Records Management & Compliance:

Making the Connection

Organizations must take a proactive and holistic approach to compliance that ensures the business, technological, and legal challenges of records management are addressed

At the Core

This article

- discusses the importance of a records management program to an organization
- defines the concept of information management compliance (IMC)
- examines the seven key elements of an IMC framework

Randolph A. Kahn, Esq.

- *In response to the WorldCom bankruptcy filing, the Securities and Exchange Commission (SEC) takes swift and dramatic action to deal with what was perceived as a wholly inadequate records management program and imposes an $800-an-hour monitor on WorldCom (now MCI). The monitor's task is to ensure that the company "has developed document retention policies and ... has complied with these policies."*

- *A U.S. federal agency notifies a flight school six months after the September 11 terrorist attacks that two of the terrorists have been approved for student visas. The agency admits that its "current system for collecting information is ... antiquated, outdated, inaccurate, and untimely."*

- *The SEC fines five brokerage firms $8.25 million for failure to retain e-mail records. In addition to the monetary penalty, the firms are required to "review their procedures to ensure compliance with recordkeeping statutes and rules."*

- *The former CFO and sales manager of a defunct Internet company are indicted on charges of falsifying records, among other things.*

- *The CEO of a pharmaceutical company is found guilty, sentenced to seven years in jail, and forced to pay a $3 million penalty for obstruction of justice because he "directed another individual to ... delete certain computer files ... containing phone messages he received ... and documents evidencing [his] instructions."*

Cases of records mismanagement, improper destruction, and falsification have cost billions of dollars, ended careers, decimated reputations, and caused some companies to wither away. Clearly, something is seriously broken. Although many records management programs probably never functioned as they should have to begin with, for most corporations it was not until the last few years that anyone took notice. Now everyone ostensibly cares about records. In reality, however, how many records management programs are effective enough to serve business objectives and protect the organization?

The Records Program as Business Facilitator and Insurance Policy

Records are the way that institutions "speak." Over time, employees transfer, retire, forget, die, or quit. Records, however, are and always will be needed to ensure that the organization continues to function and can protect its business and legal interests. More specifically, records allow organizations – among other things – to perform business planning, deal with customers' needs, protect legal interests, take care of business needs, and comply with laws, regulations, auditors, and courts. Records management is the process of managing the corporate memory in a way that makes trustworthy records readily accessible any time they are required.

While these business drivers and generalized legal needs are real, what increasingly drives the discussion today is the organization's goal to be perceived as a good corporate citizen. Corporate directors, executives, and investors all demand assurance that the records management program will not negatively impact them and will provide a degree of protection from claims of wrongdoing.

Just as they need insurance, companies of size and substance need a records program to ensure that they are covered if and when trouble strikes. In the records management context, that means an organization can demonstrate that it has an effective and institutionalized way to manage all records and to do what is expected of a good corporate citizen. At minimum, that means that an organization retains records based on sound business judgment and in conformity with legal requirements and considerations. It further requires that records management directives are written and consistently applied to all records and that all employees are taught to follow them. Finally, it requires that records do not get destroyed in anticipation of litigation and that the company can effectively search for all responsive records and make them available to their adversary or a regulator in the context of an audit, litigation, or investigation.

Is each organization's records management program properly developed for the new highly sensitive, high-profile use that seems to have taken center stage in today's business environment? When company executives inquire about the status of the records management program, they are probably not referring to file plans or scanning projects. They are asking at a high level whether the records management program has all the components in place today to insulate the company if and when it is subjected to records-related scrutiny. In other words, will their records management program "insure" against the reckless, intentional, or malicious acts of employees or others who have access to the company's information crown jewels?

E-Records Management: Ubiquitous and Flawed

Paper records get mismanaged, altered, and destroyed. However, underlying much of the concern around records management is the exponential growth of, universal reliance on, and commonplace mismanagement of electronic records. According to "How Much Information," a global study released last year by the University of California at Berkeley, in 2002, 800 megabytes of new information was created for each person on earth – with 92 percent of it stored on magnetic media, primarily hard drives. An IDC report, "Worldwide E-mail Usage Forecast, 2002-2006: Know What's Coming Your Way," predicted that the number of e-mail messages sent per day will grow from 31 billion in 2002 to 60 billion by 2006.

The importance of these gargantuan numbers is not the mere volume but rather the fact that such technologies are now used to transact real business.

How Organizations Use E-mail Today

(as a % of respondents)

Source: Managing E-Mail in the New Business Reality
AIIM International and Kahn Consulting Inc., September 2003
©2003 Kahn Consulting, Inc *www.kahnconsultinginc.com*

As the sidebar chart indicates, most companies use such technologies as e-mail to conduct important business activities. Yet e-records continue to be mismanaged by companies and governments alike.

The U.S. federal government conducted a 2002 study, "Information Management: Challenges in Managing and Preserving Electronic Records," to assess how well it was managing its own electronic records. The study concluded that there were major flaws in its ability to properly retain and manage electronic records: "Records management guidance is inadequate in the current technological environment of decentralized systems creating large volumes of complex electronic records." A 2002 U.S. General Accounting Office Report on information security at the Federal Deposit Insurance Corp. (FDIC) found a similar lack of controls that exposed critical information to "inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction, which may occur without detection."

The recipe for disaster appears already to be on every organization's plate, whether large or small, public or private. Most organizations – even the most sophisticated institutions – have a vast and growing volume of electronic records, and much of it is increasing in importance as electronic documents replace their paper counterparts as business evidence.

In a recent court case, *Flour Daniel v. Murphy Oil USA Inc.,* a litigant was reminded about how seemingly innocuous records management failures can create big headaches. Because one of the parties did not have a written policy regarding e-mail retention and because the company failed to follow its own disaster recovery backup tape recycling schedule, it was confronted with the prospect of reviewing 19.7 million e-mail messages at a projected cost of $6.2 million. What was a simple problem that could have been easily and inexpensively addressed earlier became a large, expensive problem in the context of the lawsuit.

Records Management: A Department of One?

Contrary to the popular armed forces advertising campaign touting the success of an "Army of One," a successful records management program requires much more than what any one person can deliver. Sensitive to the post-Enron/Arthur Andersen environment, a *Fortune* 500 company wanted to audit its records program to ensure it had implemented the essential elements of a viable records management program. The records manager was confident that everything had been done to protect the company. The entire records management program staff consisted of an "Army of One" in a sea of tens of thousands of other employees. While some records management program components were fully developed, only one part of one division – out of seven divisions – had even partially followed a retention schedule. In fact, the requirement to develop and follow retention rules was wholly voluntary. Also, the records manager's purview excluded managing e-records, a function left to the information technology (IT) staff to deal with – or not.

The company had no high-level records management policy telling employees what to do about managing records. Selected records-related procedures were available on an internal records management Web site, but they were seldom accessed by anyone except the records manager. Lawyers failed to contact the records manager to seek guidance in finding, preserving, and producing records in the context of litigation, audits, and investigations. Given the highly regulated environment in which they operated and the hundreds of ongoing lawsuits, it was both mystifying and damning that no one bothered to notify the records manger about the need to preserve the records subject to these actions. This is a case of *when* – not *if* –

the company will be penalized for not taking records management seriously.

Information Management Compliance

Something may be better than nothing but, in the end, that something may not be good enough. Today, when one bad news story can send the whole company into a tailspin, the records management program requires a much more proactive and hands-on approach, one that recognizes that real protection of business and legal interests comes only with the imposition of a formal discipline that considers what it will look like if and when the organization is judged by courts and regulators – and, possibly, the court of public opinion.

Information management compliance (IMC) is a model and methodology that applies compliance principles to any type of information management activity and enables a positive outcome if a records management program is challenged. IMC borrows from and adapts the principles from the U.S. *Federal Sentencing Guidelines* to develop a working framework by which one can build, rebuild, or augment a records management program. The guidelines are used by U.S. federal courts to determine what punishment is appropriate for corporate and individual wrongdoers when they violate the law. For years, these same principles have formed the basis of many corporate compliance programs. They can apply to records management activities as well. [See "The Many Uses of Information Management Compliance."]

Given the nature and magnitude of today's records-related problems, it is prudent to evaluate records management programs, analyzing them against and rebuilding them with the same criteria by which they may one day be judged in court.

The **Many Uses** of **Information Management Compliance** (IMC)

IMC can, and should, be applied to all information management activities, including:

- Storage management
- Document management
- Information lifecycle management/ content management
- Privacy
- Electronic business process management
- Business continuity and disaster recovery planning
- Information security
- Transaction management
- Application development and integration
- Technology purchasing and acquisition
- System configuration and management
- E-contracting

Applying the Principles of IMC

Merging compliance with a records management program is about building a framework to allow the records manager, the company, and all its employees to get it right. It is not and cannot be about guaranteeing results or predicting the outcome in all situations. IMC enables employees to get it right and seeks to protect the organization if and when mistakes happen (and they always do) or when someone intentionally violates policy.

The essential elements of the IMC framework include:

1) Good policies and procedures
2) Executive-level program responsibility
3) Proper delegation of program roles and components
4) Program dissemination, communication, and training
5) Auditing and monitoring to measure program compliance
6) Effective and consistent program enforcement
7) Continuous program improvement

1 *Good Policies and Procedures*

Policies and procedures are essential to IMC for two reasons. First, they tell employees what not to do as well as what to do, and how and when to do it. A formal mechanism such as written directives is essential to providing all employees with a consistent message and affecting change across a large institution. At a minimum, they tell the outside world that the company cares enough about a particular matter to have cemented its commitment in a formal and official way. When scrutinized by a court, regulator, or the wary investing public, *anything that is perceived as good and reasonable corporate policy and behavior can transform a potentially bad situation into a non-event and one that is more likely to be overlooked as a one-time occurrence.*

Depending on the nature of the organization and industry, the kinds of written directives will vary as will the messages advanced in them. But most institutions will need a records policy manual explaining, among other things, the following:

- Retention
- The employee's role in managing records
- The roles and responsibilities of the records management infrastructure
- How and when third parties should manage company records
- Special retention situations impacting electronic records
- Issues of ownership, control, classification, and coding of different categories of content
- Privacy and many other topics

This type of policy leads to a soup-to-nuts manual that at a high level helps give retention and records management context and meaning. Equally important, especially in the current records-sensitive environment, is the creation of a policy that directs the preservation of any tangible evidence even potentially relevant to an imminent, threatened, or pending audit, lawsuit, or investigation. "Legal hold" or "records hold" rules should make clear that all records policies are suspended and supplanted by new rules mandating preservation. So, until a particular matter is resolved, *nothing* is destroyed, even if the regular retention rules would have otherwise sanctioned disposition.

In a May 15, 2002, *Wall Street Journal* article, David Duncan, an Arthur Andersen partner allegedly involved in the records destruction scandal leading to the collapse of the accounting firm, said, "I thought this was all entirely appropriate until I received a subpoena." Even if Andersen could have disposed of drafts, work papers, and working files in the ordinary course of business, after the firm knew or should have known it was likely to be dragged into an investigation involving Enron, the rules needed to change. Apparently, Duncan did not understand the rules.

The lesson learned is simple: At the first sign of potential trouble, a company must not suddenly press compliance with rules it had failed to follow, even if the rules would have otherwise allowed them to clean house. When an organization learns it may be involved in any formal proceeding, it is too late for house cleaning.

2 *Executive Responsibility*

The only way records management is going to get the attention and commitment it needs is if someone at the top tells the rest of the organization that records management matters. There is no incentive for all employees, including all business unit heads, to invest limited resources in a program that may not be perceived as helping to deliver profit, productivity, or a healthier bottom line. In fact, records management has been and continues to be viewed as a cost center and *unless – and until – the executive makes clear that records management is important, it will not likely receive the attention it deserves.*

To be effective, records management needs high-level executive support. The executive should clearly communicate to all employees that he or she views records management as central to the management, growth, and fiscal health of the company and that all employees are expected to do their part to manage records. Periodic changes in policy or other significant records management-related events also should be introduced or announced from above. Records management should not expect any day-to-day involvement of the executive, whose role should be limited to sending the right messages, properly funding initiatives, and making sure all other company manage-

ment works records management into their plans. Frankly, if the employees do not follow the lead of the executive, they are not likely to follow the direction of the records manager.

3 Records Management Delegation

IMC delegation is about *giving the right employee an appropriate level of responsibility to properly carry out some information management activity.* It is about the ability to execute a particular task and the authority to ensure that it gets done as intended. Records managers cannot dictate policy to executives, but they do possess the knowledge to develop and teach policy. Executives, on the other hand, should delegate to the records manger the responsibility to implement the program and must make it clear to all employees that they need to participate actively in making the records management program a success. From top to bottom, responsibility has to be properly delegated at every step to ensure all employees are on board and know what is expected of them, no matter their position in the company. Ultimately, proper records management delegation includes telling all employees that they have some records management responsibilities.

> If a **records management policy** states that the **retention rules apply** to all records **regardless of media**, then **all electronic records** should be **subject** to the **same rules**

In *Danis v. USN Communications*, various executives were severely admonished for failing to delegate records management responsibility properly. In this case, the chief executive officer paid thousands of dollars out of his own pocket to compensate for his personal responsibility for the company's records management failures.

4 Communication and Training

Unless all employees know what to do, the records manger's hard work will routinely be undermined. Simply stated, *teaching records management directives may not be effective in every case, but there is a much better chance that employees will get it right if they are trained* than if they receive no formal guidance whatsoever.

Ongoing communication and training is critical – like records management, communication and training are a process, not a project. All new employees would benefit from records awareness training. Some institutions now have annual training for various types of records-related activities. For example, employees who want continued access to e-mail may be required to go though an annual refresher training course. Companies taking a more proactive approach to management do so with the belief that it is more productive and less expensive to make training an ongoing activity.

Could the result have been different at Andersen if the company had been able to demonstrate that Duncan knew of and was trained on the company's legal-hold policy? Creating, communicating, and training on the policy might have allowed Andersen to place blame for the destruction on the lone-wolf employee. The company could have argued (perhaps successfully) that the individual was exclusively at fault because he alone disregarded company policy that he *knew* did not countenance the destruction of anything needed for a formal proceeding and that he did so in an apparent attempt to cover up his personal wrong-doing. Andersen, however, was not able to deflect responsibility and is effectively out of the accounting business.

5 Auditing and Monitoring

The only way a sizable organization can systematically learn about problems with its records management program is by auditing past acts or monitoring current conduct. Learning about problems in the process is essential for IMC, whether it is through audits by employees or technological monitoring for offending activities. However, once problems are unearthed, they must be addressed.

In the Murphy Oil lawsuit, for example, if the party that failed to follow its 45-day disaster recovery backup tape recycling schedule learned that its technology department was not following its own policy and corrected the problem before the lawsuit, it would not have been confronted with a multimillion dollar expense for a fishing expedition into the pool of backed-up messages.

6 Consistent Enforcement

IMC can be effective only if a company consistently applies and enforces its own directives. If a records management policy states that the retention rules apply to all records regardless of media, then all electronic records – no matter where they are located – should be subject to the same rules. Yet so

many companies routinely limit mailbox sizes, making it all but impossible to manage e-mail records. Worse, many companies purge the contents of the e-mail system without regard to contents after a few weeks, even though statistics show e-mail is how business gets done and the e-mail system is full of business records. Someone must be responsible for applying and consistently enforcing the records management rules with respect to records in voice mail, PDAs, laptop computers, discussion databases, and instant messaging.

The IT department must be advised that "innocently" destroying electronic records by recycling the storage media when it runs out of storage space violates the company's retention rules. Not long ago, a company was forced to pay a monetary penalty for failing to preserve records in the context of a lawsuit. Upon closer evaluation of the destruction of evidence claim, it appeared that retention rules were not applied to e-records. The IT department made up its own rules for retention based on what the system owner decided was necessary. When they ran out of space, he or she simply destroyed otherwise needed evidence.

7 Program Improvement

The seventh IMC key is recognizing when the system is not working and doing something about it. When programmatic failures become known, the system may need an overhaul. In one company, for example, instead of having a company-wide method for determining how e-records should be stored and indexed, that responsibility was left to the technology owners' discretion. In the interest of saving some storage space, a technology professional decided to index tens of millions of insurance claims by claim number only. When a regulator asked for all retained claims to be searched by plan name, claimant name, and other criteria, it could not be done. The company had to spend millions to search for the requested e-records. Had a company-wide list of indexing criteria been developed and provided to all system owners, the problem could have been averted. It is bad business and a wasteful investment in technology to capture, store, and migrate company e-records but not be able to access them when needed.

We live in interesting, albeit particularly unforgiving, times, especially as they relate to records mismanagement. When records-related mishaps bring down companies and their executives alike, it is reasonable for a company to ask itself whether its program is really good enough to protect the company. There has never been a better time to take a closer look at just how good a records management program is and seriously consider applying IMC. In the end, if a program is going to be evaluated by compliance principles, it should be built on the IMC principles. IJ

***Randolph A. Kahn, Esq.**, is the founder and principal of Kahn Consulting and the co-author of* Information Nation: Seven Keys to Information Management Compliance. *He advises* Fortune *500 companies, governmental agencies, and court systems on legal, compliance, and policy issues of information technology and information. He may be contacted at* rkahn@kahnconsultinginc.com.

References

"FDIC Information Security: Improvements Made but Weaknesses Remain" (Report to the Board of Directors, Federal Deposit Insurance Corp.). Washington, D.C.: U.S. General Accounting Office, 2002.

"Federal Judge Appoints WorldCom Monitor." Reuters. 3 July 2002.

Guidelines Manual, §3E1.1. United States Sentencing Commission. 2002.

"Information Management: Challenges in Managing and Preserving Electronic Records." Washington, D.C.: U.S. General Accounting Office (GAO-O2-586), 2002. Available at *http://www.gao.gov/new.items/d02586.pdf* (accessed 5 March 2004).

Kahn, Randolph A. and Barclay T. Blair. *Information Nation: Seven Keys to Information Management Compliance.* Silver Spring, MD: AIIM, 2004.

Levitt, Mark and Robert P. Mahowald. "Worldwide Email Usage Forecast, 2002-2006: Know What's Coming Your Way." Framingham, MA: IDC, 2002. Available at *http://www.idc.com/getdoc.jhtml?containerId=27975* (accessed 5 March 2004).

Lyman, Peter and Hal R. Varian. "How Much Information?" Berkeley, CA: University of California-Berkeley School of Information Management and Science, 2003. Available at *http://www.sims.berkeley.edu/research/projects/how-much-info-2003* (accessed 5 March 2004).

"SEC, NYSE, NASD Fine Five Firms Total of $8.25 Million for Failure to Preserve E-Mail Communications." Securities and Exchange Commission press release. 3 December 2002. Available at *http://www.sec.gov/news/press/2002-173.htm* (accessed 5 March 2004).

"Six Months after Sept. 11, Hijackers' Visa Approval Letters Received." *CNN.com.* 13 March 2002.

© Arma International 2004

May/June 2004 • The Information Management Journal 35