



UNIFYING MANAGEMENT OF PHYSICAL AND ELECTRONIC RECORDS

The Records Management Imperative

In the past few years, executives have come to understand that maintaining and preserving company records is serious business. The pressure is coming from two directions. On one hand, compliance with regulatory mandates requires a strict program of comprehensive record keeping. In the US, Sarbanes-Oxley 404, Federal Rules of Civil Procedure (FRCP) Rule 26, the Health Insurance Portability and Accountability Act (HIPAA), SEC Rule 17a, NASD 3010 and 3110, and countless other regulations today not only formalize broad new record-keeping requirements, but stiffen penalties for non-compliance. On the other hand, records management plays an ever-increasing role in any company's risk management strategy, particularly with regard to civil litigation. The ability or inability to produce records quickly and efficiently in response to a discovery request can sway legal judgments (plus associated market consequences) measured in billions of dollars. In addition to managing risks in litigation, a comprehensive program of records management is vital to lowering the risk and cost of routine audits, protecting valuable intellectual property rights, and ensuring business continuity in the wake of natural disaster or terrorist attack.

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 well-documented and enforced business policies, and a reliable audit trail of all record-keeping activities. In addition, it means the ability to store an exponentially growing volume of records securely and cost-effectively, and find and retrieve records quickly and easily.

To complicate matters, the scope of what constitutes a record is continually growing larger. No longer confined to folders and microfilm in the company records room, most records today are electronic – word processing documents, database reports, PowerPoint presentations, emails, and faxes – and distributed throughout the enterprise. Now, even blogs and instant messages are considered records subject to regulatory compliance.

The amended Federal Rules of Civil Procedure, adopted at the end of 2006, go even further: Changes to Rule 26 and Rule 34 define electronically stored information (ESI) as a specific category of information to be disclosed in litigation discovery, removing the prior ambiguity over whether or not business data constitutes a “document”. The FRCP's new eDiscovery rules substantially broaden the universe of discoverable information to include such things as digitized voice mail, surveillance tapes, and text messages.

Point Solutions No Longer An Option

Over the years, records managers and IT departments have responded to the record-keeping challenge by implementing a hodgepodge of point solutions, each adapted to archiving, and occasionally preserving, a particular type of information. In the electronic records domain, the past several years have seen a diverse assortment of document imaging systems, enterprise content management systems, email archive systems, and data backup systems pressed into service as records management solutions. Each of these repositories typically is dedicated to one particular data type or format, and may not even offer such essential records management functions as policy-based classification and retention.

This point solution approach to records management is a problem because both the compliance mandates and litigation discovery requests are seldom restricted to a single record type or format, but are defined by the information content regardless of data type. Without a unified approach that provides a common classification taxonomy, metadata (search criteria), or retention policy framework, it's a certainty that some records will fall through the cracks. The incomplete and patchwork nature of these point solutions thus offers business executives a false sense of security where records management is concerned.

An "enterprise" approach to electronic records management addresses these shortcomings. EMC Documentum Records Manager, for example, offers a comprehensive solution that can secure and retain electronic records of any type – documents, email, scanned images, text messages, or any form of electronically stored information – to provide a unified enterprise records management platform that addresses the requirements of both regulatory compliance and risk reduction.

But not all records are electronic. We should not forget that physical records – paper, microfilm, and digital media – still exist in astounding volumes, and remain outside the new enterprise records management umbrella. Thus, a complete strategy for enterprise records management should ideally provide a unified framework encompassing both physical and electronic records, despite the obvious differences in the physical storage and tracking of these two types.

Now there is a way to do that. Software from OmniRIM Solutions, the leading provider of software for physical records management, can be integrated with EMC Documentum Records Manager, the leader in enterprise records management, to create a unified platform for managing *all* records across the enterprise. That means a single set of retention policies, classification metadata, and disposition policies can be applied to both electronic and physical records, and a single query can find and retrieve both electronic and physical records.

This white paper explains the features and benefits of such a unified approach to enterprise records management, and describes how the EMC Documentum/OmniRIM solution works.

What Is Enterprise Records Management?

Enterprise records management refers to a consistent set of records management policies – and an associated technology platform capable of enforcing and managing those policies – that can be applied to the complete range of records management requirements across the enterprise. Some of those requirements stem from the business itself – litigation discovery, intellectual property protection, business continuity, or general business governance – while others are required for compliance with a growing body of laws and regulations, such as:

- **Sarbanes-Oxley 404.** Every US public company must document and test all internal controls over reported financial information, including policies and procedures, approvals, authorizations, verifications, recommendations, and performance reviews, and must preserve that information for years.
- **SEC Rule 17a and Related Exchange Regulations.** Securities brokers, dealers, investment companies, financial advisers, and transfer agents must retain records of all electronic interoffice communications and communications with customers, including email and text messaging, with retention periods specified for each type. 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.

- **Privacy Legislation.** HIPAA privacy rules (personal health information), Gramm-Leach-Bliley privacy rules (personal financial information), and EU Data Protection Directive implementations all require information to be categorized so that the correct access control rules can be applied, with an audit trail detailing the access history.
- **FRCP Rules 26 and 34.** The Federal Rules of Civil Procedure (and similar provisions in Europe) require each party involved in litigation to be able to describe and produce all records relevant to the disputed facts within a reasonable time. Cases involving multi-million dollar costs to produce this information from backup tapes are well documented, as are punitive damages in the range of tens of millions of dollars resulting from not being able to produce this information. 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.

In all of these cases, the inability to produce certain records on demand can have a devastating business impact, measured both in money and company reputation. Nevertheless, many companies continue to ignore the dangers of inadequate records management, taking their chances on technologies designed for other purposes, such as backup tapes, email archives, and ECM repositories – often with disastrous results.

Historically, most companies have deployed records management piecemeal, focused on one specific compliance requirement affecting a specific type of content – email, for example, or electronic documents, or scanned images. The problem is that each regulatory mandate or business concern emphasizes a different set of record types, and may impose its own specific rules on retention, disposition, and other parameters of records management.

But as point solutions proliferate in the enterprise, applying retention, disposition, classification and other policies consistently across the enterprise inevitably becomes laborious and expensive. A true enterprise approach to records management should be able to apply a single set of policies and rules consistently across content types.

An enterprise approach also means accommodating the wide diversity of management policies implied by all of these initiatives. Some may require formal records management, consistent with standards such as DoD 5015.2 in the US or Europe’s similar Model Requirements for the Management of Electronic Records (MoREQ), supporting formal record declaration and classification by trained records administrators. Others simply require assured policy-based record retention and disposition, without administrator involvement.

Flexibility is a practical necessity, since providing skilled and trained records management professionals across the enterprise wherever record keeping is needed would be an impossible, and hopelessly expensive, task. Where the essential business requirement is simply retention, records management should be automatic based on policies and rules, without requiring the intervention of records management professionals. In fact, simple retention management usually covers most records management needs in the enterprise.

Different areas of the company should be able to deploy as much or as little records management as they require, dictated by their particular needs. Ideally, enterprise records management should support phased deployment of records management, allowing companies to gradually build the skills and management policies required over time, rather than make them a prerequisite to getting started.

That's the approach taken by EMC Documentum Records Manager v5.3 and Retention Policy Services, which apply this enterprise approach to electronic records. Now the OmniRIM eConnector for EMC Documentum extends that flexible management umbrella to include paper, micrographics, and other physical records. Before going into how the unified solution works, let's take a closer look at what enterprise records management solution entails, and what that means for physical and electronic records.

Physical versus Electronic Records Management

Common Features

The basic features of records management apply equally to electronic records and physical records. They include the following.

Retention Policy

Retention policies are the cornerstone of records management. A retention policy applied to an information object ensures that it is retained, without alteration or deletion, for a period of time specified by the policy. The retention period is calculated with respect to some specified base date, such as the time of creation, record declaration, approval, etc. Retention is not arbitrarily assigned by a user, but represents an explicit business policy applied to all information objects of a particular class. For electronic records, a retention policy may be applied automatically simply by storing it in a particular folder in the record repository. In other cases, business rules may automatically capture and apply a retention policy to all objects meeting some set of criteria, such as all emails sent to or received from a customer.

Retention applies both to the document or information object itself and the database record that describes it. In some instances, the record's metadata may be updated, but never deleted. For physical records, a separate retention lifecycle may be applied to the original record and to copies of the original.

For both electronic and physical records, the retention policy frequently specifies the durations of each phase of a retention lifecycle, for example, Active, Semi-Active, and Disposition. As the record ages, it is eventually promoted to its next lifecycle phase. The physical storage location and ease of access may change between the Active phase and later phases of the lifecycle.

Disposition Policy

The last phase of the retention lifecycle, Disposition, represents the final state of the record. Whether the information object and/or its metadata are destroyed or retained permanently is determined by the Disposition policy. Disposition is a critical element of any organization's records management strategy. Disposing of records at the end of their required retention period reduces both the risks of future document discovery and routine costs of storage and administration.

Legal Holds and Retention Markings

Many statutes, regulations, and rules of civil procedure mandate that any records that might be required in an ongoing or impending legal matter, audit, or investigation must be retained even after their normal retention policy would qualify them for disposition. Records management implements this by the application of a *legal hold* or similar so-called "retention marking" to the records in question. Such a hold or marking overrides the

retention policy and prevents disposition. In the case of civil litigation, the ability to find and apply holds to all related records quickly is vital.

File Plan

The *file plan* refers to the carefully designed folder hierarchy in the records management repository. Typically the file plan is created and maintained by a records management professional, who specifies the levels of record cabinets and folders, what may be included at each level, required and optional metadata for each folder, and rules for naming new documents and folders. Since retention and other policies are typically assigned to folders in the file plan, placing a record in a particular folder in the file plan *classifies* it and applies those policies automatically to the record.

Metadata

The file plan defines a list of index fields, or metadata, for each cabinet, folder, and individual information object in the record repository. Some of these fields are mandatory, meaning the field must be completed in order for the record to be created. Others are optional. Users typically search for records based on metadata.

Security

The file plan also specifies security for each cabinet, folder, and information object in the record repository. An object's security policy specifies a hierarchy of permissions for access to the object. Security policies differentiate the allowed actions of groups of end users, compliance and legal officers, and records administrators. From lowest to highest, the ladder of permissions typically runs from viewing record metadata to viewing record content, modifying metadata, editing content, and deleting the record. Special permissions such as relocating the record in the file plan, changing permissions, modifying the retention lifecycle state, or changing record ownership are typically reserved for designated records administrators.

Electronic Records Example: FRCP eDiscovery Rules

To understand how these features are used in practice, consider the new eDiscovery provisions of the Federal Rules of Civil Procedure, which went into effect on December 1, 2006.

One new provision, referred to as "early meeting," 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 enterprise records management (ERM), in which all ESI which could be discoverable in litigation is captured by ERM at the source using explicit policies and procedures. That could mean automatically capturing as a record all emails sent to or from certain accounts, or any document stored in a particular set of folders, or daily reports routinely generated from some application or database. With a properly designed ERM

framework, record creation in this manner can be automated using rules, rather than manual declaration and classification by a records administrator.

If the policies, procedures, and rules clearly establish that the information in question is retained in the ERM repository, there is no need to try to find and produce information from backup tapes or other hard-to-access locations. The savings here can be measured in millions of dollars. Moreover, if ERM metadata is designed to easily identify potentially privileged (confidential) information, it can be more efficiently and effectively excluded from production.

The early meeting is intended to produce agreement between litigants as to what information is discoverable and not privileged. Because the early meeting rule is specifically intended to prevent inadvertent destruction of discoverable information, it creates an obligation to preserve that information from normal aging and disposition. ERM implements this protection efficiently by applying a legal hold to the information objects in question. The inability to apply such a hold quickly, if it results in destruction of information, risks a charge of spoliation of evidence. Conversely, agreement in the early meeting 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. The privilege claim can be disputed, and if the producer has not made reasonable attempts to avoid disclosure of privileged information, the court may consider that a waiver of privilege. Also, the claim must be made within a reasonable time. Because of the vast quantities of information involved in eDiscovery, without an ERM system in place that provides some idea of the information that has been produced, 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. Intended to address routine procedures like deleting old emails and recycling backup media, the safe harbor does not allow willful destruction of data outside of established and documented procedures, nor does it relieve companies of the need to apply legal holds to relevant information whenever litigation is “reasonably foreseeable.” Again, this rule benefits companies who have implemented ERM with explicit retention policies.

Managing Physical Records

The central ideas of enterprise records management – retention and disposition, the file plan, security, and metadata – apply equally to electronic and physical records. They are features of the record repository, or database, which is the heart of both physical and electronic records management systems. The essential difference between electronic and physical records is the storage and access to record content, the information objects themselves. Electronic record content is typically stored in an ECM system and delivered digitally over a network, while physical records are stored in warehouses and are delivered by physically retrieving and moving the files.

Given the huge difference in the cost of storage, access, and delivery, you might ask why even try to include physical records in a unified ERM strategy. But if you’re like most companies, the answer is obvious: You already have a huge volume of physical records – typically paper and micrographics, but possibly also tapes, optical disks and CDs, or other physical media – and it is subject to the same compliance and discovery requirements as

your electronic records. Much of this record volume is legacy data, created before electronic documents were common. But in fact you probably are still creating new physical records every day.

For example, what about paper correspondence from customers, suppliers, and other third parties? What about the lab notebooks kept by your research scientists? What about contracts and other agreements where establishing the authenticity of a “wet” signature may be critical to enforcing some right or obligation, or where important information is in handwritten annotations?

For many of these newly created paper records, the simplest answer may be to scan them into image documents and manage them as electronic records. But you can’t always do that. The paper may be too large to scan, or the information too faint to be captured adequately, or you may simply require the authentic original. Besides, scanning the huge entire backfile of legacy paper is often prohibitively expensive. And which record do you think will be easier to read 100 years from now: a Word 2000 file or a microfilm image of the document? Physical records will continue to be part of your company’s records management mandate for years to come.

Applications of Physical Records Management

There are thus good reasons why the need for physical records management continues in many industries:

- Government agencies need it to satisfy statutory and regulatory retention, reporting, and freedom of information requirements consistently across multiple offices and jurisdictions; to centralize control over storage, manipulation, and access to documents and confidential material; and to ensure the authenticity, integrity, and confidentiality of records from creation to delivery.
- Pharmaceutical and biotech companies need it to manage research lab notebooks and clinical files critical to establishing and enforcing intellectual property rights.
- Energy companies need it to manage engineering drawings, well files, and other hard-to-scan media, as well as huge volumes of legacy documents, with strict control over confidential information and consistency with regulatory requirements.
- Accounting/Legal firms need it to standardize control over multiple distributed offices, enforce policy-based retention and destruction, apply legal holds, and ensure auditable individual accountability for actions on records.
- Health care providers need it to manage and share active records, patient charts, X-ray jackets, lab notebooks, microfilm, and inactive boxed records, while remaining compliant with HIPAA privacy regulations.
- Financial services companies need it to conform to the myriad retention requirements of Sarbanes-Oxley, Basel II, SEC 17a, and the strict privacy rules of EU-Safe Harbor program, PIPEDA and the Gramm-Leach-Bliley Act; to manage inactive boxed mortgage and commercial loan files over periods of decades; and to ensure the authenticity, integrity, and confidentiality of records from creation to delivery.

For example, one OmniRIM customer, a global pharmaceutical company, stores records in multiple repositories across North America and Europe, and formerly had no single point to coordinate records destruction, legal holds, litigation support, or FDA Audits. The company receives an average of 24 new litigations daily and employed 26 paralegals strictly to

support searching for documents to satisfy discovery requests. After implementing OmniRIM, this company was able to cut labor cost by reducing the number of paralegals focused on discovery, and reduce risk by implementing a common global records destruction and legal hold process. OmniRIM also provides a single access point to support FDA audits.

A second customer, a Big Four accounting firm, was facing increased oversight due to SOX regulations. With over 70 different systems to track records over their network of 100+ offices, they had no common system to manage record destruction or legal holds, or to support litigation. Now, with OmniRIM, partners, principals, directors, and general counsel enjoy global access to all the firm's hardcopy records. The firm was able to implement a common global legal hold and records destruction process, and meet its obligations related to chain of custody and 45-day reporting rule.

Special Requirements of Physical Records

Managing physical records is complicated by several factors: They consume significant storage space, so their storage must be carefully planned and organized, and they have to be tracked as they are physically moved to and from their storage location. In addition to their logical classification in the file plan, their storage location must be organized and tracked at the folder, box, shelf, and warehouse level. Records must carry physical markings, such as color-coded labels with barcodes, that link their physical location with their entry in the ERM database, with special provisions to enable reliable tracking on retrieval and return. In some cases, organizations may want to outsource the physical warehousing of records to a service provider such as Iron Mountain, yet maintain their own ERM database. Physical records storage software, such as that from OmniRIM, thus has to integrate these special features with the standard capabilities of the ERM repository.

A Unified Management Solution

Given the differences between physical and electronic records, what would a truly unified ERM solution look like? Ideally, it should provide:

- A common file plan, i.e., a single folder tree supporting both electronic and physical record folders, with the ability to apply common retention, disposition, and security policies to both electronic and physical records. Physical and electronic record folders may support metadata specific to each record type.
- A common browser-based user interface for declaring and classifying electronic and physical records in the file plan, and thereby specify retention, disposition, security, and metadata.
- A common query interface to search for and request retrieval of electronic and physical records, although the mechanism of retrieval differs greatly between the two types.

In addition to these common features, the solution should ideally provide specialized support for paper and electronic records centers, dedicated to the distinct administrative requirements of those facilities.

That's what EMC and OmniRIM have achieved with their new joint solution. It consists of EMC Documentum Enterprise Records Manager 5.3, the OmniRIM Physical Records Management solution, and the OmniRIM eConnector for EMC Documentum that provides the integration.

EMC Documentum Enterprise Records Manager

EMC Documentum is the world leader in enterprise content management (ECM) technology. Layered on top of the Documentum ECM repository, EMC Documentum Records Manager v5.3 is a comprehensive enterprise records management solution for electronic records. It supports both formal records management, compliant with DoD 5015.2 and similar standards, as well as informal records management, based on transparent policy-based retention and disposition. The software may be deployed in modular fashion, allowing different parts of the organization to apply as much or as little records management as they need or are ready for at the moment.

The layering on top of ECM infrastructure gives EMC Documentum Records Manager a big advantage over the competition. When they are declared as records, documents do not need to be copied to a separate location but can be managed in place, secured by access control and retention rules on top of those normally applied by ECM, rules specified by policies in Records Manager. For instance, a record cannot be deleted by a user; retention is enforced by the system. Since the ECM repository can manage any type of content object – revisable documents, email, scanned images, instant messages, etc. – it meets a critical requirement for enterprise records management.

While records management adds its own attributes to each record, users can search for records based on metadata that already exists in the ECM repository. The content-aware workflow capabilities of ECM can also automate and track the records management process. Leveraging that existing metadata and workflow automation is the key to making records management pervasive and invisible in the enterprise.

Moreover, in many companies users already know how to use ECM. Documentum's browser-based client environment, called WebTop, provides a common user interface familiar to users across the enterprise. Integrating records management with the standard WebTop lowers the skills and training barrier that inevitably gets in the way of traditional records management technology.

The records management software is packaged in two pieces:

EMC Documentum Retention Policy Services (RPS) supports the creation, management and application of retention policies. It can be deployed standalone to provide retention 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. 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 the 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 just 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.

EMC Documentum Records Manager 5.3 (RM) supports the creation, management, and application of security, containment, and naming policies. It is also a DoD 5015.2 Chapter 2 and Chapter 4-certified records management application for file plan creation and maintenance, formal records declaration, and general records administration. Deployment of each type of policy is optional and independent, each policy is used 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.

OmniRIM Physical Records Management

OmniRIM Solutions is the leading supplier of software dedicated to physical records management, including paper files, microfilm, and electronic media. Its approximately 100 customers worldwide include six of the top ten pharmaceutical companies, three of the Big Four accounting firms in North America, four of the top North American insurance companies, numerous public sector agencies, plus a number of large companies in banking, energy, chemicals, consumer products, and entertainment.

OmniRIM provides comprehensive support for creating, classifying, editing, circulating, searching, and retrieving records related to active and inactive documents, files, and boxes. The records database is centralized, but physical storage is frequently distributed over multiple sites, both in-house and third-party. Retention rules direct the migration of records from active folders to semi-active files and boxes to archived files and boxes, and ultimately to final disposition.

Users can apply their organization's pre-defined file plan to any records or groups of records, which automatically updates retention dates for those records. OmniRIM also simplifies record classification by providing searchable classification types. Users can monitor records through their lifecycle from creation to final disposition, and manage records at any lifecycle stage. OmniRIM provides an audit trail of all retention and disposal actions, and ensures company-wide policies are enforced.

| Eligibility for Boxing Report | | 10/30/2006 |
|-------------------------------|-------------|----------------------|
| Barcode: | 00000237 | |
| Schedule: | 01 | TOMRIMS |
| Primary: | F | FINANCE & ACCOUNTING |
| Secondary: | F25 | TAX ROL |
| Tertiary: | | |
| Quaternary: | | |
| Quintenary: | | |
| File: | 999000 | |
| Volume: | | |
| Business Unit: | CHI | Chicago |
| Cost Center: | MAR | Marketing |
| Open Date: | 01/01/2001 | |
| Active: | T | |
| Sched Archive Date: | 12/31/2001 | |
| RestrictedNo | Access: No | |
| Location: | ACCAP | |
| Enclosure | Description | |

| OmniRIM - Eligibility for Box Destruction Report | | | |
|--|--------------------------------------|-------------------------------|--------------------------|
| Barcode: | 00000294 | | |
| Schedule: | 04 | Administrative Schedule | |
| Primary: | ACC050 | Accounts Payable / Receivable | |
| Secondary: | | | |
| Tertiary: | | | |
| Quaternary: | | | |
| Quintenary: | | | |
| Box: | OmniRIM Solutions Accounting Records | | |
| Box Type: | S | Standard | |
| File Owner: | | | |
| Office Box N | | Content Range: | 01/01/2001 To 12/31/2001 |
| Office: | CHI | Chicago | |
| Department: | ACC | Accounting | |
| Open Date: | 11/21/2005 | Close Date: | |
| Active Retention: | FY+1Y | Semi-Active Retention: | NIL |
| Scheduled Archive Date: | 03/31/2007 | Scheduled Destroy Date: | 03/31/2007 |
| PIB: | No | PUR: | Yes |
| Vital: | Yes | Confidential: | Yes |
| Original: | No | | |
| Location: | A-02-A-01-A | SHELF R: | A A: 2 C: A R: 1 B: A |
| Classification | Title | Location | Barcode |

Figure 1. OmniRIM reports track the retention lifecycle of physical records. Source: OmniRIM

All file movements are tracked and monitored within the OmniRIM audit trail. Archival and disposal actions are assigned at the file level, with reports to users (Figure 1) detailing eligibility for archiving (when files should be boxed up and sent offsite) and disposition (destruction or permanent archive).

OmniRIM provides system-generated barcodes and color-coded labels that improve administrative efficiencies, reduce lost and misfiled records, and streamline circulation and space management (Figure 2). Remote barcode scanning, linked to the records database

through a web interface, provides real-time file check-out and check-in with audit trail, and enables self-service kiosk-based file rooms. Online barcode scanning allows single or batch record transfers to locations or users, immediately updating the records database. Portable batch barcode scanning provides remote check-out delivery verification, warehouse shelf put-away, and check-in/out activity tracking, with automatic database upload and verification.



Figure 2. Support for system-generated label printing and barcode tracking are important to efficient physical records management. Source: OmniRIM

OmniRIM provides a separate Records Center module dedicated to the specific planning and administration needs of records center managers. OmniRIM Records Center defines and manages shelf and storage space while monitoring activity such as check-in/out at records center sites. This software assigns rates, calculates costs for activities, and generates reports or invoices for chargeback. It also offers a space forecasting feature that calculates future storage space availability.

Included with this module is support for records housed at an Iron Mountain facility. OmniRIM's IM Connector imports and reconciles Iron Mountain activity data with OmniRIM data, helping companies save money by reconciling and resolving third party warehouse invoices. Requests for items stored at Iron Mountain automatically generate a notification to the vendor for delivery. IM Connector can be configured to automatically reconcile transaction data provided by Iron Mountain's IM-Connect application.

OmniRIM eConnector for EMC Documentum

The OmniRIM eConnector for EMC Documentum unites the two records environments. With eConnector, companies can apply federated policy management to unify records management practices across the enterprise. OmniRIM eConnector can be implemented with new deployments or retrofitted to existing OmniRIM or EMC Documentum systems.

The architecture relies on separate OmniRIM and Documentum databases united under a federated file plan. With the initial release of the OmniRIM eConnector for EMC Documentum, and EMC Documentum RM 5.3, the file plan is maintained and managed by EMC Documentum, creating a master/slave relationship. In a follow-on release of both the eConnector for EMC and EMC Documentum RM, the file plan will be maintained and managed by either OmniRIM or EMC Documentum. Both OmniRIM and EMC Documentum retain their own copy of the file plan in order to reduce network traffic and latency, but only one system can drive changes to it. Any changes made to the master file plan are automatically updated in real-time in the slave.

The architecture is illustrated in Figure 3.

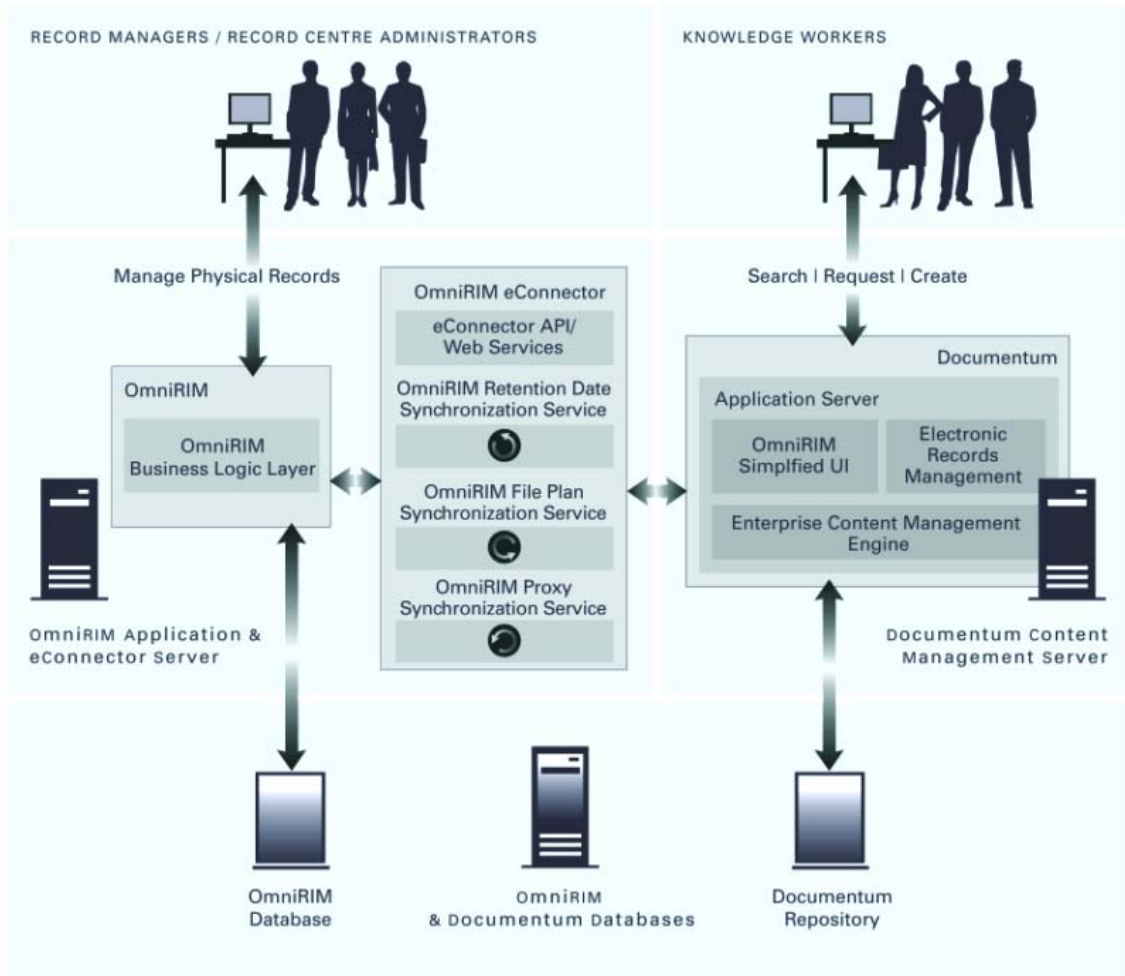


Figure 3. Technical architecture of unified OmniRIM-Documentum solution. Source: EMC

The OmniRIM and Documentum servers remain separate, but the file plan and associated metadata are synchronized between them. This federated approach enables a unified view of physical and electronic records. For example, through the Documentum WebTop, end users, compliance officers, and records administrators can view a single file plan hierarchy containing both physical and electronic record folders, and a single search will return records of both types.

For example, Figure 4 illustrates creation of a physical record folder from the Documentum WebTop.

Unifying Management of Physical and Electronic Records

New Physical Record: Info

Create physical_folder

Location Type: Location * Location Code: CHILEGAL -- Chicago Legal File Room Container Barcode: []

Title: Maintenance Invoices for OmniRIM * Media Type: F -- Folder

File Number: OSI Volume Number: 1

Content Start Date: Date Content End Date: Date

Office Code: CHI -- Chicago * Department Code: ACC -- Accounting *

Open Date: Jan 1, 2006 Close Date: Oct 30, 2006

Review Date: Date Destroy Date: Date

Authority: AB -- Art Bellis

Event Date: Oct 30, 2006

Profile Number: []

Figure 4. Physical record creation from the Documentum WebTop. Source: EMC

Here's how that integration works using the eConnector. Users wishing to create physical records enter metadata into the creation form in WebTop. The request is submitted and through API's and OmniRIM validates the metadata for completeness and accuracy and assigns a unique barcode to the item. Users can request the pickup of this physical item by the records staff through WebTop.

Search: Tilbury Go Advanced... Preferences Logout Help

File Edit View Tools Records

Search Results
Results for "Tilbury" in EMC_Default
3 Total Edit Search Save Search

| Name | Ranking | Summary | Modified | Source |
|--------------------|---------|---------|-------------------|----------------------------|
| Tilbury EDI Form | 1 | | 12/27/06 11:06 AM | EMC_Default:/04/ACC050/002 |
| Tilbury Contract | 1 | | 12/27/06 11:15 AM | EMC_Default:/04/ACC050/003 |
| F00000392: Tilbury | 1 | | 12/27/06 10:55 AM | EMC_Default:/04/ACC050/002 |

Items per page: 50

A single search will locate both physical and electronic records and display them in the same results panel. Users can request physical records directly from this view.

No Messages View Messages Job Status Classic Streamline

Figure 5. Unified search and file plan hierarchy in the Documentum WebTop. Source: EMC

Once the physical record is created in OmniRIM a web service creates a new physical record proxy object in the Documentum database. This proxy object now resides in the same

repository as the electronic records created and managed by EMC and allows the users to execute a single search for all physical and electronic records. When physical records are found in a search, users can request delivery of the item by the records staff. With all records in a single repository, unified disposition, auditing and legal hold processes are consistently managed across media boundaries.

Image Delivery With Captiva

Retrieving a physical record may mean physical transport of folders or boxes from the fileroom or warehouse to the requester site, a process usually measured in days. The eConnector also supports a faster alternative based on imaging using EMC Captiva software. Captiva offers remote scan-on-demand capability, which is often much more cost-effective than full backfile conversion.

On request from WebTop, users can either request delivery of the physical records or digital delivery of scanned images. Barcodes applied to the documents allow for efficient image scanning, since they link the scanned document image in the Documentum repository to metadata of the physical record. Scanned images can be delivered instantly over the network and routed by Documentum BPM services. This further accentuates the efficiency and compliance benefits of the OmniRIM-Documentum unified records management solution.

The Bottom Line

The federated file plan allows users to specify retention, security, and metadata of both electronic and physical records from a common interface, the Documentum WebTop. Creating or classifying a physical record in this way creates the proper access control and retention formulas and rules in the OmniRIM system, ensuring lifecycle promotion and disposition are compliant with global policies and standards. It also allows users to apply legal holds quickly, easily, and consistently across all record types.

Policy-based retention and disposition are crucial for ensuring compliance and mitigating discovery risks. The eConnector solution allows records managers to adopt a global view and design an enterprise file plan that encompasses both physical and electronic records, with the confidence that common retention and disposition policies will be implemented consistent with the unique requirements of each record type. The implementation of “archive” or “destruction” is different for physical and electronic records, but the business intent is the same. An audit trail is maintained for all record actions, physical and electronic, while retaining support for the unique tracking characteristics of each type.

OmniRIM is the leader in technology for physical records management. EMC Documentum is the leader in technology for electronic records management. The OmniRIM eConnector for Documentum, augmented by integration with EMC Captiva, brings the best of both worlds together in a unified solution for all records across the enterprise. It allows policies to be defined and applied to records regardless of their form, physical or electronic.

Physical records are not going away, and the stakes for non-compliance with regulations and rules of civil procedure continue to escalate. Applying records management policies consistently across all types of records just makes business sense. If you're thinking about a comprehensive unified approach to managing your company's records management problem, take a good look at the OmniRIM/EMC Documentum solution.

Bruce Silver