



# COMPLIANCE:

## Where Do We Go From Here?

Adaptability and flexibility will go far in aiding a team dedicated to solving problems created by compliance legislation. The records and information management professional can play an important role in identifying potential problems and in finding solutions.

**Julie Gable, CRM, CDIA, FAI**

**F**or multinational firms, compliance has become like sudoku, the logic-based, numeric puzzle grid that requires looking in several directions before putting any possible solutions in place.

Compliance is a moving target: changes in regulations and expectations have made efforts complicated, time-consuming, and expensive. Knowing what has changed and what to expect can make a real difference in how records and information managers contribute to compliance efforts.

Now that the Sarbanes-Oxley Act (SOX) is nearly four years old, and with the initial round of reporting deadlines completed, it is a good time to consider three issues with regard to compliance.

- What has changed in the world of regulation?
- What are entities doing about it?
- What trends are on the horizon for the future?

### Changes in Awareness and Complexity

Financial transparency, corporate governance, anti-terrorism, and privacy protection are major regulatory themes in the United States and abroad that affect businesses across many industries. Globalization brings the realization that more than one set of rules applies – sometimes with conflicting results. Consider the case of a publicly traded, multinational bank that operates in several countries. Its compliance profile appears in Figure 1.

To get an idea of the complexity, it helps to know that SOX applies to all companies that list on U.S. stock exchanges, whether based in the United States or not. SOX's best-known provision is

### At the Core

#### This article

- ▶ Reviews the complex tangle of legislation in the United States and abroad
- ▶ Provides a look at how companies are dealing with the compliance issue
- ▶ Scopes out the future trends with IT managers

section 404, requiring management's assessment of internal financial controls in the annual report. Meanwhile, in the United Kingdom, the Combined Code on Corporate Governance also has provisions for internal controls, but the two laws differ on several points. First, SOX places greater emphasis on testing and documentation of controls. Within SOX, responsibility for section 404 compliance rests with company management, and controls are tested on a pass or fail basis so that companies are either compliant or they are not. In contrast, Britain's Turnbull guidance, a framework for meeting the

Combined Code's provisions, specifically imposes responsibility on the board of directors as well as on company management, and a "comply or explain" approach exists. Banks doing business in Britain must also comply with that country's Financial Services and Markets Act, which requires specific conduct for banking, investment, and insurance companies.

Added to SOX and the Combined Code, Basel II began as an instance of international guidance that has now been converted to European Law. Basel II recommends implementing internal controls adequate for the nature and scale of the bank's business. It sets forth principles banks can follow to improve their risk management systems, business process models, and capital strategies. Under Basel II, banks that implement "advanced methodologies" can reduce reserve requirements for loans. Records managers will be interested to know that maintaining adequate records to allow bank supervisors to have a fair view of financial condition is required. According to Christine Ardern, president of The Information Management Specialists, compliance with Basel II is required by January 2007 and will affect the top 20 U.S. banks.

# Glossary of Financial Terms

- **Market Capitalization** – Often referred to as “market cap,” it is the total dollar value of all outstanding shares. It is calculated by multiplying the number of shares outstanding by the current market price of one share. It is a measure of a company’s total value.
- **Nasdaq** – Originally an acronym for the National Association of Securities Dealers Automated Quotation system, it now refers to the Nasdaq Stock Market Inc., where about 3,200 public companies list their stocks.
- **Percentage of Revenues** – Ratio analysis is used in the financial world to gain a sense of proportion and to make judgments about financial condition among businesses in a given industry. For example, research and development costs as a percentage of revenues indicate a company’s commitment to developing new products. Compliance costs as a percentage of revenue show how big a bite compliance activities take from a firm’s income.
- **Restatements** – Restatements are acknowledgments of accounting errors that allow investors to have a better understanding of a company’s financial performance.

Privacy is another area of overlapping regulations with serious implications for managing records. The U.S. Gramm-Leach-Bliley Act prohibits sale of customer personal information and requires banks, brokerages, and insurers to advise customers of data-sharing policies, including the ability to opt out. The U.S. Fair and Accurate Credit Transactions Act (FACTA) (See article “Fair and Accurate Credit Transactions Act Provides Additional Consumer Protection” on page 62) requires safeguards for consumer credit and financial information designed to protect against identity theft. The law affects all consumer reporting agencies, insurers, employers, landlords, mortgage companies, lenders, and others. It contains specific provisions regarding adequate measures for destruction of consumer records. But Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), Britain’s Data Protection Act, and European Union privacy protections also limit the amount of data that can be gathered on individuals and stipulate that consumers have the right to review data on file for them, including opinions about them. Beyond a company’s internal operations, compliance with privacy laws also has implications for outsourcing data collection and other back-office activities.

One unexpected change is that compliance is no longer a purely private-sector issue. Office of Management and Budget (OMB) revised Circular A-123 specifies that federal agencies must submit test plans on effective internal financial reporting and be able to implement internal controls, similar to provi-

sions in SOX for private companies. An example of an internal control might be how often account reconciliation and analysis takes place. Agencies had until March 31, 2006, to submit test plan summaries to OMB.

## Changes in Who Requires Compliance

Private companies – those that do not trade publicly – once sighed with relief at not having to worry about compliance issues. This was short-lived. A kind of after-market has emerged for proof of compliance.

Creditors, particularly those who finance the company via venture capital or outright loans, want to see proof of good governance and compliance with Securities and Exchange Commission requirements as part of debt covenants. A case in point is Dole, a privately held company that established an extensive SOX program because its lenders wanted assurance of good corporate governance and financial control.

Business partners, particularly those who will share data with another firm, seek assurance that privacy and security controls are in place for information. Partners and potential partners are concerned that reputation damage will rub off on them if it turns out that an affiliated firm has compromised privacy.

Insurers, always concerned that they are underwriting good risks, want proof of compliance with good governance requirements before they will write policies for directors and officers. In the wake of the Enron and Worldcom scandals, institutional investors sued board members for dereliction of duties.

Compliance practices (or their lack) are now part of due diligence for firms that are considering merger or acquisition candidates. The potential acquirer must weigh the cost of bringing another entity into compliance as part of the overall cost of buy out or merger.

Most surprising, perhaps, is that some non-profit organizations have adopted compliance measures on their own. An example is the Julliard School, a renowned performing arts conservatory, which has adopted the governance practices prescribed by SOX. Reasons include the trustees’ desire for more transparency and the organization’s concern that its reputation will be badly hurt among donors if money is misused or the organization falters.

## Changes in Attitudes Toward Costs

According to a survey by AMR Research, companies are likely to spend about \$6 billion in 2006 to comply with Sarbanes-Oxley requirements – an amount that represents nearly 25 percent of total spending on technical services and personnel related to all compliance issues.

The burden of cost is part of the argument currently raging in the financial world regarding whether SOX compliance should apply to small and mid-sized public companies, those with market values less than \$125 million. One school of thought, espoused by Bob Greifeld, the current president and CEO of Nasdaq, says no. Greifeld has stated that the SOX cost burden on small companies as a percentage of revenues is 11 times greater

than it is for large companies. By one reckoning, 90 percent of small companies that intend to go public choose not to list on U.S. exchanges because of SOX costs and concerns. On the other side of the debate are financial luminaries like Vanguard founder John Bogle who believe SOX should apply to small and mid-sized firms. They point out that restatements of financial results nearly doubled from 2004 to 2005 and that 66 percent of restatements occurred at small companies, those with market capitalizations of less than \$75 million. While the debate continues, SOX compliance deadlines for small and mid-sized firms have changed several times and are currently set for July 2007.

Cost is also at the center of new attitudes toward centralizing compliance efforts – both from an organizational and a technical perspective. Because regulations overlap and intersect among nations, many firms opt to formulate compliance policies centrally and develop internal standards to guide world-wide subsidiaries in implementing compliance programs locally. The hypothetical bank could set compliance policy as “the bank adheres to all requirements foreign and domestic that pertain to it.” Internal standards could include templates, approaches for analyzing regulatory requirements and risk, internal reporting expectations, and so forth. Many companies are looking to set internal standards for what constitutes adequate records management practices as well.

The centralized approach also applies to technology. Entities have realized that point solutions – for example, the customer service department’s Gramm-Leach-Bliley system and the credit department’s FACTA system – have points of redundancy, particularly in the areas of search, security, storage, reporting capabilities, and audit trails. In addition, they may not interoperate, thereby complicating overall efforts at compliance. Most importantly, siloed systems have annual software maintenance costs and require internal resources for functions like systems administration and back up. Separate, tactical solutions cost more and increase complexity.

The rationale for a strategic approach is to reduce complexi-

ty and reduce the cost associated with maintaining compliance via manual, piecemeal efforts. Gartner Research Director Debra Logan, addressing a FileNet-sponsored briefing in London, urged attendees to take an enterprise-wide view as opposed to a point solution view, remarking, “Based on the research we have undertaken, with one-off solutions, you could end up spending 10 times more in the long term.”

It is important to distinguish between costs to become compliant versus costs to maintain compliance. One of the lessons that large companies learned following the April 2005 deadline for SOX section 404 reporting was that many controls put in place require manual oversight and intervention on an ongoing basis to maintain them. So while becoming compliant was costly in itself, the cost to sustain compliance will continue year-to-year. An IDC whitepaper compared compliance costs over a three-year period under three different scenarios and estimated that using outside professional services would cost \$6.9 million dollars while using internal, manual methods would cost \$1.73 million. The best-case scenario was to use internal, automated methods at an estimated cost of \$800,000.

### What Are Businesses Actually Doing About Compliance?

Industry analyst and compliance practitioner observations identify two broad areas of compliance efforts: 1) developing internal organization structures, resources, and commitment; and 2) devising compliance architecture to support the sharing of technical resources.

Many companies begin by appointing compliance officers. Within the United States, compliance officers tend to have regulatory agency experience, audit, or legal backgrounds. Two recent ads for compliance positions in the *Wall Street Journal* confirm this. One position at a bank required federal bank regulatory agency experience at a senior level, while the other, at a pharmaceutical firm, sought an attorney with experience in government relations, accounting/audit, legal, or fraud and abuse compliance.

**Figure 1: Applicable regulations for a multinational, publicly traded bank**

	US	UK	EU	Canada
Financial Reporting & Governance	Sarbanes-Oxley Act of 2002	Combined Code on Corporate Governance; Financial Services and Markets Acts	Basel II	
Privacy	FACTA; Gramm-Leach-Bliley Act	Data Protection Act of 1998	Data Privacy Laws	PIPEDA
Anti-terrorism	USA PATRIOT Act			

## Advice to Those Just Starting Out

What advice would analysts and practitioners give to non-U.S. firms and to small and mid-sized U.S. firms that may have to contend with SOX compliance issues?

**Vivian Tero, IDC:** Do as much legwork as possible to understand your business processes, COSO, and the COBIT framework. You will likely be spending money to hire consultants to help with compliance. Having internal knowledge of processes and standards in place will help when you meet with others to craft strategy for these issues.

**Russell Stalters, Compliance Solutions Group:** Small to mid-sized firms should seek out both professional functional and technical help early and not try to go it alone. Many small and mid-sized accounting and financial services consulting firms have produced templates, best practices, and prototype frameworks that can quickly jumpstart a small to mid-sized firm quickly and more inexpensively. Applying IT and records management technologies early can ensure that the documents and documentation required for SOX compliance are managed effectively.

**Penny Quirk, CEI:** Become familiar with the [regulatory] requirements, the basis isn't that different from [domestic laws], and the ISO 15489 standard is consistent for both U.S. and non-U.S. firms. Organizations have to address similar issues: development of an accountability framework and security controls, technical controls that protect and address human issues, and e-mail security.

Outside the United States, some countries have certifications for compliance officers. Examples include Australasia's certified compliance professional and the United Kingdom's foundation certificate in compliance practice.

Efforts to build compliance usually involve a team. According to Penny Quirk who heads compliance practices for Pittsburgh-based CEI, a firm that provides IT contracting, project services, and outsourcing, many clients "are beginning to grasp the importance of incorporating compliance into all functions of the organization. I insist on working with a team that represents the various levels and functional workings of an organization. In a perfect world, the team is made up of risk and compliance officers, the records manager, IT manager, and a good representation of working staff from the various departments."

A strong emphasis on reporting has emerged. Ardern notes that part of building compliance is to recognize and define the audience for reporting, which includes regulators of course, but also executives, shareholders, and stakeholders. Russell Stalters of

Reston, Virginia-based Compliance Solutions Group, a firm that specializes in implementing document, records, and business process management solutions to address compliance issues, confirms this trend. Stalters points out that his practice sees more emphasis on better reporting for senior management, the audit committee, and the board, with more desire for insight into underlying details that are summarized in reports.

Standards have become central to compliance efforts. The Control Objectives for Information and Related Technology (COBIT) standard has been used for SOX compliance in the United States, and the Conduct of Business (COB) standard, along with its records retention provisions, has been used to comply with the Financial Services Authority regulations in the United Kingdom. Says Quirk of CEI, "Take the example of emerging identity theft protection laws that identify private data requiring protection. It includes the obvious data, such as name, phone number, Social Security number – but also data such as e-mail address, office number, and driver's license number. Organizations addressing these regulations must look at all human resource and financial applications, as well as access security, and how and where e-mail and voice mail are encrypted, monitored, and protected. Another concern is legacy backups – how are e-mail, HR, and financial applications such as payroll or commissions being protected? What level of security is administered on five-year-old backup tapes? This type of situation is perfect for the Enterprise Risk Model, ISO 15489, and COBIT, because without standardized models, things are missed. Standards can also bring clients to a level of understanding that compliance involves all business records no matter the media, or purpose."

The ability to leverage technology is key. Stalters notes, "The clients we are working with are considering workflow and business process automation technologies to help them automate the tracking and processing of tests, controls, etc. in their SOX programs. Many are using spreadsheets to track the status of their compliance initiatives, using file shares as a document repository and using e-mail as a workflow tool." Vivian Tero, senior research analyst for compliance infrastructure at IDC, observes that companies want to automate to reduce costs associated with compliance audit and response cycles. "Companies want to identify IT configurations that they can leverage across regulatory requirements. They want to automate processes and leverage their existing IT investment by adding required functionality."

What's needed for cost-conscious compliance is an integrated framework that delivers capabilities for compliance and for productivity. Best bets are solutions that offer integrated content repositories, records and e-mail retention, process management, and active monitoring, along with functionality to govern processes, monitor controls in real time, capture content, attach retention rules, search, produce reliable evidence, and report. Some firms (and some vendors) are putting greater emphasis on automated ways to monitor and report in real time to catch discrepancies before bad things occur.

Records management is part of compliance. "Records man-

agement is an enterprise program,” says IDC’s Tero. “Leading-edge companies have spent 12 to 18 months trying to understand and create an information taxonomy as part of their records management program. Much business process work is involved in this as companies create their own classification systems and address issues of records ownership and responsibility. They are taking a more holistic approach to records, focusing on having policies uniformly implemented and enforced throughout the enterprise. Smaller organizations take incremental steps to address records management issues. They are looking at solutions around e-mail archiving and will expand efforts to other content and file types, unifying retention policy across paper and electronic records.”

### What’s Next?

Ralph Canter, managing director of risk advisory services for KMPG, states, “In my opinion, compliance is an issue that will not be going away in the next four or five years. Regulations do not come off the books quickly or easily. The question for many companies will be, ‘How do we comply and make it less expensive?’” Canter draws an analogy with the total quality management trend of the 1980s. “My observation is that at some point, companies realized that inspection after the fact was a non-value added activity. What they discovered was that automated prevention – that is, designing in quality – did add value. It’s my opinion that companies should stop thinking about compliance as a separate function and just build it into processes.”

There is a strong desire to distribute responsibility for compliance testing and oversight to the line of business managers. “People chartered with administering compliance programs cannot continue to manage all aspects of these programs,” says Stalters. “Many have been supplementing their staffs with temporary help and cannot continue to fund this. Another key concern is the experience of spending more than 95 percent of their time gathering, tracking, and preparing reports while having little time to review accuracy or provide analytical review to identify trends and make conclusions.” Compliance is likely to become everyone’s responsibility.

Risk assessment will continue to play an important part in prioritizing and managing compliance efforts. Tero observes, “Understand where the risk is and tackle that first. For retention programs, the advice is baby steps rather than being overwhelmed by monumental exercises. Look at records retention and compliance as keys to enabling better governance instead of just reacting to requirements.”

Thanks to compliance requirements, the old mix of people, process, and technology has a new ingredient: control. Records and information managers have long had experience in devising information controls and can be of real use in compliance efforts. Their challenge lies in helping firms become and remain compliant in a dynamic environment. Perhaps the biggest lesson for everyone involved in compliance efforts is the ability to accept and adapt to change quickly and to develop flexible, sus-

tainable systems that prevent problems rather than just detect them. ■

*Julie Gable, CRM, CDIA, is the President of Gable Consulting LLC, a consulting firm specializing in compliance-based records management. She is also the Associate Executive Editor of The Information Management Journal. She can be contacted at juliegable@verizon.net.*

### Reference

Ardern, Christine and Julie Gable. “Compliance: Where Do We Go From Here?” Presentation to joint meeting of Liberty Bell Chapter of ARMA and William Penn Chapter of AIIM, 8 March 2006.

Burns, Judith. “Does It Cost Too Much to Follow the New Rules?” *Wall Street Journal*, 26-27 November 2005.

Canter, Ralph. Interview by author. 21 February 2006.

*Empowering the Financial Enterprise*. Costa Mesa, California: FileNet, circa 2003.

Greifeld, Bob. “It’s Time to Pull up Our SOX.” *Wall Street Journal*, 6 March 2006.

Hyowitz, Carol. “In Sarbanes-Oxley Era, Running a Non-profit Is Only Getting Harder.” *Wall Street Journal*, 21 June 2005.

Kolodgy, Charles J. and Christian Christiansen. “Using Security Compliance Software to Improve Business Efficiency and Reduce Costs.” Framingham, MA: IDC, June 2005.

Mammatt, Jayne. “Regulatory Compliance – Who Has all the Answers?” Ernst & Young South Africa. 8 February 2006. Available at [www.eylaw.com/global/content.nsf/South\\_Africa/08\\_Feb\\_06\\_Regulatory\\_compliance\\_%E2%80%93\\_who\\_has\\_all\\_the\\_answers](http://www.eylaw.com/global/content.nsf/South_Africa/08_Feb_06_Regulatory_compliance_%E2%80%93_who_has_all_the_answers) (accessed 27 March 2006).

Mosquera, Mary. “Agencies Gear Up for Deadlines on Internal Controls.” *Government Computer News*, 9 February 2006. Available at [www.gcn.com/online/vol1\\_no1/38227-1.html](http://www.gcn.com/online/vol1_no1/38227-1.html) (accessed 27 March 2006).

Quirk, Penny. E-mail interview by author. 6 March 2006.

Rapoport, Michael. “Financial Stars Urge Regulators to Not Dilute Sarbanes-Oxley.” *Wall Street Journal*, 21 February 2006.

Reilly, David. “Sarbanes-Oxley Changes Take Root.” *Wall Street Journal*, 3 March 2006.

Stalters, Russell. E-mail interview by author. 27 February 2006.

Tero, Vivian. Interview by author. 20 March 2006.