# Information Nation

# Praise for *Information Nation*

Kahn and Blair have managed to craft into one superb, readable book the information both the novice and specialist need to create an effective Information Management Compliance program. *Information Nation* is one of the best resources on compliance, in any risk topic, that I have ever read.

*Win Swenson, Former Deputy General Counsel and Chair of the Organizational Guidelines Working Group, U.S. Sentencing Commission; Partner, Compliance Systems Legal Group*

Managing information to support compliance is a monumental challenge for business and IT professionals today. This book provides straightforward guidelines to help them meet this challenge.

*David B. Wright, President, LEGATO Software*

A practical roadmap for implementing a successful compliance program. It completes the picture on information use in commercial enterprises by laying the foundation for good corporate governance, now a key strategic initiative for competing in today's global business environment.

*Andy Lawrence, Eastman Kodak Company, One of Business Ethics "100 Best Corporate Citizens for 2003"*

Many companies overlook the importance of data management. *Information Nation* is a wake-up call that reminds us all that improperly managed information is a huge liability. The book is a great starting point for those that are just beginning to put a policy in place, and for those experienced individuals who are interested in performing a reality check on their existing Information Management Compliance methodology.

*Paul Butticaz, Vice President, SunTrust Robinson Humphrey*

At a time when there is a pressing need to improve the way information is managed, Kahn and Blair's message and methodology are right on. This book is much more than a "must read." It is a "must do" action plan for achieving compliance and mitigating risks in today's new world.

*Robert F. Williams, Cohasset Associates, Inc.*

*Information Nation* provides practical advice, based on real-world examples, for anyone faced with the formidable task of developing and maintaining an effective Information Management program. An easy to read volume, packed with useful information designed to assist the legal professional or corporate manager in implementing efficient and legally sound policies and procedures.

*Candace S. Erisen, Counsel, Cinergy Services, Inc.*

One stop shopping for everything you need to know about Information Management Compliance. *Information Nation* covers the gamut of legal issues and the business risks with comprehensive analysis and advice in plain English. For an issue of increasing importance to businesses, you won't find a better work under one cover.

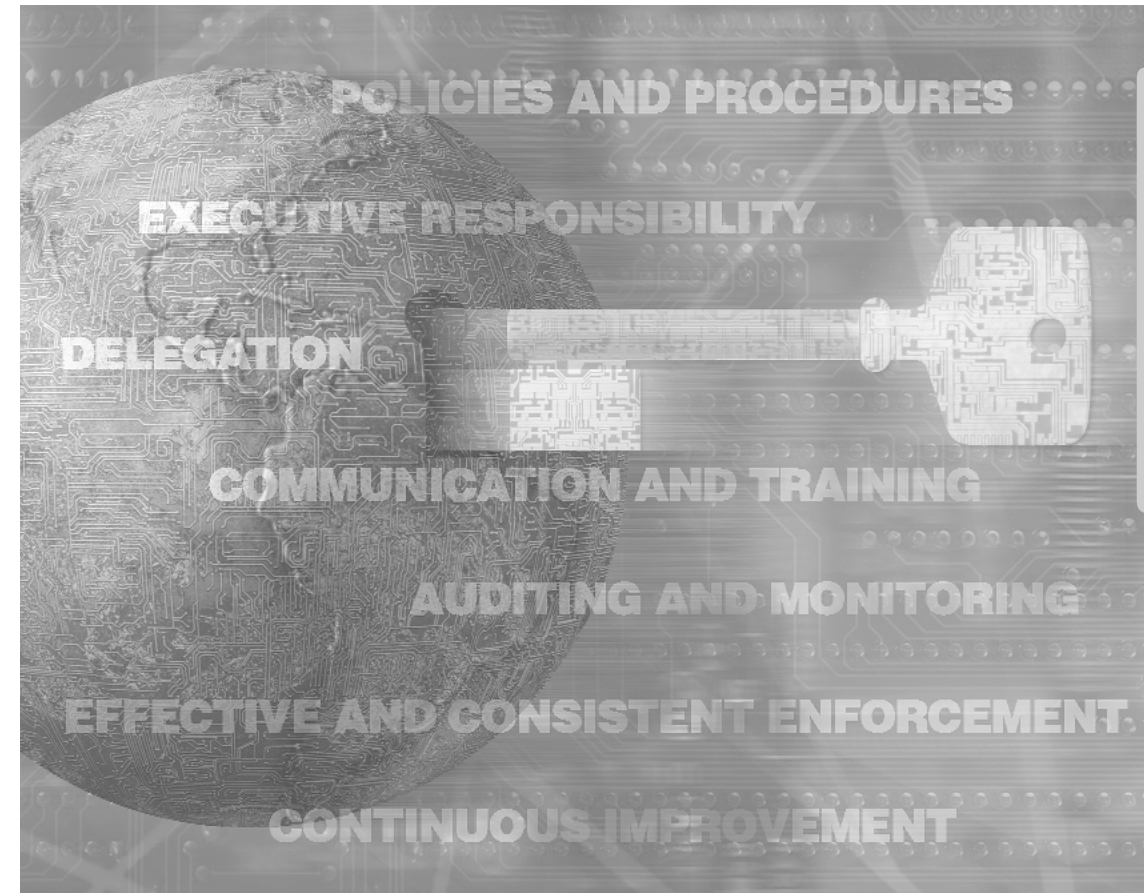*Marc Martin, Of Counsel, Kirkpatrick & Lockhart, LLP*

IMC is rapidly evolving into a paramount issue for organizations to address NOW. *Information Nation* is an excellent resource for technology management executives and professionals in understanding the inherent vulnerabilities of existing information management practices and implementing appropriate safeguards for the future.

*Evan Wagner, Network Design and Security consultant*

## Other Books from Randolph Kahn

*E-Mail Rules: A Business Guide To Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication*

# INFORMATION NATION

POLICIES AND PROCEDURES

EXECUTIVE RESPONSIBILITY

DELEGATION

COMMUNICATION AND TRAINING

AUDITING AND MONITORING

EFFECTIVE AND CONSISTENT ENFORCEMENT

CONTINUOUS IMPROVEMENT

# Seven Keys
to Information
    Management
    Compliance

**aiim**

**Randolph A. Kahn, ESQ. and
Barclay T. Blair**

**Randolph A. Kahn, ESQ.**

In loving memory of my mother
Lillian Kahn.

To my family,
Melissa, Dylan, Lily, and Teddy
who make life such a joy.

Special thanks to the
Kahn Consulting team and
our clients, partners, and friends.

**Barclay T. Blair**

To Margie.
To Brian.
To Randy.
To Farnese.

# Contents

# Forward

*by Jay Cohen, ESQ.*

Time and time again, Information Management Compliance failures have proven to be devastating. Companies flounder, and some go away altogether. Customer confidence is shaken and business is lost. Laws are broken, data is not protected, and systems are overburdened. Organizational mismanagement of information is far too common-place today and we are now reeling—trying to figure out what to do next.

The time has never been better for a book like *Information Nation: Seven Keys to Information Management Compliance*. It is a unique and practical guide for IT professionals, business executives, lawyers, records managers, and compliance officers on how best to manage information according to a disciplined methodology that will minimize organizational risks and failures.

These are not sentiments that can be applied to many books. But, *Information Nation* is no ordinary book. It provides the clearest, best organized, and most useful means of addressing the considerable challenges posed by a whole host of information management issues. Issues that we now know can threaten an organization's very existence, especially if the warnings and lessons in this book are not understood and heeded.

No matter your position at your organization, or the current stage of your Information Management efforts, this book will provide you with practical steps for better protecting your organization's business and legal interests. If you don't have an Information or Records Management program today, this book will help you create and implement a comprehensive approach that will work for your organization, day in and day out. If you already have an Information Management program, this book will enable you to measure your program's effectiveness and mitigate risks.

Organizations with inadequate Information Management programs are equally in need of Kahn and Blair's extraordinary skills, expertise, and advice as are those that have no program at all. I for one learned the hard way that failing to have a compliant Information Management program can be devastating.

Let me draw on that personal experience to illustrate the point.

I first met Randy in 1997, when I was a compliance officer at a previous firm—a large, multi-national institution. Our organization—perhaps like yours—had a records retention program, complete with policies and procedures, retention schedules, a thick binder, and even a warehouse or two where we stored boxes of paper files. Like most companies these days, we were defendants in a lawsuit and, in connection with that lawsuit, we were asked by the court to "retain all records and other information" that might be relevant to the controversy (such a request is routinely made in just about every lawsuit). Our company sent out notices to all employees, in accordance with the Records Management policy, reminding them to comply with that "preservation order." The job was done, and we could rest assured that the organization was protected.

Not exactly.

That is where my company stood when I got a call at home on a Sunday in December, to report to headquarters. It turned out that a few employees had destroyed paper and electronic records that were "relevant" to the lawsuit—and it hardly mattered to the court that this destruction may have been innocent or negligent, rather than intentional. The point was that the information was gone, and the court wanted to know what the most senior executives of the company had done to prevent the destruction. The court asked a series of questions—both about our program in general and about its application in this case—indicating its view that our responsibilities went well beyond just having a policy and issuing a notice.

We were forced to ask ourselves many painful questions:

- Who was responsible for the Records Management program in our organization?

- How and when had we communicated with our employees about the program?

- What had we done to train employees about the program, and what would happen if they failed to comply?

- What had we done BEFORE the preservation order was issued to assure that relevant records were around to be retained?

- Did the program incorporate electronic records, as well as paper files?

- How did the company ensure that employees were complying with the policies and program requirements?

- Had there been any audits, compliance reviews, or similar efforts?

- What did the company do to ensure that the preservation notice in this matter was received, understood, and complied with by each and every employee throughout the organization?

- What, if any, follow-up communication was undertaken?

- Could we identify and locate ALL of the relevant information that was needed?

- Did we have, and implement, a process to quickly investigate and respond to instances of non-compliance?

- How did we document compliance with the program in general, and with the specific retention request at issue?

We could not, unfortunately, provide satisfactory answers to ALL of these questions. As a result, the court converted the destruction of documents by just a couple of individuals into an ORGANIZATIONAL failure and responsibility. The resulting institutional damages—in fines, administrative and litigation expenses, and loss of reputation—far exceeded the value of the lost documents. That is what you want to avoid, and to do that you need to start now.

This book is by far the best resource that I know of to help you take on the complex challenge of managing your information assets. It is the only resource I have seen that is organized around the kinds of questions that courts, regulators, and prosecutors are going to ask, and that provides the answers they expect. The methodology advanced by *Information Nation* is a compliance framework that can be applied to all Information Management activities, and will tell the

courts, regulators, stockholders, executives, boards, and the public that you take your Information Management responsibilities seriously.

And if you already have a problem with Information Management, *Information Nation* and the authors can help you resolve it. Mr. Kahn came to our rescue during a critical time in our company's history. With his help—and in far less time than anyone thought possible—we built and implemented a nationwide Information Management Compliance program (not just a record retention policy) that the court accepted and that our company could be proud of.

I have had occasion to work with Randy, Barclay, and the rest of the Kahn Consulting team on a number of projects since this experience. They represent the rarest combination of technical knowledge, business acuity, legal skill, and practical experience, and that wisdom and experience come through on every page of this important work.

In my own experience as a compliance executive, I have come to view organizational compliance efforts as trying to accomplish two things: first, to make it as least likely as possible that individuals in the organization will violate their legal and compliance responsibilities; and second, to ensure that if someone does violate that trust, it is viewed as an individual and not an organizational problem, because of everything that the organization has done to address the first goal. This book gives you the tools to accomplish both goals when it comes to Information Management Compliance.

> Jay Cohen, ESQ.
> *Chief Compliance Officer*
> The Mony Group

# Preface
*by John F. Mancini*

Welcome to the world of Information Management Compliance!

AIIM International conducts frequent surveys to analyze trends within the Enterprise Content Management (ECM) industry and to identify issues and best practices related to the application of ECM technologies. Recent surveys have revealed several themes that highlight the critical need for *Information Nation: Seven Keys to Information Management Compliance:*

- The fundamentals of business documentation—the processes by which organizations prove what, when, who, why, and how they conduct their operations—have been turned on their head in the past five years.

- Electronic information has become the dominant means to document business processes.

- The amount and complexity of electronic information that must be kept to document business processes is increasing exponentially *by the day*. So too is the sophistication of those who challenge organizations based on the vulnerability of their electronic information.

- Most organizations have not recognized the scope of the change that has occurred, and are thus facing cascading risk and liability within their organizations.

In fall 2003, AIIM and Kahn Consulting surveyed over 1,000 individuals on their email management capabilities. What we found is that most organizations clearly rely on email to do business. For example, 84% use email to discuss operating and product strategies. Seventy-one percent use email to negotiate contracts. Sixty-four percent use email to convey confidential information. However, despite using email for such sensitive and valuable business activities, few organizations apply even the most basic disciplines associated with prudent records management to their email system. When asked, "Do you have a policy that outlines where, how, and by whom email is

retained?" only 36% reported this basic level of competency. And email is only a part of the problem. The same patterns and vulnerability exist for all forms of electronic information. The volume of this information is staggering—there is currently more information on the hard drive of a typical computer than can be read in a single lifetime—and current controls are marginal.

What is to be done about this? I think this book provides important lessons to help organizations address the Information Management Compliance problem. I believe the key is to recognize that the solution lies in striking the right balance between two often-conflicting demands—the demand for greater operational efficiency and the demand for improved compliance and standardization.

The technology of information management increasingly enables organizations to do things better, faster, and cheaper. At the same time, 90% of the information that organizations must manage is unstructured—information that does not neatly fall into the rows and columns of a traditional database. Moreover, unstructured information is at the heart of business processes. And processes cannot be standardized and improved until this flow of information is standardized, digitized, and managed. So, within organizations there is a constant push to rapidly deploy technologies to reduce costs and improve processes. This is a world populated by the IT departments and line-of-business managers within organizations.

At the same time, governments and courts at all levels—local, state, federal—are making increasing demands for the trustworthiness, accuracy, and reliability of electronic information. There is a temptation to think of this as just a "Sarbanes-Oxley problem" or a "HIPAA problem." But I believe this is part of a long-term trend toward defining what transparency and accountability of organizations means in an electronic era. This is creating a need to reduce the risks associated with management of electronic information. This is creating a need to more clearly define and measure the processes associated with management of this information—a roundabout way of saying a need for greater "compliance." This is a world often defined by the legal, risk management, and compliance departments of organizations.

This book pulls together these often-conflicting worlds of information management and compliance and defines a framework for looking at them *together*. The only way organizations can handle these conflicting demands is by looking at them through the prism of *Information Management Compliance*. It is no longer enough to simply automate a single department's processes, independent of the broader information management structure within organizations. It is no longer enough to assume that "someone" down in the organization will be responsible for the management of electronic information critical to documenting the business; the courts will hold the CEO accountable in the end. It is no longer enough to implement technology without a framework of policies and procedures—and a means to educate employees on those policies and procedures and to hold them accountable.

These issues will not be solved overnight. This book takes enormous strides toward defining the seven key steps to get organizations started down the path of 21st century accountability and responsibility. AIIM is proud to be a part of bringing this critical message to the public.

> John F. Mancini
> *President*
> AIIM

## Author's Acknowledgements

Many of our friends and colleagues contributed to this book by volunteering their valuable time to review and comment on the manuscript. For this we wish to extend our thanks to:

Andy Lawrence, Ben Wilson, Candace Erisen, David B. Wright, Evan Wagner, Jay Cohen, Jeanne Caldwell, Marc Martin, Michael Power, Paul Butticaz, Robert F. Williams, and Win Swenson.

Also, thanks to James Hospodarsky for his valuable contribution on Change Management. Special thanks to David M. Freedman for his editorial contribution.

# Introduction:

## Welcome to a New Era of Information Management

*It might be useful to consider reminding the [Enron] engagement team of our documentation and retention policy. It will be helpful to make sure that we have complied with the policy. Let me know if you have any questions.*[1]

Email from Nancy Temple, Arthur Andersen in-house attorney, October 12, 2001

Under normal circumstances, an email message like this might be considered innocuous, or even commendable. All companies should regularly remind employees of their records retention policies (which typically include records disposal guidelines). However, in Arthur Andersen's obstruction of justice trial, the public learned that Andersen had destroyed numerous documents and email messages related to the SEC's ongoing investigation of Enron. In this context, a seemingly innocuous email "reminder" about the company's retention policy was perceived to be a smoking gun.

By the time a jury found Andersen guilty on one count of obstruction of justice in June 2002, the firm had shrunk by 17,000 employees in the U.S. and had lost 30% of its public company clients.[2] After its conviction in June 2002, Andersen is no longer in the auditing business, was fined $500,000, and put on five years of probation—the maximum penalty under the law. (See Chapter 4 for an in-depth discussion of the Andersen case.)

The case of Andersen raises many interesting questions. Could the document destruction have been prevented? Were there flaws in their Information Management program that helped precipitate the company's downfall? What could its leaders and its lawyers have done differently? And, perhaps most importantly, why did the entire company go down, and not just a small group of accused wrongdoers?

The U.S. Congress, for its part, responded to Andersen's conviction and the seemingly endless parade of corporate scandals of the same era by passing new laws and regulations that have sent ripples (or perhaps tidal waves) through corporate America. One of these new laws was the Sarbanes-Oxley Act of 2002, a complex law that addresses many issues that have an impact on Information Management.

> Many companies, of course are retooling to meet the demands of the federal Sarbanes-Oxley Act. As the string of corporate scandals unfolded at companies including Enron Corp. and WorldCom, Inc., Congress moved last year to revamp the way boards and company officials run their business and disclose information.
>
> *How One Firm Uses Strict Governance To Fix Its Troubles,*
> Wall Street Journal, *August 21, 2003*

So began the new era of Information Management. An era where properly managing records and other information have become inextricably linked with corporate accountability and transparency, which in turn has become connected to fiscal health and stock market valuation. An era of new expectations, new regulations, new laws, new technologies, and new challenges.

## Information Management Compliance

However, this is not a book about Andersen, Enron, WorldCom, Tyco, ImClone, or any of the other high-profile cases where there have been accusations, charges, and/or convictions for improper use and management of company information (although we will examine some of these and other cases in detail). This is a book about changes in the Information Management landscape, resulting largely from cases like these and dozens of lower-profile cases. Most importantly, it is about how we can learn to avoid similar problems in our own organizations by developing and implementing Information Management Compliance programs that anticipate problems and take advantage of opportunities.

This is a book about approaching all types of Information Management activities with a new methodology, one that adopts the principles, controls, and discipline upon which many corporate compliance programs are built. While the world of records destruction is the starting point for our exploration, the book examines a broad range of Information Management activities that serve both legal and business needs, and are central to your organization's ongoing success.

This is a book about Information Management Compliance (IMC), which involves:

1) Developing Information Management criteria based on legal, regulatory, and business needs; and,

2) Developing and implementing controls designed to ensure compliance with those policies and procedures.

The first six chapters of this book define and explore the concepts of Information Management, Records Management, IMC, and the business and regulatory environments that we operate in today.

In the second part of the book we present the Seven Keys to Information Management Compliance—this is the practical, action-oriented part of the book. These Seven Keys are:

1) Good policies and procedures

2) Executive-level program responsibility

3) Proper delegation of program roles and components

4) Program communication and training

5) Auditing and monitoring to measure program compliance

6) Effective and consistent program enforcement

7) Continuous program improvement

As a model for these Seven Keys, we used a section of the Federal Sentencing Guidelines ("Guidelines").[3] The Guidelines are used by the federal courts to determine the appropriate punishment for individuals and organizations that violate the federal law. For many years, numerous companies have used the Guidelines to build general corporate compliance programs. However, until now, the Guidelines have generally been overlooked as a source of guidance for Information Management. The time has come to apply the compliance methodology outlined by the Guidelines to Information Management.

In this new era, Information Management requires a proactive approach which recognizes that legal protection *and* business value will result from taking a formal, disciplined, visible, funded, and sustained approach—an approach that begins with an understanding of how an organization's Information Management activities are likely to be judged by the courts, regulators, auditors, and its own executives and shareholders.

IMC is about more than making sure information is not destroyed due to the malicious or inadvertent acts of a few employees. Rather, it is a holistic approach that covers many areas of concern, including:

- Storage management

- Privacy

- Business continuity and disaster recovery planning

- Records management

- Information security

- Transaction management

- Application development and integration

- Technology purchasing and acquisition

- System configuration and management

- And many other areas

We wrote this book for a broad range of readers who have an interest in Information Management issues, with a specific focus on readers who have direct or indirect responsibility for making sure that information is properly used and managed in their organizations. The sphere of people who have some responsibility in this area seems to grow every day, now encompassing everyone from the CEO who needs to sign off on financial reports in accordance with Sarbanes-Oxley; to the IT professional wondering how back-up tapes should be managed; to the compliance officer trying to ensure compliance with emerging privacy laws; to the administrative assistant just trying to decide what to do with all the email messages that his boss has asked him to print out and file; to the lawyer guiding the company through troubled legal waters.

Information Management encompasses management, administrative, operational, technological, human resources, Records Management, legal, and many other areas of an organization. The Seven Keys to IMC that we advance are designed to help professionals in each of those areas understand their responsibilities and what they must contribute to their organization's Information Management efforts.

# PART 1

**Laying the Foundations of Information Management Compliance**

# Chapter 1:

## Why Information Management Matters

*In this first chapter we will explore the concept of Information Management, how it has changed over time, and how it relates to other information-based activities across an organization. Understanding the essence of Information Management will lay the foundation for understanding IMC.*

## Sink or Swim

In 2003, 800 megabytes of new information was created for each man, woman, and child on the earth—with 92% of it stored on magnetic media, primarily hard drives.[4] Businesses worldwide today use more than 300 million desktop computers that together have the capacity to store 150,000 terabytes of information.[5] The number of email messages sent per day will grow from 31 billion in 2002 to 60 billion by 2006.[6] Roughly 250 billion text messages were sent worldwide using wireless devices in 2001,[7] and business users are expected to make up nearly half of the 500 million people that will be using Instant Messaging by 2006.[8]

Information technology has become so commonplace in today's organizations that much of it is taken for granted. Some observers have even suggested that information technology and automation no longer offer "competitive advantage" because each competitor has essentially the same technology and level of automation.

From the largest Enterprise Resource Planning application in use at a corporation with thousands of employees around the globe, to the tiny credit card-size cell phone used by the independent consultant down the street, there are an ever-increasing number of software applications and hardware devices creating an ever-increasing amount of information. Information that must be sent, received, captured, accessed, stored, indexed, published, and so on. Put simply, information that must be managed.

The need for effective Information Management has never been greater.

## What Is Information Management?

In the 1970s, the U.S. government commissioned a report that looked at the way government agencies were using information.[9] This report helped to popularize the concept of Information Management. The commission was concerned with both paper and electronic information and the way it was being managed through such diverse activities as library management, microforms, and word processing.

Over the ensuing decades, the term Information Management has come to be used in different ways by a number of groups, as the following definitions illustrate.

### Selected Definitions of Information Management

The application of management principles to the acquisition, organization, control, dissemination, and use of information relevant to the effective operation of organizations of all kinds.

'Information' here refers to all types of information of value, whether having their origin inside or outside the organization, including data resources, such as production data; records and files related, for example, to the personnel function; market research data; and competitive intelligence from a wide range of sources. Information management deals with the value, quality, ownership, use, and security of information in the context of organizational performance.

*International Encyclopedia of Information and Library Science*[10]

■

The proper organization and appropriate control of information transmitted by whatever means and including Records Management.

*Comparative Glossary of Common Project Management Terms*[11]

■

The administration, use, and transmission of information and the application of theories and techniques of information science to create, modify, or improve information handling systems.

*Environmental Protection Agency*[12]

■

An imprecise term covering the various stages of information processing from production to storage and retrieval to dissemination towards the better working of an organisation; information can be from internal and external sources and in any format.

*The Society for Information Management (UK)*[13]

## Changing Times, Changing Terms

As business practices and technologies have evolved, so too have the theories about Information Management. Like others working in fields where information technology had provided a radical transformative force, Information Management professionals and their industry groups have worked to stay ahead of the curve.

For example, AIIM International started life in 1943 as the National Microfilm Association, later became the Association for Information and Image Management, and today focuses on enterprise content management (ECM).[14] ECM is a vision of Information Management that refers to several related categories of information technology and processes including:

> content/document management, business process management, enterprise portals, knowledge management, image management, data warehousing, and data mining.[15]

ARMA International, an industry association for Information Management professionals, defines the activities of their members as "recorded information management" (RIM),

> a specialized field of information management that is concerned with the systematic analysis and control of operating records associated with business activities.[16]

ARMA has also theorized that the future of RIM is SIM—Strategic Information Management,

> that body of knowledge comprised of skills that will enable professionals and their organizations to make well-informed decisions resulting in a distinct competitive advantage in the business world. It draws upon skills from records and information management, information technology, and strategic management.[17]

One of the most recent buzzwords in the Information Management world is "information lifecycle management" (ILM), which refers to the use of a combination of procedures and technology to managing an organization's information flow. Like many of the other terms used today, ILM is partly an old concept in a new wrapper, as the "lifecycle" approach to managing information has long been a central tenet of Records Management.

Part of the reason that terms like ILM, RIM, SIM, ECM, information resources management, and even Information Management have been adopted by these communities is a desire to escape the stigma perceived by some to be attached to the term Records Management (RM).

Outside the community of people and organizations responsible for managing records, Records Management is often perceived as a nonstrategic cost center. The average employee, or executive for that matter, commonly perceives RM simply as the basement where paper records are stored or part of the mailroom. It is easy to see why such perceptions have made it difficult for many RM departments to gain the visibility and funding they require to perform their corporate function. The relationship between Information Management and Records Management will be discussed further in a later chapter.

## An Umbrella Term

Information Management is about determining which information created and received by your organization is valuable in some way, based on its content; making sure that this information is properly protected, stored, shared, and transmitted; and making it easily available to the people who need it, when they need it, and in a format that they can rely on.

Information Management, then, is an umbrella term that includes a variety of disciplines and activities, each focusing on different kinds of information and different kinds of management. In fact, in the broadest sense, Information Management touches on every business activity where information is received or created.

The table below provides some general examples of business activities related to Information Management. Although these activities have separate labels and definitions, in reality there is a great deal of overlap and interdependency amongst them.

| Activity | Kinds of Information | Basic Goal |
|---|---|---|
| Records management | Business records | Making sure business records are properly retained for legal, compliance, and business purposes, and then properly disposed of when no longer needed |
| Document management | "Documents" – a wide range of digital information | Ensuring that there are controls in place for the creation and storage of business documents so that they are easily accessible to knowledge workers and others |
| Knowledge management | Operational information of all kinds | Ensuring that the knowledge of some individuals and groups in an organization is harnessed for use by others in the organization |
| Enterprise content management | Umbrella term for technologies, tools, and methods used to capture, manage, store, preserve, and deliver content across an enterprise | Often used as a broad term to include activities such as document management, knowledge management, and published content (including website content) |
| Information security | All valuable information, with a focus on sensitive, confidential, and proprietary information | Ensuring that valuable information is accessible only to those authorized to see it; and ensuring its trustworthiness |
| Information privacy | Sensitive information, as determined by policy or law, including information about clients, customers, and patients | Ensuring that the collection of and access to sensitive information is properly controlled |
| Disaster recovery | Information needed to continue business operations | Ensuring that vital information required to operate the business can be recovered in a timely fashion after a disaster |
| Customer/client relationship management | Information about an organization's interactions with customers/clients and prospects | Ensuring that the customers' experience with a company is satisfactory and consistent; identifying customer patterns that can lead to more revenue |
| Storage management | All stored digital business information | Ensuring that storage resources such as disk drives and back-up media are used cost-effectively |
| Data mining | Structured information, such as databases | Providing tools and techniques for collecting and analyzing stored data |

## Determine Your Needs

Information Management encompasses many different activities, disciplines, people, and—no doubt—departments in your organization. The people responsible for operating the company firewall, for example, are probably in a different part of the building from the people who figure out how the customer relationship management system should work. This is part of the challenge inherent to Information Management—it is difficult to get an overall picture of how your company manages its information.

When examining your Information Management needs, start by getting the "10,000-foot view," and then work down into the details. This will require executive involvement, as we'll explore in Key 2. It will also require research into the activities of various departments throughout your organization.

Make a list of all the activities in your organization that fall under the Information Management umbrella. Since many of these activities center on technology, your IT/IS department may be a good place to start.

For example, find out:

- Who is responsible for each Information Management activity on your list? Does responsibility reside with a Records Management department, a compliance department, the IT/IS department, or a combination of these and others?

- Are there policies and practices that govern each activity? For example, do employees know if they can use the company email system for personal business, and does the webmaster know what kinds of content needs to be approved by the general counsel before being posted on the company website?

- Does your organization use a different term for Information Management that means the same thing? If so, ensure that the term is well understood throughout the company and used consistently.

- Is the Records Management expertise in your company being applied to information technology? In other words, do the Records Management people and the IT people coordinate their activities?

- When was the last time that policies were reviewed to make sure they have kept pace with new laws and regulations that affect your industry? If you haven't reviewed your policies since 2001, for example, you should do so to ensure compliance with the Sarbanes-Oxley Act of 2002.

# Chapter 2:

# Building the Foundation: Defining Records

*Organizations must have a consistent method for determining if information is a record and therefore needs to be retained and managed according to special rules. Determining this can be complex, but as this chapter explores, there are several guidelines that organizations can use to help.*

## Determining If Information Is a Record

An organization does not have to retain all information that it creates or receives. However, internal policies, laws, regulations, standards, and best practices dictate that certain kinds of information—namely, records—are retained and managed in a specific way. As such, it is obviously important that organizations have a method for identifying records.

In the digital world, there are many kinds of electronic documents, messages, notes, and various other kinds of digital files and other "stuff" that might or might not be considered a record. If all of this incredible volume of digital stuff had to be captured and managed, most businesses would be overwhelmed or even crushed beneath the weight. However, to make it even more difficult, getting rid of the wrong information can have severe legal consequences.

It quickly becomes apparent that an organization needs a way to determine which information it should retain as a record, and which