A Practical Approach to Enterprise Records Management

Introduction

In the past several years, business and public sector executives have become painfully aware of the need for “compliance.” Sarbanes-Oxley, HIPAA, and industry-specific mandates have elevated record-keeping and record retention to C-level attention. In the wake of scandals and litigation has come legislation spelling out in detail what was only implicit before: that an ever-increasing fraction of electronic information in any form, including email and even instant messaging, must be logged, saved, indexed, and securely retained for years, just like paper records. In the US, Sarbanes-Oxley, SEC Rule 17a, NASD 3010 and 3110, and various other mandates today not only formalize broad new record-keeping requirements, but stiffen civil and criminal penalties for non-compliance. And it’s the CEOs, not the records managers, who are being held accountable. Moreover, the Federal Rules for Civil Procedure has dramatically expanded the record-keeping requirements for all forms of electronically stored information.

Simply preserving records is not enough. Effective record-keeping demands ironclad procedures to guarantee that everything that can be considered a record is captured by documented and enforced business policies, with a reliable audit trail of all record-keeping activities. And when we speak of “records,” we do not mean only those official records maintained by trained records administrators. Today, a wealth of information dispersed over user desktops and network servers word processing documents, database reports, PowerPoint presentations, emails, and faxes, even blogs and instant messages – are considered records subject to retention and related compliance requirements.

The biggest worry, at least in the general counsel’s mind, may be the ever-present threat of litigation, in which the ability to find and produce on demand all related documents for discovery means the difference between winning and losing millions. The amended Federal Rules of Civil Procedure, adopted at the end of 2006, extend the definition of a record to include any form of electronically stored information (ESI) and require it to be disclosed early in the litigation discovery process.

The FRCP’s eDiscovery rules’ universe of discoverable information includes formats historically outside the bounds of records retention, such as digitized voice mail, surveillance tapes, and text messages. The staggering cost of producing these records in litigation, not to mention the potentially incriminating evidence they might contain or the severe consequences when they are unlawfully destroyed, has elevated records management onto the executive radar screen.

Although executives have come to understand that records management is serious business, many still do not realize the breadth of its impact across the enterprise or the diversity of requirements that it imposes. In some cases, they mistakenly assume that their disaster recovery system, email archive, or document management repository – systems designed for other purposes – are sufficient for their enterprise records management needs. At the other extreme, they may fail to realize that requiring DoD 5015.2-compliant formal records management for information subject to eDiscovery, for example, is costly overkill likely to encourage user resistance and ultimately failure to achieve the desired objective.

The right answer is an approach to enterprise records management (ERM) that is both comprehensive and flexible. A practical approach to enterprise records management is based on a
consistent, integrated infrastructure that supports the wide diversity of record types across the enterprise – from formal electronic records to informal memos, emails and discussion threads, to traditional paper and microfilm – without imposing a single set of management procedures across all record types and user groups. Instead, each group should be allowed to implement the management elements and procedures appropriate to the business need.

The purpose of this report is to explain the diversity of records management requirements at the enterprise level, and to describe the elements of a practical enterprise records management solution. For example, it will explain why the elements and procedures required by a records management application compliant with DoD 5015.2 – today’s “gold standard” for formal records management – are appropriate for certain records management needs but inappropriate for others. Finally, it will illustrate such a practical approach, both comprehensive and flexible, using the example of EMC’s enterprise records management platform based on Documentum and SourceOne offerings.

Expanding Dimensions of Enterprise Records Management

The conduct of business has always demanded record-keeping. But few companies anticipated the simultaneous rapid expansion in the definition of an electronic record, the scope of the implied functional requirements, and the cost of non-compliance.

What is a Record?

The official definition of a record used by the American Records Management Association (ARMA) is:

A record is information created, received, and maintained by an organization or person that is evidence of its activities or operations, and has value requiring its retention for a specific period of time. It can be used in pursuance of legal and regulatory obligations.

Many statutes and regulations require that such records be identified, classified, and securely retained for a specified period of time, but each defines the information it considers a record in its own way. Regulatory definitions of records may refer to “communications with customers” in any form, including email or text messaging, historically managed completely outside the corporate records umbrella. Moreover, regulators are by no means the only source of record-keeping requirements. Information required to support audit or defend against civil litigation often imposes an even larger records management burden.

In this report, the term “record” is used to main information, in any format, intentionally stored and maintained as evidence of the organization’s activities or operations. Other forms of electronically stored information (ESI) may also provide such evidence but may not be intentionally maintained as records. An important aspect of any ERM strategy should be to minimize the volume of such ESI evidence left “in the wild” – on user desktops and network fileshares, for example – outside the bounds of ERM, while retaining the ability to recapture it when necessary.

To understand the scope of this new business challenge, one only has to look at the specific requirements individually, since the technical solution for one may not apply to the others.

Corporate Governance: Sarbanes-Oxley 404

The Sarbanes-Oxley Act of 2002 today affects every publicly traded company. Among other things, it imposes stringent requirements for maintaining records related to financial controls, and it holds executive officers and audit committee members accountable for enforcement of
compliance policies, including records retention. Everything must be documented in a way that can be reviewed by auditors, including policies and procedures, approvals, authorizations, verifications, recommendations, and performance reviews, in addition to financial data.

SEC Rule 17a and Related Regulations
Section 17a of the Securities and Exchange Act of 1934 applies to securities brokers, dealers, investment companies, financial advisers, and transfer agents with respect to electronic interoffice communications and communications with customers. Specified categories of documents and correspondence must be preserved and retained, regardless of data type, with retention periods dependent on the organization and the type of information. For example, all broker correspondence relating to stock trades must be retained for six years; any correspondence related to a firm’s larger business must be retained for three years. Electronic messages must be preserved in a non-rewritable non-erasable storage medium for the required retention period. Records must be indexed and searchable via queries using a standard user interface accessible to the SEC and NASD upon request, supporting timely retrieval of records from the storage media by an independent third party. The regulators’ intention to get tough was signaled by a penalty of censure and fines of $1.65 Million apiece against five of the largest investment banks for failure to preserve these electronic communications as well as failure to maintain and enforce a supervisory system to assure compliance with the records retention regulations.

Privacy Legislation – HIPAA, Gramm-Leach-Bliley, and the EU Data Protection Directive
Other US legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley (GLB) has added records management requirements focused on privacy. HIPAA privacy rules deal with controlling access to personal health information. GLB privacy rules deal with controlling access to personal financial information. In both cases, information must be categorized for access control and an audit trail must be able to the access history of the covered personal information. In Europe, the EU Data Protection Directive and its relevant implementations in member states, particularly the UK’s Data Protection Act 1998, have even more stringent requirements regarding personal information of employees, customers and prospects. Penalties for non-compliance are severe and accrue personally to the directors of the infringing company.

Civil Litigation and eDiscovery
For many organizations, the biggest risk related to electronic records retention comes not from regulators but from the threat of civil litigation, specifically the cost of document discovery, in particular when the evidence sought is in the form of email. Rule 26 of the Federal Rules of Civil Procedure states that each party involved in litigation must proactively provide a description of all records relevant to the disputed facts without waiting for discovery requests, typically within three months. Rule 34 states that either party may request access to any record covered by Rule 26 to view or make copies, and unless there is a specific objection, the other party must provide it in a reasonable time. Civil litigation discovery and disclosure provisions in most major European jurisdictions are similar.

Managing the Risk of Email
Email presents a special risk, since messages are typically not managed as company records. But numerous well-publicized examples have brought home to CEOs the huge problem of unmanaged
email for defendants in antitrust, product liability, and shareholder lawsuits, both in the cost of compliance with a discovery request, and the cost of non-compliance.

1. Cost of Compliance

Corporate email systems were never designed with records retention in mind. Even though mail systems are routinely backed up, you cannot search for or retrieve individual messages directly from backup media, but must restore the entire mail system first from the backup tape — a laborious undertaking that can cost thousands of dollars for each backup restored.

For example, in 2002, the case Murphy Oil v Fluor Daniel required expenditure of $6.2M to restore and print email from 93 backup tapes. In the same year, Rowe Entertainment v William Morris Agency reported a cost of $9.75M to restore email from 200 tapes, plus hundreds of thousands more to retrieve and review a quarter of a million email messages.

2. Cost of Non-Compliance

Failure to fully comply with a discovery request can create an even bigger problem, a “spoliation instruction” to the jury, which suggests intentional destruction of evidence even if there was no such intention, and greatly increases the risk of losing the case. For example, in Zubulake v UBS Warburg (2005), an adverse jury instruction sanction was imposed on UBS Warburg due to their willful destruction of potentially relevant email messages, instructing jurors to presume the email destroyed was damaging to the defendant’s case. The resulting $29 Million verdict included $20 Million in punitive damages. Also in Zubulake, the court ruled that if a party cannot comply with Rule 26 and 34 discovery, the court may grant the other party direct access to the company’s email system. Even in cases where the court supervises the search, sensitive information may be compromised. In US v Philip Morris (2005), defendant’s failure to comply with its “print and retain” policy for email resulted in a $2.75 Million sanction and exclusion of testimony. Failure to comply with discovery requests risks far more than the cost of compliance!

A New Challenge: Changes in eDiscovery

Amendments in late 2006 intended to resolve loopholes and ambiguities of these “eDiscovery” rules today have extended their scope to cover all electronically stored information, not just documents. One provision, referred to as “Meet and Confer,” requires the litigating parties to meet within 120 days of filing to discuss eDiscovery issues, in particular to prevent disposal of relevant electronically stored information (ESI) and ensure timely production. That means both parties must be prepared to agree on all relevant repositories and classes of information, formats for production, and what information is confidential, or “privileged.” They must be able to identify, for example, not only all relevant email servers and backup tapes, but also deleted data and data in remote or third party locations.

The only way to comply with this provision cost-effectively is through a comprehensive program of eDiscovery information collection and management. Ideally, in such a program all ESI that could be discoverable in litigation would be captured at its source, using explicit policies and procedures, retained as a single centrally stored copy rather than left unmanaged in individual users’ files and email accounts. In practice, however, some ESI will always remain “in the wild,” scattered throughout the enterprise. Thus a practical approach to eDiscovery combines proactive collection and management of likely eDiscovery targets, such as certain email accounts, in a central archive, with automated tools that can sweep potentially relevant information from sources distributed across the enterprise, including user desktops and fileshares.

For ESI in the archived portion, eDiscovery can be automated using rules, with savings potentially measured in millions of dollars. Moreover, if the eDiscovery system is designed to easily identify
potentially privileged (confidential) information, it can be more efficiently and effectively excluded from production.

Because the Meet and Confer rule is specifically intended to prevent inadvertent destruction of discoverable information, it creates an obligation to preserve that information from normal aging and disposition, what is termed a legal hold on the information objects in question. If the inability to apply such a hold quickly results in destruction of key information, an organization risks a charge of spoliation of evidence. Agreement on what must be preserved and what can be disposed of using standard retention policies can save money and protect against a later spoliation claim.

The new rules also deal with the inadvertent production of privileged information, allowing the producer to claim privilege after the fact and attempt to retract the information after discovery. If the producer has not made reasonable attempts to avoid disclosure of privileged information, the court may consider that a waiver of privilege. Because of the vast quantities of information involved, without a proactive eDiscovery solution in place, the producer may not be able to enforce after-the-fact claims of privilege.

Finally, the new rules provide companies a safe harbor in event of destruction of potentially discoverable information if that destruction was performed normally according to established retention policies. Again, this rule benefits companies who have implemented eDiscovery within a broad enterprise framework with explicit retention policies.

The ERM Challenge

The preceding discussion underscores the scope of the enterprise records management challenge. In addition to formal documents historically understood as records, organizations must be prepared to retain, index, and produce on demand an ever-larger set of information in non-traditional record formats email, text messages, and informal office documents.

A comprehensive, policy-based program of record retention, supported by technology that properly classifies and archives all records, can significantly reduce the cost of regulatory compliance and ad hoc discovery while keeping investigators and litigators from combing through user files at will. In addition to enforcing retention of records, the ERM program must deal with record disposition at the end of the retention period. With the exponential growth of content created, consistent policy-based approach to enforcing both retention and disposition helps organizations reduce storage and management costs while adhering to legal and corporate policy obligations. Managing disposition can reduce the potential risk posed by non-records or expired records with respect to audits and discovery requests down the road – risks that have proven extremely costly for some companies.

It is important to note that the primary requirement is to retain the information in unaltered form and be able to quickly find and produce it on demand. The regulations and eDiscovery rules typically do not require, however, the kind of formal records management elements and procedures provided by a DoD 5015.2-compliant Records Management Application. In reality, most organizations must deal with a diversity of records management requirements, each applicable to a particular information set. The rules defining what constitutes a record, how those records must be classified and named in the record repository, and whether that classification is overt (formal) or implicit (informal), vary widely across the enterprise, depending on the type of record and the business requirements. Technology designed for a dedicated records administrator may add burdensome complexity to ordinary office workers and managers.
ERM and Information Governance

A practical approach to enterprise records management protects the organization implementing it both by lowering the risks of non-compliance and by lowering the cost of producing records quickly on demand. It should be viewed as part of the organization’s broader information governance strategy. Good information governance means:

- The ability to find all content related to a particular matter quickly on demand, with confidence that it’s where it is supposed to be, unaltered from its original form, and that there are no other copies.
- Compliance with government and industry regulations and with company policies and best practices.
- Effective management of the growth of information storage and minimization of information duplication across the enterprise.

Good information governance reduces both the business risk in the event of audit, investigation, or litigation, and lowers the normal cost of everyday operations. ERM technology plays a key role in information governance by automating the capture of content underneath the governance umbrella and lowering the cost of maintaining it, ensuring its retention for the appropriate period and managing its subsequent disposition.

ERM Requirements

With the diversity of enterprise records management requirements in mind, let’s look at what a practical ERM approach needs to deliver.

1. Automatic Retention

Retention is the essential requirement governing most records management needs in the enterprise. It means that documents are preserved, without the possibility of revision or deletion, for a specified period of time. In many cases, the decision to retain a document should not require overt action by the author, but should be applied automatically to an entire class of documents, such as all documents in a specified set of folders. Once a retention policy has been established and applied to a folder by an authorized records administrator, any document in the folder automatically inherits the policy. Automated retention management is invisible to most users; the policy is applied automatically when a document is stored, without prompting for additional metadata. In addition, a practical approach to records management must be able to override the retention policy and apply special “holds” when a document must be preserved beyond the normal retention period, such as for a pending investigation or legal action.

2. Formal Records Management

Beyond retention, a subset of the organization’s records may require management as formal records. The centerpiece of formal records management is the file plan, a permanent, system-wide classification schema for records, defining record naming, organization, and descriptive metadata, specified and managed by a records administrator. A document is overtly declared as a record by storing it in a location managed by the file plan, and classified using metadata specified by the file plan. Retention is defined by the classification. Standards like DoD 5015.2, MoReq, VERS, the Commonwealth Standard, and others used around the globe to certify records management applications implementing these procedures, are actually only needed for formal records.
3. Integrated Management Infrastructure

Across the enterprise, records come in all types and formats, from documents to emails and text messages, to websites. In the past, simply managing each content type required its own dedicated repository, and managing it as a record required yet another. While enterprise content management vendors have unified lifecycle management services across content types, many have kept records management separate. Having to copy or move content from the ECM repository to an electronic records repository means supporting redundant infrastructure for storage, access control, metadata management, user interface, and a host of other features. A better way is to apply records management in place and leverage an existing ECM infrastructure.

The increased attention to compliance and risk management is now raising the bar even higher. Management of physical records – paper, microfilm, and digital media – needs to be seamlessly integrated under the ERM umbrella as well. Moreover, it should not be necessary to copy or move documents from filesystems, online collaboration environments, or report management systems in order to apply records management policies to them. Ideally, ERM should support a federated architecture, in which records management policies can be maintained centrally but applied to content in disparate stores across the enterprise.

Email presents a special management challenge, as the architecture of ECM repositories is not an ideal match for email’s high daily volumes. A practical ERM approach incorporates dedicated archives designed for email’s volume characteristics and applies classification and retention policies to that archive.

4. Modular Business-Driven Implementation

Many early adopters of enterprise records management focused on DoD 5015 compliance as the benchmark for software functionality. In large part that is because there is no standard for simple retention management, which is the largest component of the business need across the enterprise. A practical approach to enterprise records management complements unified end-to-end infrastructure with modular deployment, so that parts of the organization that only need retention policy management can implement that, while other parts can implement formal records management as needed, up to full DoD 5015.2-compliant procedures. A modular framework gives organizations the freedom to implement records management in a flexible manner, tailored to its specific requirements and budget. It can start with basic retention and evolve toward formal records management over time, or implement a total records management solution from the start. Modularity allows each department to implement just the functionality it needs, and has the resources to support.

How Companies Fool Themselves

Companies routinely delegate the ERM problem to IT, but most IT managers do not fully understand the business requirements. They may believe that their existing archiving solution, often designed for some other purpose, is adequate to meet the records management need. In most cases this is a mistake. Some of these archives can play a role in a comprehensive ERM strategy, while others should play no role whatsoever. Let’s look at some familiar examples.

Backup and Business Continuity Archives

In the wake of 9/11, many companies discovered that while critical financial data was backed up offsite and quickly restored, their contracts, customer files, and other documents vital to ongoing operations were lost. As a result, electronic copies of documents began to be stored offsite as part of a corporate business continuity program. Similarly, most companies regularly back up their
email systems, essentially for the same purpose – restoration of operations after a simple system crash or a facility-wide disaster.

Neither backup systems nor business continuity archives meet the requirements of ERM. They provide no classification, no retention period, no audit trail, no access control, no distinction between records and non-records. Unclear “ownership” for authorizing tape destruction leads to their permanent retention, while multiple uncontrolled backup copies make it hard to actually expunge expired records.

Most important, individual documents in backup systems are not typically searchable and retrievable in a timely fashion or cost-effectively. These systems are designed to restore thousands of documents or messages at once, not just a few selected ones. Nevertheless, many companies still must resort to restoring backup tapes in response to Legal or HR requests.

The cost of finding and retrieving selected emails from backup tapes can run into the millions of dollars, as proven time and again in document discovery cases. Moreover when production in this manner is not timely, a spoliation charge may result. In Zubulake V (2004), the court concluded that the defendant failed to preserve discoverable email and engaged in willful spoliation when employees deleted relevant email from their computers despite being instructed by in-house and outside counsel not to do so. While some emails were recovered, an indeterminate number could not be recovered due to the recycling of storage media. The court emphasized that even for emails that were recovered, production did not occur until long past the response date for discovery requests.

Backup and business continuity systems should not be considered part of an ERM solution.

**Document Management Systems**

Electronic document management provides a technology framework for classification, search, quick retrieval, and access control. It also provides mass storage, including non-rewritable media, and workflow that can automate procedures whenever a document is added or accessed in the repository. However, unless the document management system provides the ability to define and enforce retention policies, it should not be considered an ERM solution.

Document management systems offering retention management can play an important role in ERM. Those like EMC Documentum in which retention management is “transparent” – applied to documents in place, rather than copying them to a separate repository, are ideal.

**Email Archives**

Many of the informal records involved in eDiscovery revolve around email. Active email is usually managed as a standalone system, not part of a document management or ECM repository. First-generation email archives were designed to overcome message store capacity and performance issues with corporate email systems such as Microsoft Exchange. They did not prevent alteration of email content or ensure retention. Even those with automated policies for selecting messages moved to the archive allowed users to override the policy, creating a “lightning rod for review” by regulators and litigators.

Second-generation email archives like EMC SourceOne have added retention management and eDiscovery capabilities, and play an important role in a comprehensive ERM strategy. They support automated capture of large daily email volumes, ensured retention and legal holds.
Certified Records Management Applications

Besides putting themselves at risk by not going far enough, companies can also make the mistake of going too far, subjecting even informal records — where the business need is simply retention management — to the stringent requirements of formal records management applications. Formal records management standards specify functional requirements concerning the file plan, declaration, classification, and retention features of records management software. For example, unlike SEC Rule 17a or Sarbanes-Oxley, DoD 5015.2 does not mandate a set of business practices, but simply defines a set of technical requirements necessary for purchase by an agency of the US Defense Department. In the absence of comparable standards for general use in the private sector, DoD 5015.2 compliance has been adopted as an RFP requirement by numerous commercial purchasers of records management software.

While well intentioned, this trend is counterproductive. DoD 5015.2 is valuable for formal records, but for most record-keeping needs in the enterprise it is overkill, since it requires formal policies and trained records management professionals to correctly classify records in the file plan. In reality, such policies rarely address the retention of informal records, and companies do not employ the armies of highly trained records administrators required. Applying formal records management standards to simple retention invariably leads to user resistance. The file plan requires certain index fields or metadata to be provided whenever a document is stored as a record. That means extra work for users, who will look for ways to get around the software. What works for contracts and other formal records is rarely, for example, a good solution for routine office documents.

Technology Support for ERM

With the above examples in mind, the technology underpinning a practical ERM strategy requires several basic characteristics:

Comprehensive

First, it needs to be comprehensive, providing a common framework for managing records based on all types of content, from revisable documents to scanned images to email and text messaging to reports and statements to websites, even online “team rooms” set up for ad hoc collaboration. And we shouldn’t forget physical records either, such as paper files and microfilm. A common framework implies, for example, that the rules specifying record retention, security, or other records management properties should apply regardless of the type or location of the content. The scope of management also should be comprehensive, from basic retention management to formal records management certified to meet standards like DoD 5015.2 or MoREQ.

The unique characteristics of each type of content are often reflected in special type-specific management applications — for example, document management, image capture, web content management, and digital asset management — but records management that does not cut across content types is not cost-effective, and it cannot be relied on to track all the records required even for a single segment of the business. Trying to manage records comprehensively through a collection of point solutions means replicating the policies and rules, metadata, access control, and other management features in each records repository, and keep them all in sync on an ongoing basis. Comprehensive really implies looking at enterprise records management as an IT infrastructure issue, not simply another application.
Pervasive and Invisible

Second, it needs to be pervasive across an enterprise, touching content authors and business managers, not just records administrators. But to reach ordinary users across the enterprise, ERM needs to meet users where they already live. A formal records management application is fine for the professional records administrator, but making it the universal front end for ERM means user resistance and, ultimately, failure to capture and retain important documents. Instead, users need to be able to access records – store them, retrieve them, and when necessary declare and classify them – from the same places they interact with and manage ordinary content: from their ECM client, often via an enterprise information portal, or from Microsoft Office applications.

Pervasive records management implies invisibility. Records management policies need to be expressed in rules applied automatically, without asking users to formally declare each content item a record. For example, policies could be attached to specific folders in the ECM repository, so that any content object added to those folders inherits the policy automatically. A user trying to delete such an object might be refused, but in most cases retention of the record is invisible to end users.

Unified With ECM

One of the great advances made by enterprise content management has been creating a unified management infrastructure for disparate content types and overlaying that infrastructure with management applications and workflows specific to each type of content. For example, specialized applications are available for technical publishing and invoice processing, but these both can be managed within an ECM system.

Some records management applications, however, still require copying content from the ECM repository to a separate records repository to assure retention. That makes no sense, since a new redundant infrastructure needs to be created for security, storage management, access control, search, and the rest. A more practical approach to enterprise records management would incorporate record attributes, such as retention period and DoD 5015.2-required metadata, as part of the ECM system itself. Then content can be managed as records “in place,” without moving or copying to a special, and additional, repository.

Modular

Finally, the software needs to acknowledge the reality that the business requirements for records management across the enterprise are diverse, and a one-size-fits-all records management application is not the answer. For departments needing only invisible policy-based retention management, the learning curve and extra work imposed by formal records management will make user acceptance difficult, while departments charged with formal records management may need full functionality in order to comply with corporate and legal regulations.

Enterprise records management software therefore must be flexible, exposing its basic functions as independent modules that can be selected for implementation as dictated by the business need, and allowing a phased approach to records management rather than an all-at-once, all-or-nothing deployment.

Example: EMC Documentum

A good example of such a practical approach is EMC Documentum Records Manager, which is deeply integrated with the Documentum enterprise content platform and applications, designed with a modular architecture capable of meeting a wide variety of diverse records management
needs across the enterprise. Documentum Records Manager is not a separate environment integrated with ECM, but a layer of functionality that sits on top of Documentum Content Server and the core ECM architecture. It uses the same database, look and feel, user roles and groups, security model, development tools and APIs as the Documentum repository and ECM applications. It is accessible from the standard Documentum Webtop client environment, from Microsoft Office or SharePoint, or from any custom client built on the Documentum API. In addition, Documentum provides special Records Management Administrator and Coordinator clients that support administrative functions. Records Manager extends Documentum’s industry-leading ECM platform capabilities with records management features such as corporate file plans, retention policies, file- and field-level security.

Policy-Based

The modular architecture of Documentum Records Manager does not impose a one-size-fits-all records management approach across the enterprise. Instead, it defines four distinct types of policies that can be applied to documents and folders in the Documentum repository as needed, to support as much or as little records management functionality as required by each part of the organization. Records management functionality can be customized to specific business needs rather than remain locked into an all-or-nothing application.

The Documentum platform supports four types of records management policies:

- **Retention policy.** A retention policy determines the length of time a document, folder, or cabinet is retained, based on operational, legal, regulatory, fiscal or internal requirements. For the duration of its applied retention policy, the managed object cannot be deleted, nor can it be revised in any way, although a new version of the object may be checked in.

- **Security policy.** A security policy further restricts the access control defined by the normal Documentum security model, and prevents the ownership of the managed object from being altered and prohibits manipulation of its access control list. In addition to the normal security policy (e.g., inherited from a parent folder), additional security markings can be selectively applied to further restrict access to users with special permissions.

- **Containment policy.** A containment policy defines a consistent structure for the file plan: what content can be contained at each level in the hierarchy, how many folder levels are allowed, and how many links between a record and other content objects are permitted.

- **Naming policy.** A naming policy defines consistent naming rules for folders in the file plan, including naming conventions, separators, and level delimiters.
Core Records Services

Documentum Retention Policy Services (RPS) supports “zero-click” creation, management and application of retention policies. It can be deployed standalone to provide lightweight records management, or can be one of many components in a records management solution that supports formal records management with features such as file plan maintenance and configuration (Figure 1). By itself, it provides all the functionality required for informal records management. It works invisibly behind the scenes, binding retention policies to selected folders in a Documentum repository. Any document stored in those folders inherits the policy automatically, with no user intervention. Users are not prompted for additional metadata; Retention Policy Services simply uses the existing ECM metadata. It also supports a variety of retention markups (Holds, Review, Permanent and Freeze), which can be applied to any content under retention to override disposition at the end of the normal retention period.

Documentum Records Manager (RM) supports the creation, management, and application of security, containment, and naming policies, as well as a DoD 5015.2-certified records management application for file plan creation and maintenance, formal records declaration, and general records administration. Each policy is deployed only when and where needed. This modular approach is the only practical, cost-effective way to apply records management at the enterprise level, and supports incremental evolution from simple to more elaborate records management over time.

Documentum Office and SharePoint Integration expands records management beyond users of the Documentum Webtop. Users have a variety of alternatives linking Documentum ERM with Microsoft Office and SharePoint. Retention management is available directly from Office applications like Microsoft Word. Context menus in Office not only can file documents in Documentum folders, applying access controls and digital signatures, but can apply retention policies as well. In addition, My Documentum for Outlook combines the interface of Microsoft Outlook with full access to the Documentum repository, including ERM-managed objects.
As Microsoft SharePoint rapidly proliferates as a document collaboration environment, its content must be increasingly retained for compliance or managed as formal records. The EMC Documentum platform offers several options. For retention management, *EMC Documentum Repository Services for Microsoft SharePoint* can re-route SharePoint content to a Documentum repository, where they can be retained, transparently to the end-user, under retention policies via RPS. Another option, *My Documentum for Microsoft SharePoint*, effectively embeds Documentum client capabilities within the SharePoint portal environment through a collection of Web Parts, or portlets.

EMC Documentum core ERM services thus provide a comprehensive platform supporting all record types, electronic or physical, adaptable to the wide variety of records management needs across the enterprise, with a common user interface for browsing, searching, viewing, or declaring records of any type.

**Supporting ERM Infrastructure**

Underpinning the ERM platform, *Documentum Content Server* provides an enterprise-class platform that supports high-availability configurations with clustering and failover, scalability proven in its “billion-object benchmark,” and localization in French, Italian, German, Spanish, Japanese, and Korean.
single set of policies. Many companies have multiple ECM systems, plus unmanaged content in filesystems, databases, websites, collaboration environments like SharePoint, as well as legacy systems. While many such content stores can delegate authority over access control and update rights to a centralized records management application, they usually cannot prevent administrators from accidentally overriding that control by going through the store’s native administration console. To overcome this risk inherent in federated records management, Documentum provides a patented assurance engine that uses statistical sampling techniques to systematically compare records with the federated content they point to, generating alerts on any missing or altered records detected, along with a verifiable audit trail. The comparison and sampling rules are tunable to each remote system, or even folders within each system, to match the business and technical risks of each.

Archiving and eDiscovery

EMC SourceOne is a family of products and solutions for integrated content archiving and support for eDiscovery across content types. It supports proactive information management to improve operational efficiencies of production systems; enables good information governance and litigation readiness; and reduces time, cost, and risk by creating repeatable eDiscovery processes.

EMC SourceOne Email Management provides high-volume email archiving capabilities for Microsoft Exchange, IBM Lotus Notes/Domino and instant messaging. SourceOne Email Management helps customers improve IT efficiency and reduce costs of the messaging environment, enables litigation readiness and consistently enforces retention and disposition policies to meet regulatory and/or corporate governance requirements. Optional capabilities provide high-volume search of the email archive based on metadata, consolidating the result set into a hold folder where content is full text indexed.

EMC SourceOne eDiscovery - Kazeon automates the identification, collection, preservation, processing, analysis and review of electronically stored information (ESI) that resides “in the wild” – that is, outside the ERM umbrella, on user desktops, network file shares, archives and content repositories. Using the index, investigators tag certain items for legal hold, upon which that ESI is secured and retained in a secure EMC repository or archive. Through extensive data and metadata protection and checks and a forensically sound eDiscovery process, chain of custody is maintained throughout the entire eDiscovery workflow, and information is protected against spoliation. Extensive yet low-overhead analysis and review enable quick Early Case Assessments, thereby greatly reducing cost and risk.

Structured Data

Archive Services for Reports (ASR) provides compliance-oriented archiving of structured data such as host reports and relational database records. ASR can import both page-oriented data like statements and invoices and line-oriented data like audit logs into EMC Documentum, where they can be managed as enterprise records. Third party extract, transform, and load (ETL) tool can be used to transform live relational databases into PDF or XML content that is then imported to EMC Documentum using ASR, as well.

Renditions

Content Transformation Services (CTS) automates the creation of renditions and other transformations of a content object. A rendition is an alternate format for a source document. For example, CTS can automatically create an HTML or PDF rendition from a Microsoft Word document. Transformations create related objects from a source object, based on specified rules. Software capable of reading original source formats may not be available many years later, and
good records management practice emphasizes retention of specific archival rendition formats, such as PDF-A, MPEG-2, and TIFF. In RPS, renditions are linked to the source document, and the retention policy can specify disposition of renditions differently than that of the source record.

BPM and Workflow

**Documentum xCelerated Composition Platform (xCP)** is a unified framework for rapid design and deployment of case management solutions, combining content and records management, business process management, intelligent capture of paper and electronic data, team collaboration, and generation of customer communications. The platform provides pre-built case management artifacts and automates the entire compliance lifecycle. Emphasizing configuration rather than code, developers and IT architects are able to avoid complexity, cost, and project risk, cutting the development cycle by as much as 50 percent.

**Documentum Process Services**, a component of xCP, provides advanced workflow services tightly linked to content in the Documentum repository, with the ability to directly integrate with backend applications and databases. Users can create custom workflows that automate many aspects of the records management process.

Security and Rights Management

**Trusted Content Services (TCS)** extends the security features of the standard Documentum platform with a special layer of capabilities that achieve Common Criteria certification required by the US Department of Defense and other security-sensitive customers, including mandatory access control, repository encryption, and digital shredding. Digital shredding, a disposition option for RPS, ensures that information cannot be retrieved, even with forensic techniques that analyze residual magnetism on the storage media.

**Information Rights Management Services (IRM)** locks access rights directly to source documents, so they can be freely distributed with assurance that only authorized rights-holders can view or edit. IRM works in concert with RPS to enforce retention and disposition. With IRM, all copies of a document can be set to expire at a certain date, even if outside of the repository. Also, all access to the document is tracked in an audit trail on the IRM server.

Classification and Search

**Content Intelligence Services (CIS)** define hierarchical classification schemes called taxonomies, defining categories that can be used to organize the repository according to established rules. CIS can also autoclassify documents into categories.

**Federated Search Services** supports queries spanning diverse information sources ranging from enterprise applications, databases, content management systems, and groupware to web search engines, industry-specific databases, local archives, government portals, and syndicated content providers. An adapter framework includes hundreds of prepackaged adapters for various content sources, including LexisNexis, Factiva, Dialog, Hoover’s, and PubMed.

Storage

**Content Storage Services** provides policy-based migration of content from rapid-access storage devices to lower-cost but slower devices and media over time, implementing a cost-effective information lifecycle management (ILM) strategy. CSS can be leveraged in an enterprise records management strategy to reduce the long-term storage costs associated with huge retention volumes.
EMC Centera is a special magnetic disk storage device that provides “write-once” functionality, equivalent to less cost-effective optical storage devices, as required by certain regulations such as SEC Rule 17a for broker-customer communications. When used with Records Manager, Centera has been DoD 5015.2 certified.

The Bottom Line

With tightened regulation of corporate governance, privacy, and customer communications, combined with new eDiscovery rules, enterprise records management now has CEO attention. Records management procedures must be established and enforced by corporate policy, and supported in detail by ERM technology. Records are defined by content and purpose, not data type, so even informal communications like email and instant messaging fall within the bounds of compliance.

This makes the challenge of appropriate ERM technology more complex than many executives realize. Point solutions optimized for management of active content, such as a document management system or an email archive, is insufficient if it does not support enforced retention or eDiscovery. At the same time, DoD 5015.2-compliant records management applications, appropriate for formal records, are counterproductive for the majority of informal records across the enterprise, which lack the support of dedicated records administrators.

Effective ERM technology must span both content type boundaries and the vast range of business requirements for informal and formal records. It must be comprehensive and pervasive, yet flexible in its implementation. For some users it must be invisible, with policies applied automatically based on business rules, while for others it must allow fine-grained control over record declaration, classification, and file plan design, including record containment, naming, and security.

It’s a difficult combination, but EMC has put together such an offering in Documentum Records Manager. Modularity allows flexible deployment for varying needs across the organization. Records are managed in place, federated across disparate content stores, continuously auditable using a patented assurance engine. ERM leverages existing metadata and user familiarity with the Documentum environment, and extends access to the broad and growing base of Microsoft Office and SharePoint users.

To that, EMC adds comprehensive supporting services, including email retention and eDiscovery, content lifecycle management, BPM and case management, intelligent document capture, and world-class storage solutions. Thus the Documentum ERM suite enjoys the enterprise-class scalability and complementary services of proven EMC infrastructure. If you’re looking to solve your records management problem at the enterprise level, EMC Documentum Records Manager offers a practical approach.

Bruce Silver

October 2009