EMC Corporation

Assured Records Management:
Establish and Maintain a New Level of Performance

Prepared by
Cohasset Associates, Inc.

February 2005

Abstract

The beginning of the twenty-first century has been marred by an erosion of trust in corporate and government institutions. The waves of regulatory investigations and sanctions, the proliferation of electronic content, and concerns about the protection of privacy and intellectual property have raised awareness among business and political leaders of the urgent need to improve enterprise information management.

This White Paper introduces Assured Records Management (ARM), a rational approach to re-aligning an organization's continuum of technical and non-technical capabilities to improve corporate control over electronic information assets at the records level. The intended audience for this paper includes those individuals charged with management of file systems, technology infrastructure, and electronic record repositories who are looking for ways to gain senior level support for the strategic application of business controls to the retention and disposition of electronic information assets.

This methodology will assist organizations in setting a course and mobilizing resources in ways that facilitate the proper execution of business rules across processes and information networks with efficiency and accountability, resulting in higher, sustainable levels of retention and disposition control and management of electronic records.

Table of Contents

1. Executive Summary

Records[1] are essential to the survival, welfare, and prosperity of organizations,[2] and have been managed for centuries to meet a variety of social (legal, ethical and moral), service, and profit-related (or cost avoidance) objectives. To successfully achieve these objectives, as well as satisfy long-standing legal standards for evidential admissibility, records must be systematically identified and organized, and then preserved and protected in ways that imbue accuracy, reliability and trustworthiness for as long as they are needed.

As the volume of records produced began to grow in earnest during the twentieth century, specialized facilities for the storage of records ('records repositories') grew in number and in the quality of environmental and security controls. This method of protection provided the necessary controls to ensure the availability as well as the integrity of these primarily media-centric (paper or film) records. Disposition of these records, which included destruction as well as the transfer of discrete sets of records with historical or permanent value to an archival facility, was administered under carefully documented and audited procedures.

With most of today's business information created in digital format, **the rules of the records management game have changed dramatically.** Research suggests there's been a 30% increase in the amount of stored information (includes four types of physical media: paper, film, magnetic and optical) each year between 1999 and 2002, with 92% of new information stored on magnetic media, primarily hard disks.[3] Given these staggering volumes, organizations need efficient and scalable ways to capture and protect their electronic records, as well as an efficient and verifiable means to dispose of or destroy information and media when there is no longer a requirement to keep them.

Computer-enhanced records control capabilities must be proactively and systematically deployed on the basis of defensible retention and disposition rules that are carefully aligned with the mission and strategic initiatives of the organization.

The risks associated with poor or no formal records management programs have been well documented in the mainstream media in recent years in terms of legal and regulatory compliance risks and costs, as well as the overall effectiveness of business operations. The swell of high-profile investigations and indictments has resulted in new regulatory requirements for improved and more transparent internal process controls. In short, compliance and integrity risks associated with electronic records management have been elevated to the enterprise-level. As a result, the Information System/Technology ('IS/IT')[4] function is being increasingly brought into content management activities and compliance actions.

When courts and regulators demand prompt access to electronic evidence,[5] the consequences of deploying technology systems without first developing value-based[6] retention and disposition requirements for their content have become increasingly apparent. Failure to distinguish between backup systems and records archives[7] has resulted in multimillion dollar fines and penalties for many prominent firms. Decisions about records that are included or excluded from legal hold orders must be possible without the need to restore and conduct a file-by-file analysis of hundreds of backup tapes. Compliance with electronic recordkeeping requirements must become a proactive, not reactive, process.

This convergence of powerful forces provides impetus for government and businesses to re-examine how they will align their electronic records management objectives and operational needs in the coming years. But while recent events have evoked higher levels of awareness and a general commitment by leadership to improve performance in the management of enterprise information content, the path forward is often difficult to discern given the magnitude of the task and in light of competing priorities and limited resources. Awareness of the risks and challenges without the means to build consensus and organize resources in ways that align to the business' needs and interests only leads to frustration and wasted efforts. Focusing on meeting the requirements of one regulation or the needs of one business area at a time only exposes the organization to higher costs and increased risks.

CohassetAssociates | *Guiding the way to successful records management*

Purpose of This Paper

Based on its extensive consulting experience and on-going survey research of records management professionals, Cohasset Associates, Inc. recognized a critical need for organizations to improve performance in electronic records management. In response, Cohasset advanced the concept of Assured Records Management (ARM). EMC Corporation engaged Cohasset to prepare this White Paper which introduces a structured methodology to significantly improve the retention and disposition of valued electronic information assets.

The ARM approach includes techniques and tools that organizations can use to:

- build cross-functional literacy and cooperation to meet electronic records retention and disposition requirements,

- align technical capabilities and electronic records lifecycle management best practices[8] with the organization's strategic business priorities,

- develop long-term electronic records repository management strategies, and

- devise RM-enabling technology infrastructure and information architecture goals and action plans for the near and long term.

The intended audience for this paper includes those individuals charged with management of information file systems, technology infrastructure, and electronic record repositories who are looking for ways to gain senior level support for the strategic application of business controls to the retention and disposition of electronic information assets.

Success of the ARM approach depends upon the will of the organization's leaders to act to bring electronic record assets under the same level of management and controls that other business assets (capital, human resources and facilities) have long enjoyed. Computer-enhanced records control capabilities must be proactively and systematically deployed on the basis of defensible retention and disposition rules that are carefully aligned with the mission and strategic initiatives of the organization.

CohassetAssociates | *GUIDING THE WAY TO SUCCESSFUL RECORDS MANAGEMENT*

It is only when IS/IT can successfully apply records retention and disposition rules to the vast stores of content contained within technologies that manage and store electronic files, documents, images, and data used by the business and relied upon to protect against future audits and litigation, that the organization will be able to significantly mitigate its risk, improve operational performance of production and collaborative information and communication systems, and consistently execute compliant and legally defensible business practices.

Cohasset Associates, Inc.

Cohasset Associates (www.cohasset.com) is recognized as one of the nation's foremost consulting firms specializing in document-based information management. Now in its fourth decade of serving clients throughout the United States, Cohasset Associates provides award-winning professional services in three areas: management consulting, education and publishing.

Cohasset Associates' consulting practice focuses on improving the programs, processes, and systems that manage document-based information. Services range from establishing enterprise records management programs to planning state-of-the-art electronic records systems. Using its unique combination of records management, legal, and technical skill sets, together with its extensive problem-solving experience, Cohasset Associates works to provide its clients with cost-effective solutions that will achieve their business objectives and meet their legal/regulatory responsibilities.

Cohasset also is renowned for excellence in education and research. This includes organizing and sponsoring the annual Managing Electronic Records (MER) conference, with its special focus on the legal, technical and operational issues (www.merconference.com); preparing thought-leadership White Papers addressing key issues in electronic records management, and; providing the definitive survey research and analysis of electronic records management trends and challenges.

2. The Business Challenge of Electronic Records Management

Despite all the sensational media attention in recent years, the discipline of records management (RM)[9] isn't new or particularly exciting. It is, however, a demanding business function that has long been taken for granted. Guided by laws, regulations and the organization's culture and structure, corporate RM has traditionally been responsible for establishing proper recordkeeping guidelines, policies and procedures. For decades, the protection of significant documents, files, contracts and physical objects has been performed by caretakers relying on tried and true methods and tools such as filing cabinets, file folders, imaging, indices, and secure storage facilities to meet the organization's basic recordkeeping requirements.

Within many corporations, records management was often considered as a back-office cost center with little business benefit. Records managers have had to rely on the creators and users of business records and their administrative support staff to comply with retention rules for hard copy documents, and hoped that drafts and other non-records were systematically destroyed. Periodic audits of select business areas or processes provided a snapshot of records management program effectiveness and the level of management support for its dictates. The records management function served a custodial role for vast stores of inactive records. As the retention period for records expired, RM systematically administered an auditable, certified records destruction process. Accurate recordkeeping however, has always been difficult, if not impossible, to enforce on an enterprise-wide level.

Fast forward to the start of a new century and the landscape for business records management has become significantly more complex. The modern business

enterprise is comprised of multi-vendor network and storage environments that manage hundreds of different electronic file types and formats. Records management activities now take place within many information system and technology (IS/IT) contexts that include applications and networks for managing documents, transactions, customer and supplier relationships, electronic messages, databases, forms, images, workflow, and web sites.

2.1 Organizational Barriers to Electronic Records Management

Enforcement for and proof of the proper retention and deletion of records, regardless of where they are stored, the format in which they were created, or the media on which they exist, is expanding and shifting outside of official business and RM functions to IS/IT functions.

The creation of business records occurs at the event or transaction level and so it is here that the exploration of opportunities and barriers to control must begin. Unfortunately, the organizational structures, employee behaviors and access controls that worked for many business functions and their hard copy records of the past do not extend into the digital environment.

Users are often uncertain of how to handle drafts and official documents they produce using a host of desktop applications. Standardized naming conventions, metadata and classification schemes are frequently unavailable or disregarded which leads to vast collections of electronic records in unmanaged and unorganized environments. These collections are likely to include documents that reside in general purpose folders on network drives with no apparent method of arrangement, as well as documents located in folders on local hard drives where non-standard naming and indexing conventions render the content meaningless and inaccessible to other users.

The complexity of today's information systems environments makes it difficult for employees to control or direct the movement, storage, access/retrieval, preservation or deletion of many of the business records they produce or receive from either internal or external sources. As a result, information is widely dispersed on desktops, laptops, applications, shared servers, backup tapes and PDAs. Enforcement for and proof of the proper retention and deletion of records, regardless of where they are stored, the format in which they were created, or the media on which they exist, is expanding and shifting outside of official business and RM functions to IS/IT functions.

Users often assume that any records they create while using major business applications or databases are being managed in compliance with retention and disposition rules on the back end by the IS/IT function. The IS/IT group may be counting on the users or business function to know when and how to identify, declare and classify the records they use. They also want users to take responsibility for cleaning out files, folders, directories and other electronic document storage areas on a periodic basis. This confusion about accountability for managing electronic information assets leaves RM with retention and disposition rules which go unheeded by business staff and are not enforced in the digital environment. It also results in production systems full of mixed, unmanaged and low value/no value content.

Capabilities that enable assured levels of recordkeeping performance must be designed and integrated, over time, into the fabric of the technology infrastructure and file systems.

The 2003 Electronic Records Management survey conducted by Cohasset Associates and sponsored by ARMA and AIIM[10] confirmed many of these disconnects in the management of electronic records:

- 41% of records managers responded that electronic records were not included in the organization's records management program.

- More than two-thirds (71%) reported that IS/IT had primary responsibility for the day-to-day management of their organization's electronic records.

- An overwhelming majority (93%) believe the process by which electronic records will be managed will be important in future litigation, but by a ratio of nearly 2:1, a majority (62%) were less than confident that the organization could demonstrate its electronic records are accurate, reliable and trustworthy – many years after they were created.

Meeting the unique challenges associated with electronic records management requires new ways of thinking and a renewed spirit of collaboration to work across domains and disciplines.

2.2 Technological Challenges to Electronic Records Management

New government regulations[11] for the retention, access and storage of data have changed the ways that data must be managed as it ages. In the past, it was assumed that as the frequency of access to information decreased, the value of the information decreased. But the back-end of the information management lifecycle is no longer shrinking – it is growing exponentially – and the retention policies associated with the stored information must be based on the value to the business, not just reference activity. The tools and techniques (folders, files and filing cabinets, off-site storage, document shredding, department retention schedules, etc.) that worked in the media-centric paradigm[12] do not all have equivalents in the integrated digital environment. And the complexity of content created in computerized environments (mutable, associated metadata, dynamic) has redefined what is meant by a business record. Technology infrastructure that was built for data protection and stability, may, in fact, create significant barriers to meeting recognized standards for electronic records management.

Unlike other electronic documents and information objects, electronic records must bear characteristics that can be proven or demonstrated, including authenticity, reliability, integrity and usability.[13] The traditional principle that all records relied on in the usual and ordinary course of business can be presumed to be authentic records must be supplemented in the case of electronic records by evidence that records have not been inappropriately altered. This is because the same powerful information technologies that enable the creation, receipt and distribution of business records can also be used to alter their content.

Distinguishing between archiving and backup systems is critical to protecting electronic information assets and providing access to records when they are needed. This continues to be, however, an area of significant exposure for many organizations. Backup data is routinely stored separately on portable media. Backup systems are designed to provide wholesale recovery in the event that the production environment suffers catastrophic failure. These systems cannot provide authenticity, real time access, or security to meet regulatory compliance requirements and legal discovery related records production. Most importantly, back up systems do not enable record-level management of the content – it's

CohassetAssociates | *Guiding the way to successful records management*

an all or nothing proposition. Keeping backup tapes for months, or even years, negates the efforts that organizations otherwise make to systematically eliminate electronic information and media as part of a disciplined management process.

The diversity of communication and information systems which has accompanied achievements in areas such as financial services, health care, and product safety have created fragmented information technology environments and a torrent of data and electronic records in all business enterprises, large and small, regulated and non-regulated. With data volumes growing at an annual rate of 125%, applications and file systems throughout the enterprise become increasingly clogged with unmanaged, fixed content. Applications like email have become de facto record repositories and are being used to perform recordkeeping tasks that they were never designed to handle. Content (record and non-record, transitory and long-term, etc.) is increasingly co-mingled, dispersed and duplicated in network servers and back-up systems, making it nearly impossible to pinpoint the official record (for business use or in response to electronic discovery), apply retention policy, or establish acceptable access and recovery response parameters. Major records-related risks, created by the pervasive use of computer technologies, now exist in most organizations such as duplicate records, user indecision or inaction, and the unnecessary storage of records that have exceeded their required retention period.

2.3 The Path Forward

Dependence on technology, which has created such enormous challenges in the management of electronic records, is also a key part of proactive and sustainable solutions. Capabilities that enable assured levels of recordkeeping performance must be designed and integrated, over time, into the fabric of the technology infrastructure and file systems. These systems must be demonstrably trustworthy in the "chain of preservation;" the system of controls that extend over the entire lifecycle of records and ensure the identity and integrity of the records as they are maintained in storage repositories and whenever they are retrieved or reproduced. In this manner, IS/IT provides critical support to the creators and users of business records to meet the organization's mission and comply with its information governance guidelines.

CohassetAssociates | *GUIDING THE WAY TO SUCCESSFUL RECORDS MANAGEMENT*

What is urgently needed to move forward from this current information and records management conundrum is a strategic vision that integrates principles and business rules for effective information and records management, with an architecture that enables sustainable compliance with the rules and takes into account the planned obsolescence of hardware and software. The purpose of this paper is to introduce a methodology, **Assured Records Management,** to assist organizations in quickly developing a course of action to incrementally begin increasing enterprise control over its valued electronic records assets.

The Assured Records Management approach offers a bridge from the current state of electronic records management performance towards a progressively more RM-informed IS/IT architecture and infrastructure. Along the way, opportunities to partially facilitate or completely automate records management tasks are evaluated, prioritized, and implemented in line with the business' strategic goals and objectives.

3. Introducing Assured Records Management

Changing accountabilities for the preservation of electronic records must be acknowledged, supported and enforced by the organization's leadership.

Assured Records Management is a methodology developed to help organizations systematically improve control over their electronic record assets. ARM is a disciplined, business-centric approach that guides organizations from their current state of enterprise content management to an environment where senior management has confidence that:

- High value information is trustworthy and protected;

- Low value information is routinely purged and appropriately destroyed;

- Information system technology investments are aligned to business priorities and goals and meet corresponding information and records lifecycle management requirements, and

- Employees have the support and tools they need to comply with retention and disposition rules for managing the electronic records that they create and receive.

The ARM approach leverages programmatic elements of traditional records management (policies, procedures, education, and retention and disposition management guidelines) with the identification, design and implementation of tools and technologies that leverage computer facilitation, and where possible, automate the execution and auditing of many record keeping tasks for electronic information assets. The expertise of those who define business rules for recorded information assets are re-aligned and integrated with the capabilities of recordkeeping technologies and their custodians to serve the business priorities of the enterprise.

Cohasset Associates | *Guiding the way to successful records management*

Cross-functional collaboration between technical experts, the community of business subject matter experts, and policy makers (business, legal, compliance, records management) is the only way to ensure that business rules governing the protection of and access to electronic records are thoroughly identified, designed into processes and systems, implemented, and enforced on an on-going basis. Continuous improvement is facilitated through the use of compliance metrics that document recordkeeping system performance and accountabilities. Changing accountabilities for the preservation of electronic records must be acknowledged, supported and enforced by the organization's leadership.

Reaching a New Level of Electronic Records Management Performance

Drawing upon the skills and expertise of stakeholders representing key functions (business, IT, legal/compliance, RM), the Assured Records Management methodology deploys a series of five modules with exercises and tools to quickly design a tailored, executable strategy that aligns cross-functional resources and system capabilities to improve control of electronic record assets in areas that are most critical to the business. The most appropriate approach for any organization to take will depend significantly upon its legal and regulatory responsibilities, mission and goals, and available resources.

Individuals with the requisite knowledge and authority work together through a facilitated process to identify organizational challenges and characteristics of the technology infrastructure that have an impact on meeting electronic records management requirements. Within the framework of ARM's Dimensions of Success, the organization's current state is assessed and underlying causes and effects identified. Using strategic goals and objectives as a filter, the ARM methodology guides participants to articulate a future state level of performance and common goals for electronic records management. Opportunities to narrow the gap on the organization's performance are identified, evaluated and prioritized based on ARM Action Principles. This forms the basis of the ARM action plan for immediate next steps.

CohassetAssociates *GUIDING THE WAY TO SUCCESSFUL RECORDS MANAGEMENT*

RM-Enabled Technology Architecture and Infrastructure

The ARM methodology is technology-dependent and vendor neutral. The explosive growth in data and electronic records has spurred tremendous merger and acquisition activity in the technology marketplace which has led to dramatic advances in the capabilities of the software, hardware and systems used to create, distribute, manage, store and dispose of records.

Enhanced electronic records control capabilities, such as those embedded in e-mail archiving, content management software and storage management components, can now be deployed and the performance of end-to-end systems monitored for compliance with defensible, value-based business rules for retention and disposition. Computer-facilitation for the process by which records are managed makes it possible to achieve an "assured" level of performance that ensures the credibility and trustworthiness of the organization's electronic information assets.

Benefits of Assured Records Management

The Assured Records Management approach offers significant benefits in terms of operational efficiencies and user and system productivity, as well as liability and enforcement risk and cost containment by providing a rational means to:

- Achieve a new level of excellence in compliant recordkeeping practices – one that is highly resistant to legal attack.

- Document and independently authenticate the details and results of the records management process.

- Leverage the power of information systems, relieving knowledge workers from burdensome and time consuming tasks.

- Lower operating costs – particularly to achieve a similar level of excellence.

- Contribute to an organization's risk mitigation initiatives.

- Reduce legal, and particularly discovery, costs – the most significant uncontrolled cost in American business today.

Cohasset Associates | *GUIDING THE WAY TO SUCCESSFUL RECORDS MANAGEMENT*

4. Managing Electronic Information Assets at the Records Level

The preservation of authentic electronic records is a continuous process that begins with records creation, and whose purpose is to transmit authentic records across time and space.

The ways in which information is created, managed and preserved in the digital environment are inherently different from those in the paper or film world. Electronic records management is a discrete process that takes place within the broader context of an organization's overall content or information lifecycle management environment.[14] The preservation of authentic electronic records is a continuous process that begins with records creation, and whose purpose is to transmit authentic records across time and space.[15]

4.1 Electronic Records Management Requirements

Principles and criteria for the creation and protection of authentic electronic records and trustworthy record-keeping systems which are based on the research, standards and laws of governments[16] and major industries are summarized in Table 1 (starting on next page).[17] The ARM methodology is predicated on these best practice electronic records management requirements.

Cohasset Associates | *Guiding the way to successful records management*

Table 1. **Electronic Records Management Requirements**

Records Lifecycle	Definition	Requirements
Acquisition	Records are identified, declared and classified in accordance with the organization's retention rules.	1. Takes place at or near the time of the event or transaction when the record was created (finalized) or received. 2. The record is placed under tight and auditable recordkeeping control. 3. Complete and accurate content, context and structure of the record are captured, including associated search and administration metadata. 4. Records must be organized to enable retention, accessibility and retrieval. 5. Training and on-going education regarding the rules for business records creation, use and organization should be provided to stakeholders (employees, partners and suppliers) to facilitate compliance.
Access and Production	Records should be maintained in a trusted record-keeping system and preserved by a trusted custodian.	1. Records must be accessible ("readily" accessible per some regulations). 2. Records must be reproducible in human readable form upon request by regulators or authorized business roles or persons, or in response to legal discovery. 3. Systems must be designed to track every access to a records system and every action on any record in the system. 4. System design must preclude any alteration or destruction of records except by authorized individuals. 5. A trusted recordkeeping system comprises the whole of the rules that control the creation, maintenance and use of the records and provide a circumstantial probability of the authenticity of the records within the system.
Disaster Recovery Copy	A duplicate "recovery" copy of the original electronic record is stored.	1. The duplicate copy is usually stored in a separate geographical location from the original. 2. Enables recovery in the event that a production system or environment suffers catastrophic failure. 3. Includes records that contain information critical to the continued operation or survival of an organization during or immediately following a crisis.
Retention Management	Records are retained for specific periods of time (and in some cases, retained in specified ways).	1. Retention periods are time-based, action/event-based or a combination of the two. 2. Retention rules are based on an appraisal of the value of the record to the organization, and may be specifically designated by an internal or external authority that mandates the record's retention. 3. Records must be protected from alteration, overwrite or deletion for their full retention period.[18] 4. Requirements for the official record should be specified. 5. Retention policies must be periodically updated to accommodate legal, regulatory, organizational, industry or other business-related changes.
Repository Management/ Storage	Implicit requirement to provide a substantively equivalent "non-rewritable, non-erasable, non-alterable" management environment – whether by the content and/or records management application or by the storage management software, or both.	1. Most regulations include authorization for the storage of specified records on an alternative media – optical storage, magnetic storage or microfilm. 2. Some regulations specify the type of media, the functionality of media, and how the records are recorded on the media.[19] 3. Content custodians and technology custodians should be designated to ensure the physical storage and protection of records throughout their authorized retention periods.

Records Lifecycle	Definition	Requirements
Disposition Management	The final business action carried out on a record (usually to destroy or to archive) is performed in the regular course of business.	1. Disposition should include all copies of the record along with associated metadata. 2. Disposition should occur upon expiration of the established retention period (taking into consideration any records holds or suspensions). 3. Electronic records disposition can include 'soft deletions,' 'hard deletions,' hard deletions with overwrite,' 'archive to long term store,' 'forward to organization,' and 'copy to another media or format and delete (hard or soft).'
Legal Hold / Preservation Order	Legal discovery and regulatory investigations may require that records be placed on hold or suspended (from being destroyed or disposed of) until the legal or regulatory action is completed.	1. Hold orders are independent of the retention period established for records. 2. Persons authorized to suspend normal destruction procedures and impose a legal hold must be identified.[20]
Audit and Compliance	Evidence that the integrity and retention requirements of records have been met is required.	1. Provides proof of the "chain of custody" regarding such events as migration and final disposition (deletion) as well as any changes made to the record and its associated metadata. 2. Trusted recordkeeping systems and custodians must be capable of implementing all the baseline requirements of authentic electronic records.

Key characteristics of information systems which create, transmit, archive and dispose of electronic records include:

- Reliability over time and in the normal course of business;

- Control measures to monitor, verify, authorize and secure access;

- Compliance with changing business, regulatory and legal requirements;

- Ability to manage media-centric and content-centric records produced by the complete range of business activities for the organization;

- Systematic creation, maintenance and management through the design and operation of rule-based records and business systems.

The retention, distribution, protection and disposition requirements for the organization's electronic records should be imbedded into its policies, procedures and tasks as rules, and applied across all technical and business systems and processes. And while regulatory authorities are largely technology neutral in establishing their recordkeeping requirements, each organization

is responsible for knowing and understanding the specific requirements that apply to their records, and for making the appropriate investments and implementing electronic records management process controls. In addition to regulations, best practices, and changing organizational requirements, business rules for the retention and disposition of records are also influenced by regulatory enforcement actions, information standards promulgation, and a growing body of case law related to electronic discovery.

Recordkeeping functions can now be performed at a level of quality, efficiency and reliability that is simply unattainable through manual means.

4.2 Technological Solutions

Meeting the requirements described above for the preservation and management of electronic business records is a daunting challenge given the volume, type, variation in retention requirements, and complexity of today's business environments and technology infrastructures. A shift in emphasis from media-centric to content-centric records and the speed and ease by which records are created and distributed, has fueled new demands for intelligent, tiered storage networks and computer-facilitated retention and disposition controls. Since many widely-used commercial information and communication systems lack true records management capabilities, other software, hardware and infrastructure solutions that offer dramatic technological advances in policy-based capabilities to capture, manage, store and dispose of electronic records have emerged to fill the requirements gap.

Breakthroughs in the functionality of records management software, for example, have resulted in new levels of computerized facilitation of tasks which include the declaration and classification of records. Computers can precisely track information about which user did what to which data and when – creating an audit trail that proves the authenticity of electronic records. Policy-based software offerings can now automate migration of data from applications to archiving and storage environments as well as effectively 'freeze' records in response to anticipated or in-force legal holds. Greater intelligence in archiving solutions allow organizations to decrease their dependence on backup tapes and the use of local hard drives for storage of records, thereby reducing risk and potential discovery costs.

Recordkeeping functions can now be performed at a level of quality, efficiency and reliability that is simply unattainable through manual means. The Assured Records Management methodology helps organizations determine **where to act** to align processes and technologies that increase corporate control over the electronic information assets, mitigate risk and increase operational efficiencies. It is imperative, however, that computer facilitation for core electronic records management functions be used in accordance with the baseline requirements for production and preservation of authentic records.

An assured level of operational performance can be demonstrated via inherent audit trail capabilities that track the movement of content and the actions of users and which can conclusively document the performance of records management process components. For management, a process that was once based on "hope" can now be based on detailed and precise performance metrics – providing assurance that the process by which electronic records are managed achieves a level of performance that ensures the all-important credibility of the organization's recorded information assets.

5. Case in Point: The Rise of E-mail Archiving

Electronic mail has become the primary means for business communications, making e-mail archiving capabilities a 'must have' for the majority of businesses and government agencies. News of lawsuits and enforcement actions appearing daily in the headlines highlight the tension between staying compliant with laws that specify the retention of e-mail messages and attachments, and simultaneously reducing exposure through the timely, routine disposition of transitory records, non-records, and records that have exceeded their respective retention periods. As the #1 business collaboration tool, analysts estimate e-mail storage needs will continue to increase at least 65% annually so organizations can no longer afford to wait to apply greater control over these ubiquitous electronic information assets.

With an estimated 75% of most companies' intellectual property contained in the messages and attachments sent through e-mail systems,[21] the need to apply new levels of retention and disposition control is urgent. Effectively applying retention and disposition rules to content within e-mail applications have proven to be challenging, however, for reasons relating to the technology, confusion about applicable business rules, as well as user resistance. The dominant e-mail platforms were designed to send and receive mail, not to act as document repositories. Individual in-boxes and the ability of users to create and manage personal folders runs counter to proper recordkeeping protocols. Many users tend to think of their e-mail inbox as a private repository for business and personal content of all sorts, and when forced to clean out their cache, find ingenious ways to squirrel away messages and attachments on local hard drives, CD, or DVDs which are often outside the reach of the official backup system. In short,

a records management program that relies solely on individual users to consistently apply records retention and disposition policies to all their e-mail or on the IS/IT administrators to apply an arbitrary time-based purge policy (60 day or 90 day) fails to meet baseline requirements for authentic electronic records.

Table 2 (on next page) examines the electronic records requirements for three components of the lifecycle – Acquisition, Retention Management and Repository Management – to illustrate Assured Records Management scenarios. In the first example, all inbound and outbound communications must be preserved as business records while in the second example, the organization relies on employee involvement to identify and declare records. Note that organizational, IT, compliance and RM program components are equally represented as part of an e-mail archiving solution.

CohassetAssociates | *GUIDING THE WAY TO SUCCESSFUL RECORDS MANAGEMENT*

Table 2. **E-Mail Archiving**

Records Lifecycle	Requirements	Assured Records Management
Acquisition	Records are identified, declared and classified in accordance with the organization's retention rules.	Example 1: All communications to/from a particular individual must be saved for a specified retention period: • Before delivery to the user, a copy of the e-mail is archived. • Before transmission to the designated recipient(s), a copy of the e-mail is archived. Example 2: Users in a specific work group are authorized to identify and declare e-mail and attachments as records. • Secure folders are created and designated as repositories for certain types of records. • Users mark e-mail messages that meet records criteria via some mechanism: a records "flag" or drag-and-drop. • Users are trained on records acquisition procedures. Access rights and security are applied to the folders.
Retention Management	Records are retained for specific periods of time (and in some cases, retained in specified ways).	• All messages are automatically tagged with metadata. • Time-based retention policy is assigned to each e-mail as it is archived. • Message protections and controls are governed by the file plan classifications applied; assuring equal treatment of e-mail and non e-mail records. • Only one instance of each e-mail and its corresponding attachment are filed in the archive; pointers back to the authorized users allow access. • User access to her/his messages is seamless; no additional user training required. • E-mail messages and attachments are deleted in accordance with retention policy, unless covered by a current hold order.
Repository Management / Storage	Records should be maintained in a trusted record-keeping system and preserved by a trusted custodian. Reproducing an electronic record means to render it with the content and any required elements of documentary form and annotations.	• The e-mail archive securely stores messages in accordance with retention policy. The archive is under the direct control of an administrator. • Metadata and indexing allows for quick search and retrieval capabilities. Access rights are determined by role and enforced by the system. • Legal holds can be applied to individual messages and attachments; retention policy is suspended as long as the legal hold remains in force. • Disposition of the e-mail and attachment is performed automatically by the system in accordance with retention policy (absent any current legal hold). • The contents of the archive and all functions performed on the archive can be audited at any time.

CohassetAssociates | *GUIDING THE WAY TO SUCCESSFUL RECORDS MANAGEMENT*

6. Conclusion

In a relatively short period of time, a sea change in the management of records has occurred due to the:

• Advent of electronic records as the overwhelming "record of choice" in the conduct of business,

• Complexity and variety of electronic records,

• Exponential increase in the volume of records, particularly electronic records,

• Increase in litigation and the newfound importance of electronic records discovery,

• Ever-changing requirements of compliance, together with the high stakes consequences of non-compliance,

• Great compression of time and the expansion of geographic boundaries associated with all business activities.

While retaining many traditional programmatic elements, modern records management now has a critical dependency on Information Systems/ Technology (IS/IT) and must rely on the leadership, organizational structures, processes and relational mechanisms of this key business function to enable and sustain computer assisted and/or automated records lifecycle management capabilities.

The Assured Records Management methodology offers a way for organizations to achieve this elevated level of performance by focusing and mobilizing stakeholders around common goals that are aligned to the business' priorities

Cohasset Associates | *Guiding the way to successful records management*

and resources. Stakeholders that include legal, compliance, IT, records management, and business process owners must collaborate to articulate the value of information over time, define and institutionalize the business rules and accountabilities that protect electronic records and which can be audited across all domains and architectures.

As the reliance on digital information and technologies increases in business and government, and the volumes and types of records continues to grow at an exponential rate, an evolution in the governance of enterprise information assets must begin in earnest. While there is no silver bullet for meeting the demands of legal/regulatory compliance and operational needs, the Assured Records Management methodology embraces the dynamic evolution of digital technologies because they offer better and more sustainable solutions for electronic records management. The ARM approach also depends on building a common understanding across disciplines and domains of what is required to achieve an "assured" level of recordkeeping, and management commitment to provide funding and resources to adapt records systems as business, technology and compliance requirements change over time.

Stakeholders in the organization's electronic records management success are encouraged to fill out the Current State Assessment checklist provided on the next page, and to use the results to begin to identify opportunities for increased retention and disposition controls.

7. Assured Records Management Self Assessment

1. Does your organization have an enterprise-wide Records Management (RM) program (policies, procedures, guidelines and retention schedules) that incorporates electronic records?

2. Has your organization identified how electronic records management fits into the overall information and technology management strategy(s)?

3. Does the organization have an effective stakeholder team working on the challenges of electronic records management that includes Information Technology (IT), computer security, Records Management, Legal, Finance, Audit/Tax, and business people?

4. Has your organization determined when and how electronic documents are classified as records, and who is responsible for their protection?

5. Has your organization determined where the electronic records repository (if a single location) will reside and who has responsibility for maintaining it?

6. Does your organization have a long term retention and disposition management program for electronic records?

7. Does your organization effectively use metadata?

8. Has your organization inventoried its electronic records?

9. Has your organization performed a cost/benefit analysis for electronic records management systems and technologies?

10. Has your organization addressed the cultural change issues associated with managing electronic records?

11. What resources (time, facilities, money, and people) are dedicated to your organization's electronic records management program?

12. Can your organization effectively 'freeze' or 'hold' records that are requested as part of a legal hold order, regulatory investigation or audit?

Organizations that fail this self assessment are at substantial risk and need to get moving on the road to Assured Records Management.

These questions have been adapted from the U.S. National Archives & Records Administration (NARA) Electronic Recordkeeping planning checklists for IT and Records Managers.

8. End Notes

1. 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 or in the transaction of business.

2. Throughout this document, the terms "organization" and "enterprise" are used to refer to companies, businesses, government agencies, institutions, associations and other entities conducting profit and not-for-profit activities.

3. Lyman, Peter and Hal R. Varian, "How Much Information 2003," is found at: www.sims.berkeley.edu/research/projects/how-much-info-2003/

4. The terms "Information Systems" and "Information Technology" (IS/IT) are used in the broadest context here in terms of hardware and software functions and roles that include software technologists, storage administrators, application designers, developers and managers, database administrators, systems control, etc.

5. Electronic discovery is the identification, location, retrieval, preservation, review and production of information in regulatory and civil matters.

6. The term "value-based" is used in this document to represent the outcome of an organization's records appraisal process, namely the evaluation of records on the basis of their operational, regulatory, legal, fiscal, or historical significance; arrangement; informational value; and relationship to other records.

7. A repository for electronic records, sometimes called "records archives," is a direct access devise on which electronic records and associated metadata are stored.

8. Dollar, Charles M. *Authentic Electronic Records: Strategies for Long-Term Access.* Chicago: Cohasset Associates, Inc., 2002.

9. Records Management is the planning, controlling, directing, organizing, training, promoting and other managerial activities involving the life cycle of information, including creation, maintenance (use, storage, retrieval) and disposal, regardless of media.

10. The 2003 Cohasset/ARMA/AIIM *Electronic Records Management Survey: A Call to Action,* can be downloaded from: www.merresource.com/whitepapers/survey.htm.

11. Examples include the Sarbanes-Oxley Act of 2002 (www.sarbanes-oxley.com/) and Healthcare Insurance Portability and Accountability Act (www.hipaa.org/).

Cohasset Associates | *Guiding the way to successful records management*

12. For a more detailed discussion, please read the Executive Summary of the Cohasset/ARMA/AIIM White Paper *Electronic Records Management Survey – A Call to Action,* which can be downloaded from: www.merresource.com/whitepapers/survey.htm.

13. Readers are directed to the International Standards Organization, ISO 15489 – Information and documentation – Records management, (parts 1 and 2).

14. Information Management Lifecycle (ILM) is the policies, processes, practices, services and tools used to align the business value of information with the most appropriate and cost-effective infrastructure from the time information is created through its final disposition. Information is aligned with business requirements through management policies and service levels associated with applications, metadata and data. This definition is from the DMF Dictionary found on the Storage Networking Industry Association website at www.snia.org.

15. International Research on Permanent Authentic Records in Electronic Systems, InterPARES 1 Project (www.interpares.org). Strategy Task Force - Intellectual Framework (Principles and Criteria).

16. Most notably the work of the governments of Australia, New Zealand, the United Kingdom, the Netherlands and the United States.

17. Electronic Records Management (ERM) practionners are advised to consult legal counsel and records management experts to determine how these general requirements apply to their organization and its legal and compliance obligations.

18. Confidentiality protection is required by some laws, such as HIPAA, and for certain administrative business records areas such as payroll and employee medical records.

19. Agencies promulgating these specific storage regulations are among those with the greatest regulatory visibility and include the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Nuclear Regulatory Commission (NRC). Electronic records management regulations from these agencies explicitly call for the use of a non-rewritable, non-erasable information recording process. This is commonly referred to as WORM (write once, ready many) functionality.

20. The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, Public Comment Draft 2004, Comment 5e. Readers are encouraged to visit: www.thesedonaconference.org.

21. Per the Enterprise Strategy Group as cited in 'Message Therapy,' January 15, 2005 issue, www.cio.com.