

Navigating the

Sarbanes-
Oxley

21CRF 11

SEC11a-4

ISO 15489

HIPAA

DoD 5015.2

Compliance Landscape

Compliance issues are changing the RIM industry. RIM professionals must adjust their mindsets to understand the importance of compliance in the corporate culture to better serve their company and their profession.

Julie Gable, CRM, CDIA, FAI

In his book *The Tipping Point*, Malcolm Gladwell says, “Crime ... isn’t a single discrete thing, but a word used to describe an almost impossibly varied and complicated set of behaviors.” Ironically, the same thing can be said of compliance.

Compliance is the name given to multi-faceted programs designed to ensure that an organization’s culture and collective processes meet legal, regulatory, and ethical requirements. At present, compliance is a binary state – a company either is or isn’t compliant – and there are, as yet, no objective measures of progress to assess whether a firm is 50 or 80 or 90 percent compliant. Companies find out whether their compliance programs are adequate through highly publicized investigations or court cases that have devastating effects on corporate reputation, stock price, and shareholder loyalty. In one recent example, a J.P. Morgan Chase subsidiary was fined \$2.1 million for failing to keep e-mail communications for three years as required by New York Stock Exchange (NYSE) and National Association of Securities

Dealers (NASD) regulations. In short, in the compliance arena, it is easier to see failure than it is to measure success.

Any and all compliance events, whether routine inspections, examinations, or regulator reviews, pose huge risks to corporations and the officers and directors who oversee them. (See sidebar.) Records can either mitigate or worsen those risks, so records management has become integral to compliance efforts. Compliance concerns are often the motivating force behind electronic records management programs and the chief source of funding for such efforts. In compliance, stakes are high, consequences are harsh, and records are pivotal, so it pays for records and information management (RIM) professionals to understand the compliance landscape in more depth.

Dispelling Confusion

Fear, uncertainty, and doubt surround compliance and for good reasons.

It can be hard to determine what regulations apply. Those involved with compliance efforts often rely on pub-

At the Core

This article

- ▶ Examines issues surrounding compliance initiatives
- ▶ Reviews common approaches to compliance
- ▶ Explores the RIM manager’s role in compliance efforts

lished articles and conference presentations to become familiar with various mandates. Reliance on secondary sources of compliance information, however, can give false impressions about what is actually required. Most published articles are limited by space constraints, and all articles are routinely edited for clarity and brevity. The content that remains varies in detail and depth. In addition, some white papers and presentations are produced by those with vested interests in selling compliance-related products or services. For example, much has been made about the need to write once read

many (WORM) media in financial services, but a closer look at U.S. Securities and Exchange Commission (SEC) rule 17a-4 reveals that other media are also acceptable.

One way to assess a secondary source's compliance expertise is to look for distinctions between mandatory and optional requirements. (See chart: "Mandatory vs. Optional Requirements.") For example, compliance materials often list DoD5015.2 and ISO 15489 as compliance concerns. Neither is exactly true: DoD5015.2 is a standard and certification program for records management software products that applies only to software vendors who wish to sell to the National Archives and Records Administration (NARA) and federal agencies; ISO 15489 is an international standard for the development of records management programs. Neither is a mandatory compliance requirement.

Another telling sign is the claim of a compliant product. The fact is that businesses are compliant, products are not. Software products that have successfully passed DoD5015.2 testing will declare themselves "certified" rather than compliant.

The point is, published pieces and web materials might provide interesting background, but the only sure way to know what regulations actually say is to read them.

Compliance is not one-size-fits-all. The regulations that apply to a given company depend on factors such as the industry in which it operates, whether it is a public or private entity, whether it is national or multinational in scope, and so on. The best known and most ballyhooed regulation is the Sarbanes-Oxley Act (SOX), a grab-bag of provisions governing public accounting firms, corporate boards, whistleblowers, financial statements, insider trades, internal controls, changes in operations, and records falsification or destruction. SOX applies to all publicly traded companies in the United States and to foreign companies that list on U.S. stock exchanges.

Beyond SOX, other regulations apply to specific industries. The Health Infor-

mation Portability and Accountability Act (HIPAA) applies to all health plans, healthcare providers, prescription drug card sponsors, and others who handle individually identifiable health information. Its provisions cover patient privacy but also include requirements for the integrity and availability of electronic patient data. In pharmaceuticals, 21 CFR 11 is a set of requirements governing the use of electronic records and signatures. [Editor's note: See "Digital Archiving in the Pharmaceutical Industry," p. 54].

For financial services, SEC 17a-4 governs records required to be made by stock exchange members, brokers, and dealers regarding client records and communications. In multinational banking, Basel II specifies that banks that implement "advanced methodologies" can reduce the reserve amount for loans. Basel II spells out 25 "Core Principles for Effective Banking Supervision," one of which is that adequate records enable

supervisors to have a fair view of a bank's financial condition.

The common thread in diverse regulations is information and how it is handled. As RIM managers know all too well, most laws spell out what is expected but not how to accomplish it. No law stipulates that companies must use electronic technologies; the choice to do so is always optional. For that matter, all laws are technology neutral, since no authority wants to dictate a particular solution in an age when new tools are evolving every day. Most laws are purposely vague and broad; otherwise the rule makers would have to list every possible contingency, leaving loopholes. And rarely, if ever, will a regulation or law tell how to accomplish compliance; the intention is that methods remain flexible and appropriate to the size and resources of the complier.

Compliance is a moving target. Important changes occur after a law first appears, usually in the form of final rules and enforcement guidelines that can

Rule:	Deals with:	Mandatory?
Sarbanes-Oxley	Corporate governance, financial reporting, records	Yes, for all publicly traded companies
HIPAA	Privacy of patient medical information	Yes, for healthcare insurers and providers
SEC 17a-4	Records kept by brokers, dealers, exchange members	Yes, for financial services
21 CFR 11	Electronic records in pharmaceutical industry	Yes, for pharmaceuticals
Basel II	Reserve requirements in banking industry – European and U.S.	Yes, for multinational banks
DoD 5015.2	Standards and certification for records management/document management software products	No
ISO 15489	International standard for design of records systems	No

Figure 1: Mandatory vs. Optional Requirements

clarify how given agencies will interpret the regulations. Regulations also change over time based on public comment and refinements, and compliance deadlines may change as well – as they have several times for small company compliance with SOX, now slated for June of 2006. Eventually, most laws will have test cases that provide further enlightenment by showing what the regulator considers a violation. Currently, the HealthSouth case is considered a major test of SOX.

Regulatory interpretation often depends on the background and former experience of those involved in the compliance effort. Compliance officers come from diverse backgrounds and often have little experience regarding records management. Some have expertise related to a specific regulatory agency, such as someone who previously worked for the Food and Drug Administration (FDA) who now heads pharmaceutical company compliance efforts. Compliance officers may also be attorneys or corporate counsels charged with interpreting legal matters, sometimes with mixed results. One attorney believed that SOX's records provisions meant that no records should ever be destroyed in case they are needed for any investigation, no matter how unforeseeable or distant in the future. Compliance officers may also be ex-auditors with specific experience in determining whether rules are adequately met. In smaller firms and in academic settings, it is not unusual to find a staff member with other roles assuming the responsibility and duties of compliance officer.

The compliance officer's degree of experience with records management can affect compliance decisions. For example, at one financial services firm in midtown Manhattan, the SEC's requirement to keep "six years of client files, the first two in an easily accessible place" was interpreted to mean keeping two years of paper files onsite at all times. The SEC's Office of Compliance Inspections and Examinations has since clarified that requested information should be compiled and made available within 24 hours of investigators' requests, a turnaround

Compliance Risks

According to the *Wall Street Journal*, shareholder lawsuits are up 137 percent since 1995. Such suits result when institutional investors – for example, pension funds – charge boards of directors with dereliction of duties for failing to spot and stop fraud. Lawyers who prosecute such cases receive higher contingency fees if they can secure settlements from corporate officers' own pockets, a move aimed at emphasizing personal accountability. A high-profile example is the \$31 million settlement agreed to by 21 directors of Enron and Worldcom, with the bulk of the amount to be paid from each one's own personal resources.

time that most offsite storage companies could meet.

Compliance Realities

Compliance is expensive. A January 2005 *Wall Street Journal* article noted that a survey by Financial Executives International found the average total cost of SOX section 404 (adequacy of internal controls) compliance to be \$3.1 million for companies with revenues exceeding \$2.5 billion. The chief information officer (CIO) of Barclay's Bank, quoted last November in *CIO Magazine*, stated that the firm has spent \$251 million on compliance issues. More telling, perhaps, is the estimate from AMR Research that 90 percent of compliance spending is on consultants and internal staff according to the July 1, 2004, issue of *CIO Magazine*. [Editor's note: See "Executives Praise SOX but Seek Changes," p. 22].

For all the lavish spending, companies do not want to win awards for outstanding compliance programs. Most would rather spend the money on additional research and development or on projects that promise increased revenues. Firms that have never committed any fraudulent act, and small firms in particular, deeply resent the additional work that compliance dictums have imposed on them. When it comes to compliance projects, corporate leaders want to be just behind the curve for their industry, not singled out as leading edge. RIM managers need to be mindful that, while records are key to compliance, funding

for records projects will not be unlimited.

Compliance Approaches

Given the significant amounts of time and money to be invested, most companies adopt an overall, unified approach to compliance. Work will involve interpreting requirements, crafting policy and procedures, using technology, training employees, and auditing to assess how well behaviors actually adhere to internal rules. It takes clout to initiate compliance efforts and a strategic vision to move them forward. Revised records management programs are very likely to be part of overall compliance strategy.

In the initial phases of compliance efforts, most companies form stakeholder teams whose objectives are to interpret regulations, decide on an approach, and drive progress in attaining compliance. The stakeholders must include senior executives who can convey the effort's importance throughout the enterprise. Obtaining executives' buy-in is not difficult, because they are likely to be held personally liable for non-compliance as illustrated in former Chief Executive Officer (CEO) Bernard Ebbers' conviction in the WorldCom fraud. Executive participation is a must for success because compliance is a top-down effort and a culture change that will require human and financial resources. Other stakeholder committee members and their roles appear in the chart: "Stakeholder Committee Roles."

Because information technology (IT)

is all-pervasive in business, IT plays a big part in compliance projects. Even though SOX only requires chief financial officer (CFO) and CEO certification of financial statements, many companies now have CIOs certify the statements in advance of top executives because the numbers are derived from IT-based systems. In firms that have consolidated IT into a global service, CIOs have been surprised to be the recipients of regulatory violations.

Stakeholders' committees guard against the "off-my-desk" approach that was relatively common in the early days of compliance and still is common in cases where one person has been appointed to assume responsibility for an organization's response to new requirements. This project-based approach, which is not recommended regardless of circumstance, seeks the most expedient means to meet deadlines – usually by implementing an exact replica of another entity's program, complete with rules and tools. The problem with project-based approaches is that they are not easily sustainable as requirements change, and they often ignore the need to test or measure adherence to what has been put in place.

Current best practice favors compliance approaches that are based on risk assessment and mitigation, where compliance is attained in phases. Risk-based approaches acknowledge the need to respond to multiple requirements simultaneously and provide a method for assigning priorities. The risk-based approach focuses on identifying risks, assessing their magnitude and probability of occurrence, and deciding an appropriate response – which may include avoidance, acceptance, reduction, or sharing of the risk.

For example, a pharmaceutical manufacturer is subject to SOX, 21 CFR 11, and several other FDA requirements regarding Good Manufacturing Practices. In assessing risks, the company considers that major risks regarding SOX include financial reporting and internal controls that could result in negative publicity for the firm, a drop in stock price, and reputation damage. The probability of occurrence, however, may be relatively low. On the other hand, risks that come with not meeting FDA requirements are very high, with serious potential consequences that could include plant closures, greatly affecting

the company's ability to continue producing revenue. The probability of occurrence is also high because FDA inspections are a certainty. Although the example is oversimplified, the examination of all risks helps companies prioritize compliance efforts and make decisions on how to apportion human and financial resources. In fact, the idea of risk evaluation has applicability beyond compliance requirements. (See sidebar "COSO's ERM Framework".)

Once priorities are determined, companies normally survey what is already in place to address requirements, reviewing the adequacy of policies, procedures, recordkeeping practices, technologies, training, and audit capabilities. Some companies have grown very sensitive – particularly within corporate law departments – regarding the availability of reports on inadequacies. The thinking is that such documents could be used by adversaries in litigation to show that the company was aware of problems but did little or nothing to solve them.

One common pitfall in compliance surveys is to focus on technology deficiencies while ignoring gaps in practices, standards, documentation, oversight, assigned responsibility, and accountability. While it is naive to think that electronic information handling can be adequately served without well-thought-out use of technology, it is also unrealistic to believe that compliance solutions are merely a matter of choosing the right technology. The truth is that technology investments are worthless unless the required policy and procedural infrastructure is already in place. Controls on who may authorize checks, for example, are far more important than the technology involved in check printing. The same is true for electronic records management, where records series, retention rules, and the policies that govern them are essential to ensuring effectiveness.

The next step is a plan based on identified priorities and regulatory deadlines. While many firms simply devise work plans to address deficiencies in current processes, others take a broader approach

Committee Representative	Purpose
Executive	Lend credence and political clout to effort
Legal	Provide guidance regarding regulatory interpretation
Finance	Oversee funding needs; essential for Sarbanes-Oxley Act (SOX) internal controls requirements
Internal Audit	Give input on current practices
Records Management	Assist with records-associated risk
Information Technology	Provide input on current processes; determine practical use of technology in support of compliance efforts
Outside Consultants	Deliver insight on peer company practices

Figure 2: Stakeholder Committee Roles

by developing compliance programs emphasizing policies, procedures, and work rules. These programs often feature common methodologies, structures, and templates for meeting current and anticipated compliance requirements.

This principle-based framework defines the highest levels of ethics, integrity, communications, monitoring, and information system controls. The point of such an approach is to establish expectations and adequacy standards centrally, while subsidiaries implement specific measures locally. In this scenario, a corporate headquarters might develop standards for audit trails, for example, or have specific templates for testing critical systems at given intervals to ensure that they deliver consistent results.

Companies that adopt a comprehensive approach hope to leverage their investment in compliance and often plan to use ongoing compliance and/or risk assessment for continued improvement purposes. Six sigma principles – define, measure, analyze, improve, control – adapted from quality control disciplines, have been used in this scenario, which may also involve organizational change and establishment of a compliance department. In this environment, records management often reports to the compliance function.

Compliance Changes RIM

A key element of any compliance program is the ability to prove adherence to internal policies, practices, and standard operating procedures. Records kept with integrity, reliability, and availability in mind provide such proof. The strategic alliance among compliance, legal, IT, and RIM will ensure that systems produce and maintain accurate records and that internal mechanisms are in place to prevent alteration. As investigations proceed and shareholder lawsuits proliferate, it will be critical for companies to demonstrate that an effective hold can be imposed and enforced to deter destruction.

The elevated status of compliance means that fewer records decisions will

COSO's ERM Framework

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission has published an enterprise risk management (ERM) framework. The document identifies key elements of an effective enterprise risk management approach for achieving financial, operational, compliance, and reporting objectives. The ERM advocates identifying all risks, to include such factors as compliance, litigation, and other potential exposures. The ERM concept is to develop a uniform way to identify all risks and assess their magnitude and probability so that a firm can develop its "risk appetite," that is, its stance on how risks are handled. This information can be important to potential investors who want to match their investment risk profile with a company's. For example, conservative investors who shun risk would not invest in firms that have an aggressive risk appetite. The degree to which companies have control of their electronic records will likely factor into enterprise risk calculations.

be entrusted to reluctant end users. As a result, automated records declaration, classification, and retention rule application methods will dominate. Consequently, changes to RIM programs are a certainty. Records schedules developed around organization structures will give way as the need for fewer, broader records categories emerges for use with automated systems. Event-based retention periods will be less favored than finite retention periods because the latter are more easily handled in software applications without the need for

human intervention.

System flexibility will be prized as the need to adapt to changes in regulatory requirements and deadlines continues. In the future, companies will look for overall risk reduction and cost control from compliance-driven initiatives. RIM managers who can adjust their focus to big-picture, enterprise efforts, and who realize that trade-offs and compromises will be necessary along the path to compliance, will distinguish themselves in service to their companies and their profession. ■

Julie Gable is the principal of Gable Consulting LLC, founded in 1989 to provide solutions to document based information issues. She is also the Associate Executive Editor of The Information Management Journal. She may be contacted at juliegable@verizon.net.

References

Berinato, Scott. "Risk's Rewards." *CIO Magazine*, 1 November 2004.

Canter, Ralph, director, Risk Advisory Services, KPMG LLP. Interview by author, 10 March 2005.

Gladwell, Malcolm. *The Tipping Point*. New York: Little, Brown and Company, 2002.

Gullapalli, Diya. "After the Scandals: More Work, More Money." *The Wall Street Journal*, 31 January 2005.

Koch, Christopher. "The Sarbox Conspiracy." *CIO Magazine*. 1 July 2004.