civil discovery, the IBM team believes that a significant number of companies have yet to manage their e-mail systems as a key source of discoverable information and establish a searchable e-mail archive.[3] The IBM team thinks it likely that even fewer companies recognize that all ESI is potentially subject to the same scrutiny and investigation as e-mail and have taken steps to implement systems, policies, and protocols to manage retention of ESI across the enterprise.

Highlights

The tremendous volume of ESI, e-mail being a primary example, creates challenges for legal discovery. Managing and controlling the growth of ESI through retention policies and enabling technology can help to address this challenge.

A major challenge in the discovery process is the tremendous volume of ESI, even if the discovery request is limited to e-mail. This is because of increasing corporate reliance on electronic communications and the ease of exchanging information electronically. At the same time, we believe many companies have not implemented e-mail management policies which would enable them to safely reduce their storage of older documents.

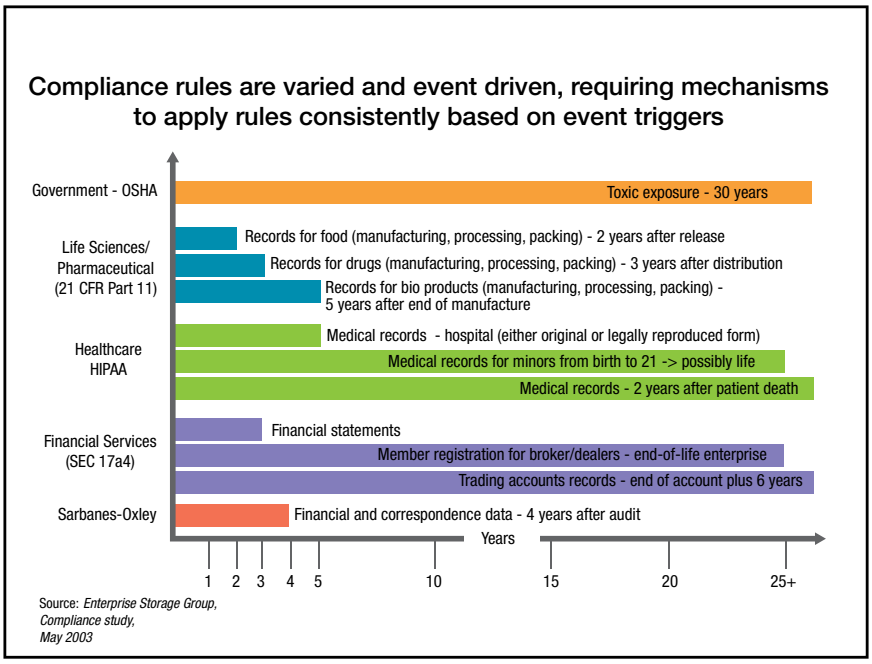

Figure 1. ESI retention requirements, in some cases, do not begin until a particular event has occurred.

Also contributing to the growing volumes of e-mail and other forms of ESI is the potential difficulty of implementing consistent destruction policies. Retention requirements are often event driven, based on the occurrence of a future payoff event (such as settlement of a claim or payoff of a mortgage). This has posed a significant challenge for records and content management technologies that can handle only simple retention rules (for example, destroy five years from the creation date). It is our experience that a great many retention requirements in formal records management programs are event dependent, as illustrated by a study conducted by IBM in May 2003 *(see Figure 1)*. Newer technologies (such as Integrated Content Management) have the capabilities to address these issues to help companies manage the lifecycle of ESI and implement complex retention rules. Improved capabilities to facilitate the compliant destruction of ESI may significantly reduce the amount of ESI being maintained across an enterprise.

Highlights

To be prepared for electronic discovery, have a plan and a process that you can improve upon over time.

Reducing the volume of ESI requires records management and retention policies supported by a technology solution that is flexible, scalable and capable of consistent operation in the normal course of business. E-mail is a good example of why organizations should revisit their records management and retention policies and consider the risks and other issues posed by ESI. Of particular concern should be how new technologies impact these policies. Organizations that fail to understand and consider new tools and methodologies may not only increase risk, but also miss a substantial opportunity to remove cost.

Be prepared for electronic discovery

How can one prepare for a future electronic discovery? Experience shows that there is no silver bullet, but potential solutions are beginning to emerge. Examining your practices and capabilities in light of the following approaches can be helpful:

- *Have a plan and a process for discovery of ESI that you can improve over time. Understand your end-to-end process from discovery to production and the implementation of "holds." This encompasses methods and practices that make sense for your organization, understanding where technology is needed to facilitate or improve process efficiencies or quality of results, and identifying which specific technology capabilities are required to make your end-to-end process effective. It is best accomplished through a cooperative effort among legal, IT, and the line of business (LOB) organizations (see Figure 2).*

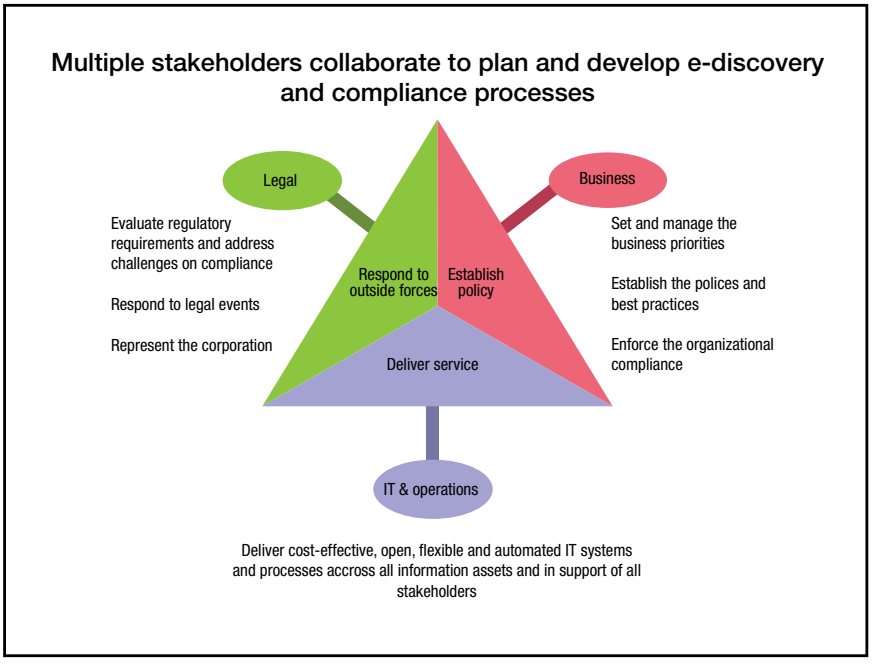

Figure 2. Electronic discovery and compliance processes stakeholders

Highlights

Other activities to prepare for electronic discovery:

- ***Consider technology capabilities***
- ***Conduct benchmarks***
- ***Develop processes***
- ***Implement records management***

- *Consider technology capabilities such as dedicated computer storage and processing resources with robust security, inventory, and identification of sources of ESI potentially relevant to the request. Also look at search and retrieval tools that can be responsive to the request and are robust enough to deliver results in tight time frames and with the appropriate degree of precision, among others. You should also consider integrated content management, which provides "middleware" to link multiple sources of ESI for search, retrieval and possible collection, if there are multiple content sources.*[4]
- *Conduct benchmarks to test and establish estimating parameters for various electronic discovery scenarios. Repeatable processes that have been tested to provide evidence of results sought after records production for a given set of metrics can be a significant key to negotiating e-discovery requests, to effectively planning the response activities and timeframe, and to prudently applying resources and budget.*
- *Develop repeatable processes that have the flexibility to accommodate a variety of discovery and regulatory requests. Electronic discovery is not a one-time occurrence for many organizations. Requests for information continue to increase whether from regulators, courts, government, or public interest groups. Traditionally, each "case" might have been managed by a different functional unit, attorney or firm dictating different approaches, practices and technical framework. Many now realize that the basic process and technology used to conduct electronic discovery can be separated from the legal or business strategy and these need not be "unique" solutions. Whether discovery results should be siloed or not is a question to be determined in consultation with professionals (legal counsel, accounting professionals, or others) and based on particular circumstances. However, the technology methods and solutions can be developed with the flexibility to accommodate a variety of capabilities, scenarios and needs, while being based on a common architectural platform and a common set of products.*[5]

Highlights

Maintaining an inventory of ESI sources, implementing an ESI records management program, and keeping the program updated with changing regulatory and enforcement requirements will help you prepare for electronic discovey negotiations.

- *Develop and implement records management and retention policies that can effectively preclude retaining nonmaterial information. Formal guidance to promote the appropriate and prompt disposal of unneeded ESI is an important component of records management.*
- *Maintain an inventory of ESI sources that documents system descriptions and characterizations such as computing system and location, software product and version, business purpose and scope, data storage (active drives or archives), retention location and periods for backup data, estimated volume of data being retained, native capabilities for search and data formats, and so forth. This inventory provides auditors and legal counsel with data needed to estimate electronic discovery time and costs and to determine an efficient and reasonable approach to develop the body of material for legal review. If this type of inventory does not presently exist, a potentially reasonable approach is to create it through a project led by the technologies team, with the active participation of those needed to help gather and evaluate such data, such as legal counsel and auditors. They should provide guidance as to their requirements and needs, and as beneficiaries of the inventory project, might also provide budgetary support. Even electronic discovery requests for e-mail can result in subsequent requests for data from other systems to which messages can be linked or referenced, and this separate inventory can provide considerable value.*
- *Implement an ESI records management program that controls the volume of information through appropriate and regular destruction of ESI in the normal course of business. In addition to establishing and implementing destruction policies, the records management program also should provide the mechanisms and protocols to suspend destruction for specific ESI required to comply with discovery and preservation orders. A major cause of the explosion in ESI volumes is the practice of keeping "everything" because of hold orders, rather than limiting holds to only the information required. Hold orders ideally should not cause major disruptions in document- or ESI-management processes. The protocols for implementing and ultimately releasing holds should be built on and leverage the records management system used in the normal course of business.*

Highlights

Legacy data can be a major concern.

Addressing legacy data requires an understanding of the record retention and accessability requirements, determining which data needs to be retained, and determining the best approach for storage.

- *Keep pace with changing regulations, new requirements and trends in enforcement. Have a process whereby compliance or regulatory affairs, or whatever organization has the responsibility to monitor regulatory initiatives and implement compliance measures for new regulations, communicates the requirements across the enterprise. These communications would include, for example, legal, technologies, risk management, records management, audit and relevant LOB management. Potential impact of legislation such as SOX and Basel II (financial services) on requirements for controls and audit trails across intra-organizational boundaries should be understood. Records management mechanisms, technologies, and protocols for retention and destruction should be reviewed and appropriately updated in a timely manner.*

For further information and considerations about preparing for the new Rules of Civil Procedures for electronic discovery, see the appendix of this paper.

Root causes of common electronic discovery issues

Corporate legal counsel can more effectively approach electronic discovery when armed with specific knowledge of what information is being maintained, how it relates to business activities, and how it can be accessed and produced in the event of a discovery order. It is a challenge for any company to predict electronic discovery costs and issues, but there appear to be some common factors that may make electronic discovery difficult and costly across a variety of enterprises.

Issue 1: Legacy data and ESI

- *Legacy data can be a major concern. This data might have been inherited from an acquired company or be data that was not migrated after a technology upgrade. These systems, which in many cases can be made accessible only by maintaining older or obsolete software and hardware, can contain accounting, finance, customer data or other LOB information. In addition to the administrative costs of maintaining this data on the network, people with the skills to understand the context of the data and the available access protocols must be kept on staff. These systems can be especially troublesome to search, and it can be difficult to collect, cull and produce required ESI because of their obsolete or historical design or lack of support for these functions.*

Highlights

Assess your legacy data.

- *The first step to address legacy data issues is to inventory the information and identify what records retention requirements apply. It might be preferable to document the inventory and analysis, and establish appropriate retention policies in advance of the need to produce ESI because of legal or regulatory actions or for other purposes. This important first step can lead to decisions to eliminate some of the systems, and can decrease the volume of data for others where there is still a retention requirement. You might want, in consultation with your business experts and counsel, to document the process of decommissioning systems and the method of ESI destruction.*
- *The second step is to weigh the costs of retaining the data using another approach, compared to current costs and the difficulties of producing the data when required. Some options are:*
  - *Converting the data or migrating it to the current technology platform in a manner that will not jeopardize its integrity.*[6]
  - *Migrating the data to an archiving platform where it can be maintained on lower-cost storage and would no longer be an administrative cost or performance burden on the network, but where data can be accessed, searched, and retrieved in a useable form if needed.*
- *Determine how significant the legacy data issue is:*
  - *One company that the IBM team knows of accumulated more than 30 000 databases from its collaboration system over a period of ten years. With no records management and retention policies in place for ESI, many of these databases had become "orphans" with no current owner identifiable who could aid in establishing possible business value of the databases.*
  - *Another company the IBM team knows of had more than 25 existing systems (mainly because of acquisitions) that were burdening its network, and required additional staff with the special skill sets needed to maintain these applications because the business value and retention requirements for this ESI had not been established.*

Highlights

Electronically stored documents have a distinct lifecycle and some organizations may benefit from instituting controls appropriate to each life-cycle stage in accordance with their management policies.

- *To help prevent the legacy data issue from reappearing in the future, update IT governance processes to include identifying record retention requirements as part of the systems implementation methodology (including absorbing data from corporate acquisitions or mergers). The costs and methods for dealing with legacy data in accordance with appropriate compliance practices should be part of the overall system implementation and maintenance budget. You should not leave data-migration and conversion requirements to the end of the project, and you should evaluate and disposition legacy data as part of the records management program implementation.*

Issue 2: Lack of life-cycle management and controls for ESI

Both poor retention practices and issues such as orphan records (those having no identifiable owner) can be mitigated by recognizing that electronically stored documents have a distinct lifecycle and that controls can be imposed appropriate to each life-cycle stage after management policies are established. Each type of ESI may have unique life-cycle stages with differentiated controls and policies. Archiving and migration policies for messaging-type ESI provide one example of how life-cycle management is being applied. (See Figure 3.)

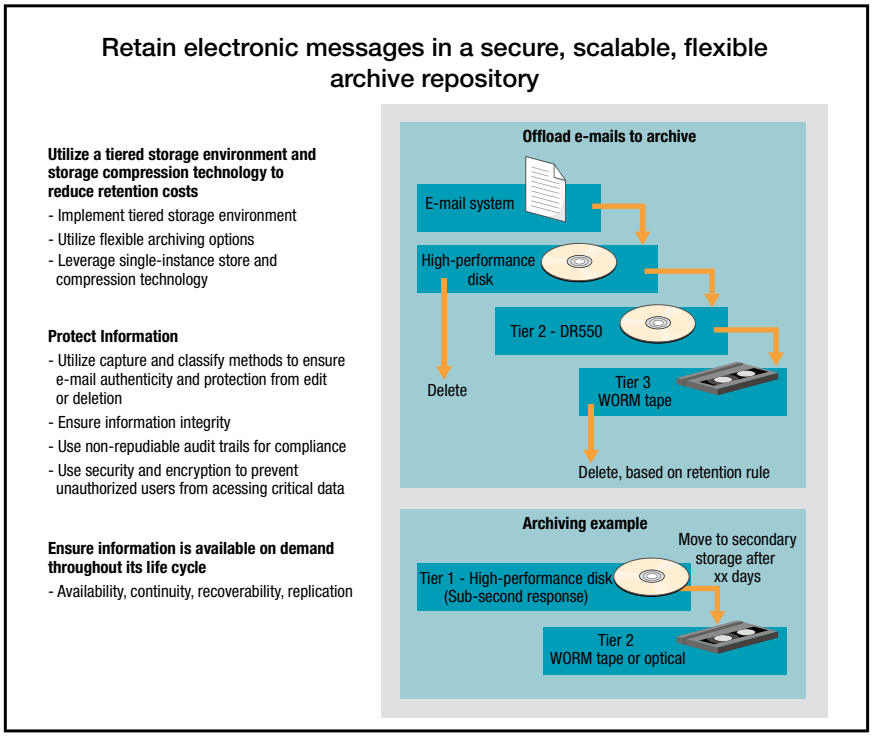

Figure 3. Archiving and life cycle management example for electronic message systems

Highlights

Document management technology facilitates application of lifecycle controls and can provide a chain of custody, mitigating the occurrence of orphan records.

Other considerations for ESI lifecycle controls are:

- ***Proper use of CD's***
- ***Security and disposition of laptop data***
- ***Automating the application of standards***

- *Document management systems are gradually replacing the use of shared drives for storage and access to electronic documents. Document management technology also provides abilities to purge, disposition and search for electronic documents in ways for which there is no physical paradigm. For example, compound, complex documents consisting of embedded files (a spreadsheet within a text document, for example) or hyperlinks require new types of methods and tools for effectively responding to discovery and document production requests. In addition, the metadata (much of which cannot be directly accessed or printed) can provide helpful ways to manipulate, search and contextualize the data.*
- *Orphan records – which can be database backups, files on shared drives or other electronic information with no apparent or designated owner – represent costs and risks that could be potentially mitigated with more effective document management practices. It might be difficult to ascertain whether these are duplicates of other record holdings, drafts or otherwise out-of-date information that should not be retained. Orphan records create a burden for discovery efforts, and can be more easily overlooked when searching for materials, because there is no current business owner with responsibility for dispositioning these records or even cognizant of their location and content. Orphan records can be a significant portion of files on shared network servers as well, increasing network maintenance and backup costs as well as the number of servers to be procured and maintained.*
- *Use of CDs to store copies of information can result in loss of control of ESI. CDs can be easily transported and are outside any technical system of accountability and could easily be misplaced or misused.*
- *Information stored on laptops is a growing threat to the security and confidentiality of ESI and this kind of information is discoverable. Laptops have been subpoenaed in court actions and they also can pose risk of data privacy breaches. Incidents with laptops, as well as magnetic tapes, have been reported on a regular basis in the United States.*

- *Awareness of relevant life-cycle stages and instituting associated controls is a key means of automating standard practices such as:*
  - *Deleting drafts after the document has progressed to the "record" or "published" state where appropriate to comply with corporate policy*
  - *Promoting the use of metadata standards for identification, classification, ownership and other useful denominators*
  - *Promoting security and change privileges for documents that are differentiated based on their life-cycle stage*
  - *Providing for the disposition of documents based on life-cycle stage and retention policy (for example, archive when superseded)*
  - *Providing capabilities to trigger archiving or transfer to lower-cost storage based on aging combined with attaining a life-cycle stage (for example, archive two years after attaining record status)*
  - *Automating the migration of e-mail and messaging content as well as application data (for example, enterprise resource planning [ERP] systems) to online archives where ESI can be easily accessible while improving the efficiency of the source applications*
- *Steps some companies are taking to improve life-cycle control of ESI:*
  - *Inventory ESI on shared drives and obtain assessment of business use and value from owners*
  - *Develop retention categories and policies that are practical for both auto-assisted and manual classification of ESI*
  - *Migrate documents required for compliance with retention policies to a document management platform with life-cycle capabilities to control storage, access, and dispositioning with automated or semi-automated rules; eliminate "shared drives" from the network*
  - *Enforce storage and retrieval of "controlled" files using only the document management system by eliminating "desktop" document files and folders as well as shared drives*

Highlights

- *Control what information is retained on employee computers using records management software that automatically attaches and enforces disposition rules*
- *Promote other policies and practices that will bring "order from chaos" in regards to document retention.*
- *Establish protocols for electronic discovery leveraging the standards and capabilities of document management, archiving, and federated records management and search platforms. E-mail archiving and complex query technologies are high priority.*

Corporate record retention programs and policies—especially classification schemes—may need to be realigned to effectively support both records management and legal discovery for ESI.

Issue 3: Outdated corporate retention policies and implementation methods that are ineffective for ESI

- *Our recent experience discussing records management for ESI with a variety of companies shows that many have not yet taken significant steps to realign their corporate record retention policies and methods to effectively address ESI and support electronic discovery. Some examples:*
  - *Retention schedules are based on organizations, departments or business units rather than business functions, processes and systems. Modern business systems are used by multiple departments and data ownership might be dispersed as well, requiring updated classification models.*
  - *Nomenclature on corporate records retention schedules can be based on titles of physical reports or documents that can have multiple files, file types or system components in today's ESI technical environment. Some examples are embedded files (spreadsheet within a text document) and dynamic Web content. Understanding how the ESI is structured and which ESI is the equivalent of scheduled physical records can be a significant project.*
  - *If corporate records management policies do not address ESI, electronic documents and data stores may have no formally designated retention. Retention practices and policies might be formulated and implemented by IT without due consideration of compliance needs or consultation with appropriate professionals, such as auditors or legal counsel.*

Highlights

Doing an overhaul of the records management program to accommodate ESI and dealing with the growing volumes of ESI may require new skills, protocols, and technologies.

- *Nomenclature and classifications are not structured in a manner that it is feasible to create automated or semi-automated rules for an ESI implementation. Simplifying and rethinking the approach and design of retention and disposition "rules" might be needed to effectively match ESI with applicable compliance requirements and to best conform them to be adequately responsive to electronic discovery and document preservation orders.*
- *Data recovery files become the means of fulfilling retention requirements. Retention periods for these files can be established by IT with no consultation or formal approval of appropriate corporate personnel, such as auditors legal counsel or compliance experts. Files created with data-recovery software are designed to be used with "restore" programs should that need arise. They typically are not designed for any other purpose (for example, searching or viewing of data), and if the backup files do not match the current technical configuration (not created with the current version of the system or application, for example) they will be the most costly and difficult to "restore" to an accessible format.*
- *Protocols and mechanisms for expunging or certifying destruction of records, which have been an important element of physical records management programs, might be nonexistent, informal or not adequately documented to evidence that disposal of ESI was done in accordance with the company's records management and retention policy and in compliance with requirements for audit trails.[7] Use of Write Once Read Many (WORM) media, implemented without consideration of requirements for expungement of ESI having diverse retention periods, can result in companies violating their own retention policies.*

- *To avoid increasing risk and costs of noncompliance, it is probably advisable not to just update the records retention and management program, but to completely overhaul it. This requires knowledge of electronic records, records management, and ESI technology issues and characteristics, as well as an understanding of the total information fabric of the business encompassing information in all forms.*

Highlights

Fully automated end-to-end business processes may result in ESI being the only record, with no physical counterpart. For this reason as well as trends in legal discovery, ESI should not be overlooked by corporate records managers.

- *Recognizing that a growing volume of digital information has no physical counterpart (absence of system data, metadata, embedded files and so forth differentiates any attempted physical representation), and that litigation discovery demands can routinely require the production of ESI,[8] more companies are beginning to manage ESI as records. One example is e-mail records being retained in searchable, electronic archives to meet requirements of U.S. SEC Rule 17a-4 for retention and timely production of specific communications when requested. Meeting this requirement would not be feasible in all but the smallest of organizations without the electronic records archive.*
- *How pervasive is this phenomena? Today's fully automated business processes may result in ESI being the only complete record (for example, the IBM team observed in one insurance company that 80 percent of the claims were auto-adjudicated [settled using software and automated transactions] with no corresponding physical record file of the transaction. Another example is that it is unlikely that all e-mails containing essential business information are all printed and, even when they are printed, they lack valuable metadata, which makes the physical form "incomplete" as a record).*
- *As systems and processes are changed, for example, to take advantage of new technology, there might be unanticipated effects on records. At one company that the IBM team studied, the system for producing customer replies – correspondence from customer service – composed responses on-the-fly (from various text components in the system) but did not produce a record that could be filed with each customer's account record and therefore be available, in the event of subsequent customer inquiries, to the account representative. Customers might, therefore, complain that they did not receive notification by the company of procedural changes having an impact on their business, and there would be no record to prove they had been appropriately notified. This is a not uncommon example of how electronic systems might not create (much less retain) a "record" unless they are specifically designed to do so.*

Highlights

- *Digital information can be searched, analyzed, shared for collaboration or processing, and produced more readily than physical forms if appropriate policies, tools, and protocols are in place. A concerted effort to create an effective records management program for ESI might reduce volumes of physical material held in storage considerably and significantly decrease discovery efforts and production of physical records.*
- *Documents created as ESI can be handled in consideration of record requirements from the beginning of the lifecycle (for example, identify with a record series or case file at creation). This can be done effectively with a combination of document management and records management enabling technology, and be facilitated further with archiving strategies and tools, especially for massive volumes of ESI in e-mail and messaging systems.*

A hold management and e-discovery strategy should consider:

Developing a standard appproach.

Maintaining a document production and investigation capability.

Establishing a consistent team with appropriate skills.

Establishing a set of tools for providing results and establishing protocols.

Issue 4: Lack of hold management and e-discovery strategy and support

- *Both hold management and electronic discovery are processes that can benefit from a more standardized approach than is used in many companies, based on our experience. Although the IBM team has observed that some companies have designated a team to disseminate document preservation orders, the actual implementation of these, as well as discovery orders, might be undertaken with sparsely defined, ad hoc processes and minimal preparation, rather than with a structured approach. Lack of an established infrastructure, repeatable protocols, and a skilled, experienced electronic discovery team means that lessons learned are not learned, ineffective approaches might be repeated and unacceptably voluminous amounts of material might need to be culled after initial collection, increasing response time and costs.*

- *Maintaining a timely document production or event-investigation capability means having the required people, business processes, technology and data readily available as needed. Typical steps for such a process to consider in readiness and planning exercises are:*
  - *Preparation for the discovery or investigation effort*
  - *Project, event or matter folder creation*
  - *Keyword, advanced search and analytic tools*
  - *Appropriate reviews and analysis*
  - *Output media creation*
  - *Output media delivery*

  You should consider all these steps when developing a document or data production plan. An understanding of each in the context of a specific business can in turn be helpful in promoting the negotiation of reasonable timelines and efforts when faced with demands.
- *Effective use of electronic discovery and search tools is often influenced by the amount of experience with the process and the tools. Establish a consistent team with appropriate skills in electronic discovery and knowledge of your company's ESI sources, technology platforms and tools.*
- *Establish a set of tools that can provide predictable results based on established protocols. Also conduct benchmarking exercises periodically against a variety of ESI sources to establish metrics using your tools of choice. These metrics will help to establish the time frames and costs of searching various electronic source systems using various scenarios and parameters. For example, how long does it take to search and report results on 20 named individuals in your e-mail system regarding one matter over a period of three years?*
  - *Understand the metrics and time requirements for simple search, de-duping and creation of "collection" stage files, separate from the time and effort required for legal or other reviews, advanced searching, and culling of nonrelevant or privileged information. Conduct the benchmarking on current systems, retired systems and archive systems.*

Highlights

The electronic discovery strategy should consider:

- ***All sources of messaging data***
- ***Hold management rules***
- ***Records management versus retention management policies***

- *For an e-mail production, it is important to have a catalog of all messaging data sources. To maintain full legacy retrieval capabilities, this might, for example, include:*
  - *Optical disk catalog*
  - *Tape backup catalog*
  - *Legacy tape backup hardware currency*
  - *Legacy tape backup software availability*
  - *Legacy e-mail software versions*
- *Hold management rules (prelitigation identification of potentially material information and ongoing implementation of document preservation orders) requires special attention and tools for ESI. The "rules" that will determine which ESI are to be held (beyond their scheduled retention period) require careful crafting (by legal counsel, perhaps with assistance from IT and LOB managers) and an analysis of holdings in the context of ESI and business systems. A lack of a clearly defined "registry" for records (such as can be provided by a document management or records management system) to which the rules can then be applied, constrains adoption of automated techniques and can lead to an outcome that all ESI is "on hold forever." This means, for example, that although one or another large litigation has been settled, other litigations might still be ongoing and because of the inability to clearly distinguish which records are under any specific hold order, all ESI continues to be retained indefinitely. Lack of effective hold management can threaten to paralyze IT organizations struggling with massive volumes of ESI that has been on hold indefinitely.*
- *Investing in a "retention management only" approach compared to a records management approach that can manage the lifecycle of specific records appropriately might not be the shortcut it appears to be when one needs to implement preservation orders or event-based retention periods. Having retention policy embedded in each siloed repository (Large companies may have more than 15 repositories), or retention folders crafted by users on-the-fly, means that each of these will need to be addressed in the event of a hold order. In this manner, retention management can create further complexity rather than reduce complexity. Also, the communication of events – such as the expiration of a contract or completion of an audit – becomes far more difficult to implement. When records management is treated as an automated service (with a single rules engine that enforces controls across multiple repositories), legal holds and corporate retention policies can be centrally managed. This simplifies administration and facilitates compliance because the affected ESI can be locked down regardless of the repository or application in which the ESI resides. Investment in records management (compared to retention management) is a time-proven approach.*

Highlights

Management of e-mail entails determining which e-mail should be treated as records and establishing classifications and retention rules based on business context.

E-mail management

Perhaps the most-frequently asked question when an IT organization begins to establish retention protocols for e-mail is "How should e-mail be handled?" The best practice is for IT to consult with compliance, legal and audit advisors, and identify the key regulatory requirements applicable to the business. For example, there are specific requirements for retention and retrieval of communications (which would include instant messaging and other technologies in addition to e-mail) if your company is in the brokerage business. Examples would include the U.S. Securities and Exchange Commission (SEC) Rule 17a-4 and National Association of Securities Dealers rules (NASD 3010/3110), and other SEC and NASD rules can apply depending on the specific services offered by your business. Another example of industry requirements is the U.S. Federal Energy Regulatory Commission (FERC) 18 CFR, Part 125, which describes a detailed list of record classifications and retention requirements applicable to electric utility licensees.

There are also laws such as SOX that apply to many enterprises by virtue of their public company reporting requirements. Enforcement agencies often have broad authority to examine company records, especially those which evidence chain of custody and audit trails for developing financial information that is made public.

Other laws, such as the U.S. Patriot Act, may also be applicable to many types of businesses. Regulations are promulgated by the federal agencies in the executive branch of the U.S. government that are responsible for enforcement of certain laws. There can be several agencies which have responsibilities for different aspects of a statute. Creating the regulations and having them reviewed, approved and released is generally a lengthy process, and there can be many months between the time that a law goes into effect and the time that the regulations that specify compliance requirements are published and made effective.

Retention policies are, as a best practice, based on the business value and business context of the information, not on the "system" in which it is maintained. Therefore, e-mail communications associated with employees engaged in one role can be given a three-year minimum requirement for records retention, whereas in another role, e-mail communications can be subject to different retention policies – such as a seven-year minimum if related to company financial information.[9]

Highlights

Implementing records management for ESI requires a pragmatic approach. Keep classifications, file plans, and retention categories as simple as possible when first establishing the program and refine as the implementation and the cultural acceptance matures.

Is records management practical for ESI?

As a starting point, the business needs ought to drive ESI retention policies. To promote the establishment of reasonable as well as practical policies, it is possible to establish some ground rules that can be broadly applied in the absence of any specific regulatory requirement. For example, considering that many retention periods are event driven, a policy might be established that retention periods that are triggered by completion of an audit (quality audit, financial audit, regulatory audit and so forth), are all the same number of years. This rule could be, for example, expressed as audit + 3 months and, in some enterprises, could cover a wide range of records.

Another useful strategy when dealing with ESI retention policies, and especially with a system such as e-mail that covers a wide range of business activities, is to establish — as an initial step — some broad categories, which can be refined in later stages of a records management implementation. These categories could be as broad as financial, engineering, manufacturing, customer relations, human resources and so forth.[10] The retention periods initially assigned to the whole category can be longer than required for some information classes within the category, but these provide an initial level of management that is not complex to implement, and through the prudent use of audit trails, can later be refined without undue risk. Those categories presenting the greater business implications or risk can be made the priority for the refinement step, as the goal is generally to retain the minimum amount for compliance.

Audit considerations

Supporting audits — whether regulatory audits, financial audits, internal audits or other — requires some additional ESI management capabilities beyond those most often needed for general legal discovery. These capabilities pertain to safeguarding the integrity and trustworthiness of records and being able to demonstrate those controls.

Auditors require that records produced for their review be trustworthy and authentic, and maintained, therefore, with safeguards that prevent tampering or modification of completed records. Auditors must be comfortable that the records they examine are objective evidence of business processes and of the controls that have been exercised in those processes.

Highlights

Consider an "evidence repository" for ESI that provides a record of the proper application of business controls

Auditors might be reviewing records for a special investigation or to periodically verify that the organization is in compliance with pertinent regulations. Certain regulatory bodies conduct audits on a regular schedule, such as once every two years. To be prepared for these audits, protocols should be established that leverage previous audit results and documentation, types of records that are customarily requested, and ESI that must be made available. It is a common practice for auditors to send the organization's compliance officer (or other designated contact) a list of documentation and ESI (sometimes specific data sets) that he or she needs to review or test and therefore expect to be available at the commencement of the audit. If this information is not available, or not acceptable because of a lack of controls, the organization can be cited with a deficiency, which could result in a reported noncompliance and possibly penalties. One example that was widely reported in 2005 is the SEC/NASD and New York Stock Exchange levy of $8.5 million in fines on five brokerage firms for failure to preserve e-mail communications.

To evidence authenticity and trustworthiness, ESI that are records being retained for compliance should be: 1) locked down in a manner that prevents modification or premature destruction, 2) created and managed in a manner that provides an audit trail and demonstrates the chain of custody, and 3) controlled throughout their lifecycle and captured as closely as possible to the time that the ESI became a record (upon completion or upon final approval, for example, in accordance with predefined protocols).

Summary of best practices for electronic records management

Best practices for electronic records management, which can help support both compliance and legal discovery processes, include: 1) repeatable processes guided by policies, 2) standards for various types of ESI classifications and metadata, 3) enabling technology to support consistent practices and policy implementation, 4) a change management strategy based on leadership, education and awareness, and 5) enforcement and measurement of compliance through management audits and corrective action programs.

Highlights

Design the retention program within the context of your business.

Evaluate sources of ESI.

Implement policies and records-destruction practices.

Update IT governance practices.

Consider the impact of encryption policies.

Consider the impact of destruction methods.

Control through a corporate records management policy.

- *Consider the information fabric of your organization and create policy-based rules for managing ESI that will not only facilitate discovery and document production activities, but will yield business benefits as well. Defining and incorporating records life-cycle-based controls and retrieval protocols will also facilitate meeting trustworthiness and authenticity requirements. Across the enterprise, e-mail, instant messaging, call center records, files on shared drives and personal computers, and so forth, can all contain records related to the same business event or activity. These cannot be consistently managed and controlled without a policy.[11] Policies ideally should be based on business context and value, not the format of the ESI. Policies might cover not only retention requirements, but management practices and controls also, with minimal standards for metadata, for example, across the enterprise.*

Make retention decisions in the context of what the data represents, where it resides, longevity of preservation, and vitality of systems

- *Evaluate systems (sources of ESI) and determine how older information might reasonably be accessed – and if it cannot reasonably be accessed, examine critically why it is being retained. Technology organizations can evaluate needs for archiving and retention systems that can provide reasonable access in the future to ESI that has aged beyond the time it is required to be maintained in the current information stores. Establish total retention periods and those for each life-cycle stage, such as "archived, but online." Basic retention classes could be based on business roles of the originator, the organization of the originator, or the business activity (for example, customer service communications).*
- *Implement policies and records-destruction practices in accordance with documented protocols that become part of the normal course of business.*
- *Update IT governance practices to include identification of retention requirements (based on legal, regulatory or other factors) in the design requirements for new systems. If the enterprise is involved in a merger or acquisition of another company, identify requirements before data conversion activities or legacy systems disposition decisions begin. Create a linkage to the overall records management program for ESI.*
- *Consider the impact of encryption policies on search and retrieval capabilities. With the increasing adoption of encryption for e-mail and attachments, there are concerns that e-mail will not be searchable because of "loss" of the appropriate encryption keys, introducing further complexity to maintain accessibility of aging ESI. ESI that is subject to production but cannot be decrypted could result in raising suspicions of spoliation.*

Highlights

The capability to trigger retention periods based on a business event, for records residing in a variety of repositories, is required for enterprise records management.

- *Consider the impact of destruction methods and available technology. If ESI that is aged past its required retention period is not destroyed in a manner that addresses the complete record (metadata as well as the document or content, for example) and expunges in a manner that reasonably precludes reconstruction, you might be creating risk. In any event, ESI should be destroyed using standard protocols and in compliance with established policies and practices directed at "electronic shredding."*

Maintain documentation of corporate records retention policy changes

- *Maintain an audit trail of policy changes, approvals of changes, and effective dates of policies and policy revisions.*
- *Multiple regulatory requirements can pertain to any particular class of ESI. Therefore, when there are changes in any particular regulation affecting records, the impact of that change on the retention policy must be evaluated in consideration of other requirements that might apply.*

Implement records management policies for ESI across the enterprise

- *Many organizations are making e-mail communication an early priority for ESI that is brought into a records management program. It has long been a rule of thumb among records management professionals that with the implementation of a records management program, volumes of information being retained in primary storage might be reduced as much as two-thirds. That is, approximately one-third of the material can potentially be destroyed in accordance with established corporate policies, and another one-third can be moved to less-costly records storage (with appropriate controls to provide security, protection from loss and so forth). Considering the volume of ESI in messaging systems, this might make records management a more attractive proposition and a higher priority for those systems.*
- *Establish standard practices (automated where feasible) for regular destruction of ESI (for example, on a monthly or quarterly basis) that are not unduly burdensome on employees.[12] Establish communications and oversight practices that reinforce awareness and promote compliance. Destroy ESI as soon as is possible, on a regular, consistent basis and use methods that promote security and privacy for the information being destroyed (for example, don't toss a CD in the trash basket).*

Highlights

- *Because many retention periods are triggered by an event, an event notification to the records management system to trigger the start of a defined retention time period is critical. Uncertainty over whether or not an event has occurred (such as termination of a contract, for example) might cause excessive retention beyond legitimate requirements. To remedy this, the best practice might be to provide either a system event-notification capability that communicates from the business system to the records management system, or provide manual procedures to address the areas of greatest risk or expense. With an understanding of the key retention requirements (such as ability to recreate customer transactions and communications for a lengthy period to satisfy some regulations), records might also be tagged at the time they are created or declared in a manner that facilitates this process, such as standard customer identification schemes. Any ESI that is on hold would have the retention period trigger set "on" when the event has occurred, but would not be destroyed until two conditions are met: the "hold" was lifted and the retention period has expired.*

Trends in legal discovery indicate that the legal team can benefit by being armed with knowledge of ESI sources and retention processes.

Establish traceability and provenance where required

Establish basic metadata[13] that will be maintained as part of the record for each class of ESI and implement metadata standards.[14]

- *In the case of e-mail communication, maintaining who sent it, who viewed it and who replied, can establish the provenance and context of the business activities.*
- *Consider methods to externalize the content using a text format like XML, tied to the metadata of the record where there can be cost or business benefits.*
- *Establish definitions and policies to clarify and distinguish final documents versus drafts as part of the life-cycle controls.*
- *Metadata associated with specific classes of ESI can be leveraged to also accomplish risk management goals. For example, metadata could be used to identify and then secure transactions by embedding the appropriate rules in routers (based on roles and responsibilities) or by triggering encryption.*
- *Identify audit-trail requirements when developing metadata standards. If there are requirements for traceability and chain of custody, for example, capturing (as metadata) who did what and when they did it (who created, who updated, and so forth) should be part of the metadata standard.*

Highlights

Begin evaluating your readiness for legal discovery and the new rules of civil procedure by reviewing your technology and IT infrastructure capabilities as well as management policies.

Negotiate what makes sense

- *The legal team should be armed with an understanding of what ESI is accessible and what is not before entering electronic discovery negotiations.*
- *Consider establishing a prototype (model of the system) for initial implementation of policies and standards and development of key protocols and training. Use the prototype to drive out requirements in meetings and workshops and achieve agreement among technologies, legal, compliance and business stakeholders.*

Establish a document management system for lifecycle management

- *Document management technology enables controls to be implemented prior to ESI becoming a declared record. For example, automatic destruction of drafts can be triggered after a document is finalized and declared a record, reducing the volume of ESI and storage costs.*
- *Shared drives – often used as a "dumping ground" – can be eliminated over time.*

Be prepared for electronic discovery and production needs

- *New U.S. Federal Rules of Civil Procedure may become effective by the end of 2006, and are designed to provide some added ESI-related consistency in federal discovery procedures across the United States. Refer to the Appendix for highlights of the new rules and considerations to help prepare for them.*
- *Technology is an important element for enabling retention policies and supporting compliance and legal discovery for ESI. In many cases, this can be accomplished in ways that are transparent to the end user and nondisruptive to business activities. Some of the potentially most useful technologies to consider are:*
  - *E-mail archiving (online, single instance e-mail archive)*
  - *Metadata management*
  - *Records management*
  - *Contextual analysis and classification*
  - *Analytic tools (visualization and relationships)*
  - *Document management*
  - *E-mail search*
  - *Content integration*

Conclusion

Managing ESI within the context of a company-wide records management program facilitates a number of corporate goals — risk management, corporate governance, compliance with regulations and less-disruptive legal discovery efforts. The greatest benefits are achieved by these programs through strong leadership that promotes a culture of compliance and with the aid of supporting processes and technologies that manage the growth and structure of ESI in the normal course of business. In many companies, this is a significant undertaking and requires the ongoing cooperation of legal, compliance, technologies and LOB stakeholders to evaluate ESI sources, participate in policy decisions and provide for effective implementation practices.

For more information

To find out more about how IBM can help you, contact your IBM representative, Business Partner or visit www-306.**ibm.com**/software/data/commonstore/

Appendix

Preparing for the upcoming electronic discovery amendments to the U.S. Federal Rules of Civil Procedure

The Judicial Conference has recently submitted a series of amendments to the Federal Rules of Civil Procedure to the Supreme Court and the U.S. Congress for final approval.[15] According to the Judicial Conference, these amendments are specifically targeted to address problems associated with the discovery of electronic information that were first discussed at an advisory conference in 1996. The advisory committee first began work on this in 2000 and has involved a large number and variety of experts in the fields of law and computer science and members of the public to arrive at these amendments, which are anticipated to take effect in December 2006. For businesses in the United States, these amendments will be of interest to compliance and regulatory affairs executives as well as general counsel as the rules of civil procedures also apply to regulatory investigations.

One of the committee's key findings was that the discovery of ESI differs markedly from that in paper form, which naturally has been the focus of conventional discovery procedures. A few of the differences it cited include:

- *Exponentially greater volumes exist than with hardcopy documents*
- *Unlike paper, the information is dynamic, being affected by the turning on and off of the computer itself, or by the computer deleting or overwriting information without the operator's intervention or direct knowledge*
- *Electronically stored information, unlike words on paper, might be incomprehensible when separated from the system that created it (loss of context, structure and other problems)*

It also found that the discovery of electronic information is becoming more costly, time-consuming and burdensome than for hardcopy information. The committee determined that unless timely action is taken to address these problems and make the federal discovery rules better able to accommodate the distinct features of electronic discovery, a patchwork of local rules might arise that could lead to inequalities in the American judicial system.

Likewise, timely action by legal counsel and compliance officers to prepare their business for the amended discovery rules could make a difference in turning these rules to their advantage or disadvantage in future litigation. To facilitate assessing the impact of these rule changes on present protocols and practices for maintaining ESI in your business and identifying possible actions you may wish to proactively initiate, Table 1 provides a quick summary of the rule changes with some limited, suggested actions that you might want to consider. The list is not intended to provide legal advice, of course, or to be complete or exhaustive, but can be a starting point for consideration and discussion with your counsel. Without a doubt, a greater understanding of the technology environment and ESI controls on the part of legal counsel, and their partnering with IT leaders and decision makers in regards to approved practices for ESI preservation and destruction, will be a requirement for prudent businesses in the future.

A secondary assessment of the impact of these rule changes on protocols for each of the stages of the discovery process would also be appropriate: that is, how they can affect implementing preservation orders (record holds) for ESI, collection of ESI, culling of the ESI collected, electronic review of the culled ESI and production of ESI. This can then provide a framework for identifying new skills, systems, planning, training and supervisory functions necessary to provide for compliance with legal and ethical obligations regarding the discovery of ESI.

Rule reference	Rule change	Strategic	Tactical actions	Goals
26(b)(2)	Procedure to negotiate ESI sources for electronic discovery	Counsel partners with IT leaders to understand and influence ESI storage and destruction practices	1. Take an inventory of ESI sources: • Systems • Repositories • Network drives • Notebooks • Mobile devices • Locations • Business content • Business owners • Retention and destruction practices • Formats 2. Develop protocol and metrics for ESI collection 3. Develop metrics and estimates for "burden" of discovery from each source	1. Proactively understand sources of ESI and relevance to discovery 2. Be prepared to identify potential sources and the difficulties and costs associated with producing such material, production of which might be deemed an unreasonable burden 3. Successfully negotiate appropriate limits of discovery*
Rule reference	**Rule change**	**Strategic**	**Tactical actions**	**Goals**
26(b)(5)(B)	Withdraw privileged or attorney work product information inadvertently produced during electronic discovery without inferring waiver of protection	Policy for identifying ESI as privileged or attorney work products	1. Categorize and rank ESI sources and content as privileged or attorney work products 2. Develop method and supporting technical approach to identify privileged and attorney work products (for example, content attributes) 3. Develop protocol for requesting return, sequester or destruction of protected material by receiver	1. Mitigate risk of inadvertent production of ESI that is privileged or attorney work products 2. Mitigate risk of waiver of protection

Table 1. Summary of rule changes

Rule reference	Rule change	Strategic	Tactical actions	Goals
34(b)	1. Negotiating the forms in which ESI is to be produced 2. Allowing for production of ESI in the form in which the party ordinarily maintains it or in a reasonably useable form (and requires it be produced in only one form)	1. Counsel and IT leaders partner to mutually understand the structure and capabilities of their IT resources 2. Establish policy for standard, "useable"** formats that make sense for both the business and electronic discovery needs	1. Identify software and versions needed to access ESI in each ESI source 2. Identify legacy and archived ESI and software and protocols needed to access 3. Identify protocols for production of ESI in standard formats (per policy) 4. Develop method and protocol for determining metrics, and time and resource estimates for production in standard formats	1. Minimize cost and time to produce ESI by solid understanding of capabilities and resources early in the discovery process. 2. Improve predictability of discovery costs through standard protocols and standard formats.
Rule reference	**Rule change**	**Strategic**	**Tactical actions**	**Goals**
37(f)	Limitations on sanctions for certain losses of ESI, typically caused by routine system operations***	1. Counsel partners with IT leadership authorizing retention and destruction policies 2. Counsel and IT together develop and approve policies and methods for data destruction	1. Identify data-destruction protocols for categories of data and consistent with each ESI source 2. Identify which ESI records or data classes are "at risk" of premature destruction as a result of "routine, good-faith operation of an electronic information system." 3. Determine appropriate methods and protocols to suspend routine destruction to prevent loss of information known to have possible relevance to litigation	1. Substantiate "good faith" and due diligence to preserve relevant information 2. Avoid potential sanctions through appearance of inattention or indifference to preservation responsibilities 3. Have measures to ensure preservation of ESI that is not "reasonably accessible" under Rule 26(b)(2)*

Table 1. Summary of rule changes - continued

** According to the firm of Morrison & Foerster,[16] a party that makes information "inaccessible" because it is likely to be discoverable in litigation is subject to sanctions now and would still be subject to sanctions under the new amendments.*

*** The definition of useable more frequently includes word-search capability (that is, would exclude TIFF or other nonsearchable formats).*

**** Some examples of routine operations that might be examined in a good-faith effort to protect against spoliation sanctions include:*

- *Suspension of overwriting protocols for backup tapes that are being retained for recovery of data in the event of a broader disaster or a system failure, or migrating data on potentially relevant backup tapes to a "reasonably accessible" electronic archive.*
- *Suspension of automatic e-mail deletion and destruction processes.*
- *Implementation of measures to protect hard drives for departing or transferring employees and for recycled computers.*
- *Communication of methods for preservation of potentially relevant ESI to all "covered persons," including that ESI normally stored on their own computers and disposed of at will.*
- *Protection of servers and file shares from decommissioning or migration that would make ESI "inaccessible."*
- *Retention of obsolete (legacy) software that might be needed to make ESI "accessible" that is stored in obsolete applications.*
- *Preservation of "snap shots" and time stamps of data in relevant databases.*
- *Preservation of documentation for legacy or obsolete systems that is necessary to interpret the data, produce reports and otherwise make the data on those systems comprehensible.*

End notes

[1] Throughout this paper, the term ESI is used to refer to all electronically stored information, whether as structured data or "unstructured" content, including metadata. This is in keeping with the terminology used by the U.S. Judicial Committee in the proposed amendments to the Rules of Civil Procedure, April 2006

[2] AMR Research reported in 2006 that 18 percent of companies they surveyed regarded the establishment of a legally defendable information environment the most-influential issue driving technology investments to address compliance. In addition, 84 percent of companies surveyed were addressing compliance enterprise-wide within North America. Source: John Hagerty and Fenella Sirkisoon, Spending in An Age of Compliance, 2006. AMR Research, Inc., 2006. p. 15.

[3] In 2005, Network Computing reported that only 17 percent of companies used a policy-based archiving system to preserve e-mail. Source: Network Computing, May 12, 2005. www.networkcomputing.com/

[4] According to Forrester Research, the typical enterprise has at least three content repositories, and 40 percent have six or more.

[5] Content integration technology is being used by some companies as they move to a common technical platform. This technology provides a single "content bus" or application programming interface (API) that allows the connecting of multiple repository products, network file systems and existing systems so they can be searched or managed as if they were one. This can provide a near-term alternative for companies wanting to gradually migrate their ESI from multiple, departmental platforms to a corporate, standard technology platform, according to Intelligent Enterprise. Bruce Silver, "Content: The Other Half of the Integration Problem," Intelligent Enterprise, Vol. 8, No. 10 (2005), pp. 33-37.

[6] See "Audit considerations" for further information regarding trustworthiness and integrity.

[7] Gartner cites destructibility as a principal difference between paper and electronic records, stating "Electronic evidence is much harder to destroy than paper evidence, mostly because it is easier to disseminate and has metadata stored with it. There are multiple copies of electronic communications. Although one can easily find 10 paper copies of a document in a company, there may be hundreds of electronic copies. E-mail often is stored outside the originating company on Internet service providers' servers, as well as recipients' servers and hard drives." Debra Logan, John Bace, Mark R. Gilbert, Understanding E-Discovery Technology, Research ID G00133224, Gartner, Inc. November 29, 2005, p. 2.

[8] According to the U.S. Judicial Conference Committee on Rules of Practice and Procedure, there are inherent differences between physical documents and ESI. "The proposed amendment to Rule 26(a) clarifies a party's duty to include in its initial disclosures electronically stored information by substituting "electronically stored information" for "data compilations" (p. Rules – 26). Also, "Under proposed amendment to Rule 34 electronically stored information is explicitly recognized as a category subject to discovery that is distinct from "documents" and "things".(p. Rules-28).

[9] Keeping track of the basis of retention decisions is also a best practice. Specific retention policies might need to be reevaluated in the future because of changes in laws or business activities, and it is important to understand if retention decisions were driven by specific regulations, business activities, roles or other criteria.

[10] Corporate records management policies can designate a "disposable information" category constituting, for example, any information that is not essential or reference information required for the business, and mandate that this information should be disposed of immediately. If this class of information is identified in, for example, an archive for ESI, the policy can be applied to give it a minimal default retention period in the system, or even to not migrate it into the archive. This precludes the accumulation of extraneous messages, for example, in the messaging archive. This would facilitate consistency with the company's policies for physical records management practices in cases where this "disposable information" is excluded from physical corporate records retention schedules and prohibited from physical records storage.

[11] The technology strategy and platform is critical to enable the consistent application of policies applicable to any particular category of business information for which the corresponding ESI is maintained in disparate systems. Experience has shown that employing a technical approach that centralizes records management policy administration but can provide a "federated" approach to records controls might be necessary in many organizations.

[12] That is, destruction based on records management policies and any applicable court orders for preservation of ESI.

[13] Metadata should be consistent with standards for master data and data standards for official system of record where applicable as best practice.

[14] Changing or enhancing the metadata of legacy ESI (any ESI retained as a record prior to implementing the standards) should be considered with care if it is being retained for compliance because this could be construed as "altering" an existing record.

[15] .1. Committee on Rules of Practice and Procedure, Report of the Judicial Conference: Committee on Rules of Practice and Procedure Federal Rules of Civil Procedure, Agenda E-18 Rules, Appendix C-1 (US Courts, Federal Judiciary), (www.uscourts.gov/rules/), September 2005, pp.C18 – C109.

[16] Steven M. Kaufmann, J. Alexander Lawrence, John L. Kolakowski, "Upcoming E-Discovery Amendments to the Federal Rules of Civil Procedure," Legal Updates & News, Morrison & Foerster (www.mofo.com), March 2006.

IBM Corporation
IBM Raleigh (RTP)
Building 500
4205 S Miami Blvd
RTP, North Carolina 27709-2195
U.S.A.
(919) 543-0091

Produced in the United States of America
10-06

G224-7582-00