

THE BANKING  
MAGAZINE  
OF THE  
CENTRAL STATES

# BankNews

www.banknews.com JULY 2004

## RECORDS MANAGEMENT:

*keeping out  
of trouble*

20

## OVERDRAFT PROGRAMS:

*rules and best  
practices*

28

## ASSOCIATION CONFERENCES:

*Illinois,  
Missouri,  
Kansas*

36

# Compliance: a guide through the maze





## It's after Sarbanes-Oxley. Do you know where your records are?

Attention to records management practices  
is vital to avoiding trouble

By Mark Greisiger and Bob Tillman

**R**ecent regulatory requirements, such as the Gramm-Leach-Bliley Act of 1999 and the Sarbanes-Oxley Act of 2002, make managing and protecting information both a business priority and a legal obligation. These requirements demand the attention of executives and corporate boards of directors. Unfortunately, many financial institutions lack effective policies and procedures for systematic control of recorded information. For that reason, they may be caught unable to produce records or destroying records, resulting in a fine and loss of reputation for the bank.

*Mark Greisiger is president of NetDiligence ([www.netdiligence.com](http://www.netdiligence.com)), an information security assurance services company. Bob Tillman is public affairs director for ARMA International ([www.arma.org](http://www.arma.org)), a not-for-profit association for records and information management professionals. Reprinted with permission from BankNews Publications.*

Some of the most common records management problems banks have include:

- Storing records too long, not long enough or not at all.

Losing information needed for proper SEC reporting.

Failing to properly safeguard and protect information and records from hackers or unauthorized insiders.

Lacking a system to place holds on documents that are, or can reasonably be expected to be, part of a legal or regulatory inquiry.

Not having a system to find and produce requested records in a timely fashion.

All of these shortcomings can result in the penalties for non-compliance with recordkeeping regulations, a tarnished reputation and possible legal liability. Because the stakes are so high, this is

an issue that must be addressed at the highest level of the organization.

One of the smartest things a bank can do is to make sure it has a certified records manager who is given adequate time and resources to manage information and records internally. Records and information management is a specialized field concerned with the systematic analysis and control of business operating records and information – both paper and digital.

Some of the day-to-day activities involved in a solid records and information management program may include:

Scheduling document retention.

Determining document storage (possibly including off-site options).

Overseeing information backup systems and processes.

Retrieving requested records.

Destroying records according to the proper retention schedule.

Protecting records storage systems.

Coordinating electronic records management schedules and processes with the department.

Defending intellectual property, including protection of copyrighted and trademarked materials.

## Why is RIM vital ?

Being able to demonstrate an attempt to comply with federal regulations can go a long way toward resolving issues with the regulators. But aside from the clear danger of not being able to comply with federal regulations, other risks exist for banks that fail to address the issue of records and information management head on.

Litigation costs can skyrocket for banks with poorly managed records. With the proliferation of electronic records – from Word files to spreadsheets to e-mails – it has become easy to store more information in less space. While the sheer filing cabinet space requirements once acted as a natural deterrent to indefinite storage of records, adding more server space can appear to be a simple solution today. But what happens when a lawsuit looms and discovery begins? Companies have had to settle defensible cases simply because the cost of retrieving all those electronic documents covered by discovery, hiring para-

legals and attorneys to review them, was too great.

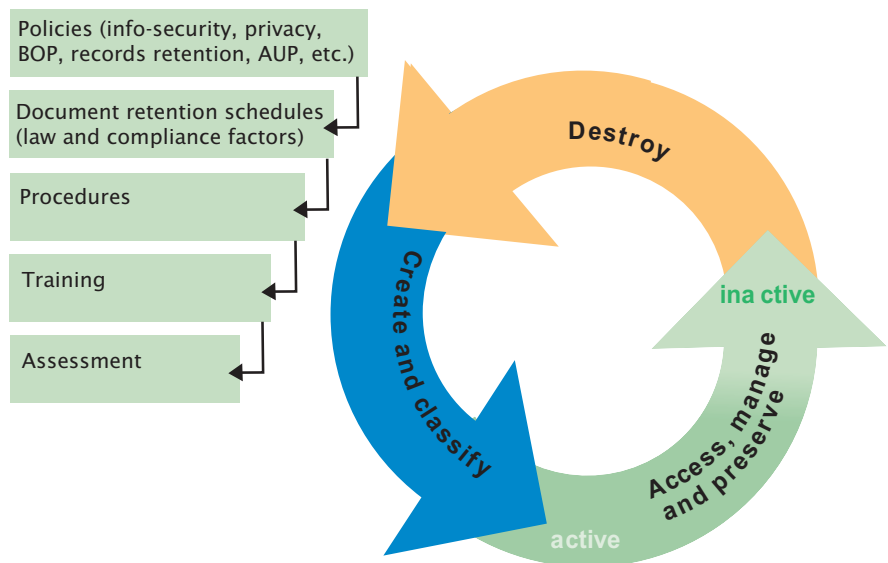
Then there are liability issues. Records information management systems need to demonstrate a prudent level of due care to mitigate corporate risk from events that can lead to errors and omissions liability and/or directors and officers legal exposures.

But putting aside all the fear of enforcement and concerns about big costs, effective RIM practices can increase the organization's efficiency. "Knowledge workers" can spend their time making decisions or analyzing information, instead of wasting time trying to locate

pertaining to recordkeeping have received far less media attention.

Sarbanes-Oxley includes important recordkeeping provisions, including mandated retention requirements for certain types of records. It also criminalizes and provides severe penalties for executives and employees who obstruct justice by destroying or tampering with corporate accounting records. Most notably, the act creates a new federal crime, effective immediately, for the destruction, mutilation or alteration of corporate records with the intent to impede or influence a government investigation or other official proceeding, either "in relation to or in

## Information life cycle



the records and information they need to make decisions.

## The Sarbanes -Oxley factor

The Sarbanes-Oxley Act of 2002 brought into sharp focus the importance of good records. By providing expanded corporate governance, disclosure, reporting and accounting requirements, the act will undoubtedly have a significant impact on public companies, their officers, directors and shareholders and the accounting, legal and the records/information management professions. While accounting and financial reporting provisions contained in the act have received much attention, the portions of the act

contemplation of any such matter or case."

This provision expands upon previous laws relating to the destruction of records with presumed intent to obstruct justice. In addition, Sarbanes-Oxley specifies minimum retention periods for accountants' work papers, correspondence and other records that contain analyses, opinions, conclusions, financial data, or other information about corporate audits.

Whether it is done by a RIM professional or overseen by a high-level executive, there are some basic things most banks should do to make sure they comply with Sarbanes-Oxley and the thou-

sands of other recordkeeping laws and regulations:

- **Review retention schedules.** Make sure accounting records, audit work papers, financial statements and supporting documentation are consistent with the new requirements.

Also review voice mail and e-mail retention policies to ensure that any material associated with key investigations or audits is being retained and that the appropriate operating systems necessary for restoration and retrieval are also being maintained. As part of this process, review current procedures for categorizing or indexing e-mail and voice mail.

Banks that are not categorizing e-mail or training employees to select documents for retention need to be aware that they may need to retain all e-mail for no less than five years and possibly up to seven years in order to be able to retrieve e-mail associated with audits and investigations.

**Review document storage procedures.** Look at current practices for origi-

nating and storing documents. Consider whether all communications, documents and workflows should both originate and be stored on central servers rather than on individual PC hard drives, where document retention and destruction rules are difficult to enforce.

**Meet the audit department.** Review with the internal audit department audit plans for key systems used to generate financial statements. Make sure the regularly scheduled audits are performed on the systems and data to ensure data integrity, change control and user access security.

### **The bottom line**

Corporate RIM programs have a solid track record of preventing or minimizing recordkeeping problems. Key components of a good program include:

A written policy that defines corporate records and standard procedures for storage, retrieval, dissemination, protection, preservation and destruction of recorded information associated with all business operations.

Retention guidelines that specify how long records are to be kept and fully address a company's legal, fiscal, regulatory, and administrative requirements.

Procedures for the timely, secure destruction of corporate records when their prescribed retention periods elapse, including provisions for suspending the destruction of records if warranted by litigation.

Design and implementation of manual and computerized methods for convenient retrieval and dissemination of recorded information.

Storage of active and inactive records that need to be retained for legal, fiscal, regulatory or administrative reasons.

Policies and procedures for identifying and protecting records deemed essential for continuity of mission-critical business operations.

Compliance assessment initiatives to monitor, audit and enforce records management policies and procedures. **BN**

