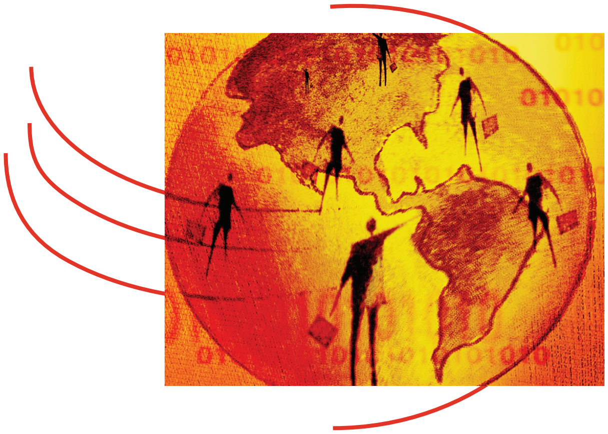


Collaboration

The New Standard of Excellence

SNIA
Data Management Forum

ARMA
International

Introduction

Defining the Collaborative Model

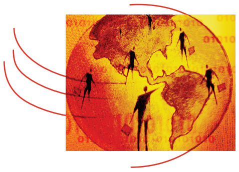
Escalating costs from compliance, legal, and security risk exposure, have created a critical need for organizational transformation and collaboration among records and information management (RIM), information technology (IT), and security professionals. The authors of this paper, ARMA International and the Storage Networking Industry Association (SNIA), have already embarked upon this collaborative process. These groups are working in tandem to establish ways to bridge the gaps between IT, RIM, legal, and security professionals. ARMA and SNIA understand and fully appreciate the contributions that each of these professional disciplines make to the organization and to achieving information management compliance.

ARMA and SNIA's goal is that the collaborative process evolving between the two associations will serve as a model for enterprises now needing to quell the impending chaos brought on by the convergence of regulatory and legal imperatives with the continued need for IT, RIM, legal, and security professionals to deliver competitive value to their business partners.

The role of professional and trade organizations includes anticipating environmental trends that will impact their members, professions, and industries, and providing guidance and education that will equip their stakeholders with the necessary tools and skills to remain marketable, competitive, and of value to their organizations and customers.

The notion of collaboration between the professional disciplines seems so simple, yet, in the real world may be politically difficult. We urge you to find a way to break down those barriers and cooperate. It is essential.

Collaboration between IT, RIM, legal, and security professionals is the new standard of excellence in managing records and information, enhancing organizational efficiency, mitigating risk, reducing operating costs, and ultimately providing organizations better value and return on investment.



Collaboration

The New Standard of Excellence

All organizations that own and use information are challenged by the convergence of legal and regulatory compliance requirements, the need to continually extract new business value from information, and simultaneously reduce risk. Failure to respond exposes the enterprise to lost productivity, lost business opportunities, and loss of reputation. The solution is the organization-transforming process of collaboration.

Collaboration engages the information owners, administrators, and operators in working together for the organization's cause. This community centers on four groups – IT, RIM, security, and legal professionals – working in tandem with business groups to map technology and best practices to meet business process requirements. Coordination across this community's disparate interests is a challenge to overcome. Thus, the collaborative process begins with an understanding of the professional strengths and requirements that all participants bring to the table, then moves to the establishment of a cooperative, actionable plan to address the organization's information management needs.

For example, through working together, teams can define organizational requirements, classify information, and then coordinate and implement appropriate information-based management methods and practices. Their charter is to establish an orchestrated, collaborative process, driving toward the goal of creating an organization in which the value and requirements for information define the operating practices.

For many organizations, managing risk has taken precedence over value creation. This often means that far more resources are dedicated to regulatory compliance, information security, and reducing exposure to legal discovery than to creating new solutions and implementing new processes that move the organization forward within today's highly competitive business environment. Collaboration offers a way to regain control and put new value creation back on an equal footing with managing risk. Organizations must do both to survive.

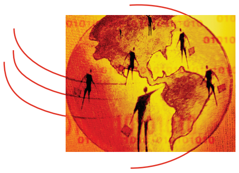
Convergence Is the Problem, **Collaboration** Is the Solution

Regulatory compliance, legal discovery, and security risks are compelling organizations to realize that enterprise information is both an asset as well as a potential liability. These drivers create powerful requirements for new business processes, new operations practices, and new methods for infrastructure management. Common to each of these new requirements is the need for collaboration across functional responsibilities. The convergence of business processes, operations, functional responsibilities, and infrastructure management around the value, risks, and requirements for information define a transition point for all organizations. The paradox is that many disparate operating groups now own a piece of the puzzle, whether these groups know it or not.

RIM and IT professionals must work collaboratively alongside security, legal, and business unit stakeholders to develop a holistic definition of requirements in order to mitigate risk, reduce operating costs, and achieve efficiencies. Beyond coping better with enterprise information as assets and liabilities, this collaboration creates new opportunities for business process innovation, increased profitability, and competitive advantage.

The Need for Collaboration

The current state of information management affairs within many enterprises ranges from highly complex to chaotic. Different groups within the enterprise need to come together to formalize the requirements and policies that can be extended to all information touched by the enterprise – both physical and electronic. Organizations face a complex problem in balancing legal and regulatory



compliance requirements for information with the need to continually extract new business value from information. The principle, ideally, is to reduce risk effectively.

Reducing Risk

Exposure of the organization's information to security, legal, or regulatory compliance violations can subject the enterprise to significant risk – risk that can be expressed in a number of ways :

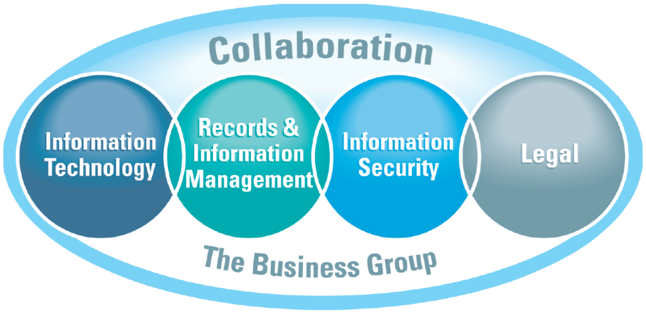
- Loss of strategic opportunities due to the inability to recognize or leverage valuable information
- Increased costs of doing business from inefficiencies related to difficult-to-locate or inaccessible data
- Inability to retrieve and productively use business critical information on a daily or historic basis
- Failure to comply with statutory or regulatory retention and destruction requirements
- Reduced ability to comply with court orders and other litigation-related imperatives requiring access to existing information
- Inability to respond promptly to government inquiries
- Regulatory fines and penalties
- Increased consequential costs of civil litigation including legal fines, adverse inference instructions, default judgment and civil contempt
- Vicarious liability for responsible senior management
- Criminal liability for organizations and individuals

Indeed, failure to properly manage stored information has become fodder for the evening news. Simple violations such as lost and misplaced tapes have cost large corporations billions of dollars in court judgments, litigation fees, and damaged corporate images.

Reducing Cost

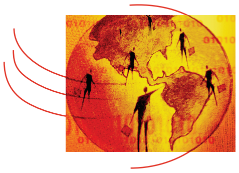
It is now quite common to find enterprises that are without a comprehensive information management strategy. It is also not surprising that they are struggling in the face of relentless information growth and rising costs. How do you cope with information growth of 50% or more per year and compliance rules that require long-term retention? Without collaborative leadership, some enterprises choose to keep all information "forever," while others purge and delete without a structured set of retention and disposition policies. This paradox creates three escalating cost pressures:

1. The cost of storage hardware and management application software to meet these new demands is escalating significantly within enterprise IT operations. This escalation is taking place in spite of the fact that the cost of raw storage capacity continually decreases on a per GB basis.
2. The cost to own and operate the required computing and storage infrastructure escalates even more rapidly. These costs include but are not limited to human resources, power and cooling, computer room floor space, and cost of capital.
3. To these costs, add the costs of mitigating risk exposure, inefficiency, and lost business opportunity already identified.



The increasing volume of electronic information with its increasing compliance, legal discovery, and security risks compels organizations to have appropriate records retention and disposition methodologies in place. Electronic storage without records and information management practices and requirements cannot produce successful results. Similarly, RIM practices without robust IT automation and storage system capabilities cannot fully meet retention needs.

Taken in total, the responsibility for managing and coping with information retention costs over the long term are a burden that is owned by the organization. Therefore, it behooves all stakeholders to collaborate on controlling these costs and risks. IT professionals cannot and should not try to automate information management and retention processes in a vacuum. They must have guidance and input from RIM professionals along with advice from corporate



attorneys and security officers and requirements from the business. RIM professionals can provide the principles and practices for the records management and retention, and IT can assist in automating these processes.

What Does Collaboration Look Like?

> ***Collaboration will require the establishment of a team led by RIM and IT professionals. However, this team must recognize the strengths that all stakeholders – including legal and security professionals – bring to the collaborative process.***

Successful information-based management practices now require a new type of collaboration as information owners and administrators work together to understand and classify the business value and requirements for information. The collaborative process should be lead by IT and RIM professionals with the advice and support of legal and security professionals. However, it is recommended that the process begin with providing all participants with an understanding of the professional strengths that each brings to the table. The following discussion highlights these strengths.

IT Professional Strengths

Hardware/software infrastructure expertise – Non-IT professionals usually have an understanding of how systems operate. However, presenting IT services to all interested parties in the information management process is the primary responsibility of IT professionals.

It is IT's job to enhance the value of the enterprise via new applications delivery as well as translate business requirements into technology that delivers the required services to business users. The definition of what services are required and the justification for needing them, however, lies in the hands of the business stakeholders. Additionally, there must be a level of trust between IT and business stakeholders. A collaborative process between IT and RIM professionals can be built upon mutual trust as well.

Acquiring the necessary infrastructure components and matching systems to the needs of the business also has traditionally been the responsibility of IT. These decisions increasingly are being made within the enterprise with input and advice from non-IT employees – in this case RIM professionals, legal counsel, and security officers. IT brings additional expertise to the table in building financial justification models for information management solutions, such as total cost of ownership and return on investment.

Finally, as the relationship between IT and RIM professionals continues to evolve, IT professionals will be called upon to help explain information management technology and project implementation to the whole enterprise.

Ability to automate processes – IT professionals understand how to automate business processes. Indeed, business process automation has long been a cornerstone of the IT value proposition.

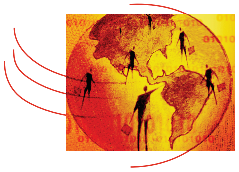
Understanding of performance issues – IT professionals understand how to deliver a consistent quality of IT services to users. In fact, most IT operations managers must now regard their operations centers as information "utilities" in order to satisfy a spectrum of user demands that ranges from corporate executives to remote users and customers/suppliers outside the enterprise firewall. IT professionals are sensitive to the fact that care must be taken to ensure consistent performance levels when automated records management software is layered on top of existing user-facing applications.

Ability to manage availability and integrity of electronic information – Data availability, protection, and integrity traditionally have been IT responsibilities.

RIM Professional Strengths

Records and information management best practices – For decades, RIM professionals have worked in the establishment of numerous standards, best practices, and guidelines for managing records throughout their lifecycle – from creation to disposition, regardless of media type – in order to meet legal, regulatory, and knowledge management and preservation requirements.

It is RIM's job to manage the records aspects of information created and received by the enterprise by working with various stakeholders to define what types of records are critical elements of business processes and translate this knowledge into a managed, sustainable, auditable records management process. The identification and capture of records metadata and resulting records taxonomies is a core competency of RIM and a strength that IT professionals share in IT-led projects of knowledge management categorization and taxonomies for enterprise searching.



RIM professionals have long held symbiotic partnerships with legal counsel within their organizations, as the laws governing operations across international, federal, state, and local jurisdictions all influence enterprise records management policies, procedures, and systems. In particular, should courts or investigating bodies issue litigation or preservation hold orders, legal counsel relies on RIM staff to implement legal hold processes that halt records disposition processing so as to preserve records that could be identified as evidence.

Building, managing, and enforcing records retention policies has traditionally been the responsibility of RIM professionals in conjunction with legal counsel, but success in effective management of both electronic and physical record types requires a partnership with IT and security experts. As these relationships continue to solidify, RIM professionals will be asked to identify the records requirements aspects of information processes as emerging record types, media types, and legal constraints evolve.

Organizational records policies – Policies are governed by processes that have been established over time by many contributing professionals within the organization, including legal counsel and security staff. Policies are successful when they are governed by processes. RIM professionals are best positioned to translate RIM requirements, processes, and principles for their IT and legal counterparts.

Governance and compliance – Organizational governance programs are traditionally directed by records management offices and legal counsel. This team also leads the charge in evolving compliance initiatives, bringing together other stakeholders and business units in the effort to map business process to compliance requirements.

Data retention schedules – There are more than 900 regulations in the United States alone that control records retention periods – electronic and otherwise. Both records management and security professionals have an awareness of the breadth of the regulatory environment.

Record interrelationships – Separate and discrete records can be related to one another via many different circumstances and RIM professionals have a critical awareness of these interrelationships. Factors that must be considered include:

- The business reasons that caused the creation of a record set
- Security level
- Confidentiality of customer data
- Confidentiality of employee data
- Authorized usage
- Regulatory requirements
- Contractual agreements

While IT and RIM professionals may be the two primary groups that must work together, forming a leadership team, the business and financial stakeholders plus the legal and security professionals also play a critical role in making essential contributions to the collaborative process.

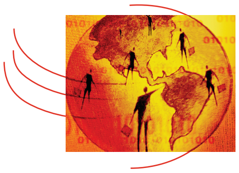
Legal Professionals

All aspects of the enterprise are visible to corporate legal counsel, who can also enforce policy declarations once they are formulated and adopted. Therefore, legal professionals are critical resources when it comes to defining organizational policies and procedures, particularly those governing records and information management. Areas of responsibility fall into three different categories:

- Communications standards – the definition of protocols for modes of communication both within and outside the enterprise. This would include a definition of mediums for formal and casual communication, as well as how to present oneself within and outside the enterprise.
- Legal retention – establishing retention schedules for specific types of records as well as other content not defined as records (drafts, reference materials, etc.) in order to meet federal, state, local, industry, and best-practice guidelines.
- Legal hold. – establishing rules for the use of mechanisms that suspend all activity on certain records in the event of pending litigation or investigation.

In addition, legal professionals are aware of the expanding U.S. and international laws regarding personal privacy and the management and disposal of personal information. This capability will become increasingly critical over time as state and federal governments draft legislation aimed at controlling personal identity theft. A number of U.S. states, including California and New York, have already enacted such legislation, with dozens of states currently drafting it as well.

Legal professionals should also be consulted on policy and procedural issues regarding legal discovery, content creation and distribution, email, Internet usage, and compliance.



Security Professionals

Along with legal counsel, security professionals have experience in dealing with privacy issues, record tampering by corporate employees, international laws regarding the retention and dissemination of personal information, Sarbanes-Oxley, non-disclosure agreements with business associates, and the security risks inherent in the absence of detailed data retention schedules.

Electronic messaging is an example of an area where security professionals can offer critical insight. Email and other forms of messaging (instant messaging, for example) pervade the business environment. Email is now viewed as a business-critical application. Nevertheless, it also is abundantly clear that email poses a significant security risk. Security professionals are keenly aware of this risk and consequently have become messaging experts, aware not only of how sensitive records can appear outside the corporate firewall, but how email-bearing viruses and malware can wind up on corporate systems.

Security professionals also are aware of the transient nature of email ownership. The ability to copy and forward messages with a mere mouse click allows both messages and attachments to proliferate, creating an additional burden for RIM and IT professionals alike who are tasked with email management.

Establishng Best Practices

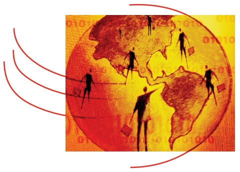
Next, the leadership team should establish a number of best practices for the organization. These range from establishing guidelines for how the members of the collaborative process work together, to agreeing on uniform methodologies. The following list is not to be considered complete and exhaustive, rather it is a starting point on which each organization can expand.

- *Corporate information policy formulation* – Information policies cannot be established in a vacuum or by a single group within the enterprise; it is a collaborative endeavor involving all stakeholders. Compliance and governance initiatives are excellent and requisite opportunities for collaborative partnerships to develop, educate, and better meet policy requirements.
- *Process automation* – Information-policies that have been formulated as a result of the collaborative process can be translated to a series of business automation processes.
- *The tools to implement and measure conformance to information policies* – The collaborative team drives operational requirements, forms the policies that serve as governances over these requirements, and translates policies into processes with supporting management tools. All parties have a resulting stake in putting those tools into daily practice and monitoring the results.
- *Identification of all information and records repositories* – Organizations are struggling to manage the proliferation of information across the entire organization and need a contribution from all stakeholders to identify all information and records repositories, their contents, and their value and relationship to business processes.
- *Creation and capture of business-related metadata* – The capture of business-related metadata is a critical part of the information lifecycle process, with all parties invested in the who, what, when, why, and how of the metadata capture process.
- *Shared responsibility with regard to risk* – It is critical that all stakeholders acknowledge and understand the risks attached to records. Records originating from both within and outside the enterprise, and formal and informal records of all electronic and physical media types, must be assessed for their value as records as well their risk potential. Specific, measurable actions should be outlined when records are stored, retained, moved, or destroyed.
- *Records integrity and authenticity* – All parties in the collaborative team may be called upon to represent certain electronic records as unmodified since their creation. It is the job of all stakeholders to guarantee the integrity and authenticity of information as required and to put in place tools to aid in this process.

Creating Change in Your Organization

The convergence of business processes, operations, functional responsibilities, and infrastructure management around the value, risks, and requirements for information define a transition point for all organizations affected by these drivers. The organizational paradox is that many disparate operating groups now own a piece of the puzzle. To solve it, they have to collaborate.

Teams lead by IT and RIM professionals, with support from security, and legal professionals finally have the opportunity to work together and collaboratively solve huge problems that plague the organization. Collaboration is the new standard of excellence.



What are the benefits? Collaboration offers a way to regain control, and a way to put new value creation back on an equal footing with managing risk. It is the first step in using new information-based management methods that will:

- Establish, instrument, and automate operations based on the requirements for information
- Fully comply with regulatory mandates plus reduce security and legal risks
- Reduce cost of operations and reduce complexity
- Successfully implement efficient methods to preserve an organization's important records under the onslaught of overwhelming information growth, globalization, and complexity
- Improve the overall quality of IT services delivered to the corporation

Join with ARMA International and SNIA as we collaboratively educate and encourage our constituencies to proceed down the path of collaboration within their organizations. Start by getting your peers together and identifying and classifying the requirements for your critical information assets.

This paper was produced by the collaborative efforts of teams from ARMA International and the SNIA's Data Management Forum.

Authors
ARMA International:
Susan Avery – Senior Strategic Advisor
Michele Kersey – Chair, ARMA International Technology Advisory Committee
Fred Pulzello – Treasurer, ARMA International
SNIA:
Michael Peterson – Program Director of the Data Management Forum
Edgar St. Pierre – Co-Chair, ILM Initiative, Data Management Forum
Larry Cormier – Vice-Chairman, Data Management Forum
Data Mobility Group: John Webster and Joe Martins – Principle Analysts
Data Mobility Group acted to coordinate production of this paper

About ARMA

ARMA International is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. For additional information, visit *www.arma.org*.

About SNIA

The Storage Networking Industry Association (SNIA) is a not-for-profit global organization, made up of more than 460 member companies and close to 7,000 individuals spanning virtually the entire storage industry: vendors, application developers, integrators, and many "end-user" professionals. SNIA's Data Management Forum is focused on delivering standards and educational services for data management and information lifecycle management (ILM). To learn about the information-based management practice we call ILM and its related data services, visit the DMF's site at *www.snia-dmf.org*, and SNIA at *www.snia.org*.