Whitepaper for Compliance
July 2007

Ten Things You Need to Know About Compliance

Julie Gable
Gable Consulting

Executive Summary

The compliance net is widening. U.S. companies with less than $75 million market capitalization and foreign firms registered to trade securities in the U.S. face a July 2007 Sarbanes-Oxley deadline.

Compliance is a marathon run over changing terrain. Those who win know how to conserve effort, reduce cost and position their companies over the long haul.

The SOX 404 deadline for reporting on adequacy of financial controls marked a fundamental shift in emphasis for compliance efforts. Beyond becoming compliant is the real task of remaining so. In this second phase of SOX compliance, emphasis is on adhering to the policies and procedures put in place during phase one, and on providing proof of compliance.

Becoming compliant focused on meeting external regulatory requirements and deadlines, many of which weren't well understood. While Sarbanes-Oxley is the icon of broad-based laws, it isn't alone. Anti-terrorism regulations like the USA Patriot Act and privacy laws such as Canada's PIPEDA impose broad new restrictions on the information that businesses collect, manage and use.

Well-founded fear of consequences drove early compliance efforts, and diligent enforcement continues to keep certain industries – notably financial services – in the hot seat and the headlines. Damage to corporate reputation remains real, but the drama of high-profile investigations, shareholder lawsuits and executive culpability has been replaced by subtler penalties. CEOs in handcuffs and million dollar fines are nothing compared to the chilling reality of deferred prosecution agreements, where a company's criminal liability is deferred, but its ongoing control passes to a U.S. attorney for years.

Proof of compliance is a fact of life in phase two. Inspections, examinations, reviews, investigations and litigation thrum throughout an enterprise like a migraine headache. The theme of each is fundamentally the same: What transpired, in what context, who was involved, how much was known and when? As many have found, records can either mitigate or exacerbate compliance risks – working to exonerate or convict those involved. While no laws mandate technology use, response expectations clearly do. Regulators increasingly impose time limits on the ability to produce requested information. The SEC's Office of Compliance Inspections and Examinations, for example, states that requested information must be available within 24 hours of request.

In addition to regulators, third parties have emerged with proof-of-compliance requirements of their own. Some lenders now require compliance with SEC requirements as part of debt covenants. Potential business partners, concerned

with being tarnished by association, are interested in their associates' data protection and security controls. Compliance adequacy – and the cost to remediate ineptness - has become a due diligence consideration for merger and acquisition candidates. Insurers remain anxious over shareholder lawsuits charging directors and officers with dereliction of duties, a fact reflected in D&O premiums that have risen exponentially.

Compliance phase two is marked by lessons learned. Narrowly-focused compliance efforts led by affected business units – for example a bank's customer accounts section leading its Gramm-Leach-Bliley efforts – tend to concentrate on short-term tactics for putting structures and controls in place. In this scenario, software applications purchased as point solutions to individual regulatory requirements met with limited, if any, success. Forrester Research estimates that fewer than 1,000 companies bought Sarbanes-Oxley software in 2004, and CIO Magazine (July 2005) found that those who did haven't deployed it yet. Furthermore, point solutions are proving far more expensive in the long run because each one duplicates capacity and functionality, actually making tasks associated with maintaining compliance far more complex. In short, haste to meet regulatory deadlines separately has resulted in corporate waste.

What corporate officers have learned along the path to compliance is that if information is a corporation's lifeblood, then technology is its nervous system and CIOs are responsible for overall health. Many companies quietly require CIOs to certify financial statements in advance of CEOs and CFOs. In environments that have consolidated IT operations into global resources, CIOs become the recipients of regulatory violations. Clearly, when business is conducted under scrutiny, CIOs are center stage. Here, then, are ten things to know about compliance:

1. **Orders to "Just get it done" now add "at reasonable cost."** According to a recent NYSE survey, most CEOs believe overregulation is the risk factor most likely to affect profitability over the next five years. Data from Financial Executives International shows why: SOX 404 compliance costs averaged $4.36 million in 2004, a 39 percent increase over the prior year. Meanwhile, CIOs report that 8 to 10 percent of their budgets are spent on compliance efforts. In many companies, the urgent drive to meet regulatory deadlines has given way to a sober assessment of ongoing compliance costs and the realization that such costs must be reduced.
2. **The emphasis on proof of compliance implies recordkeeping expertise.** As has been shown time and again, if the firm has the requested information, it must produce it. The implication is that the entity knows what exists, knows where to find it and can compile it quickly. Where this has not been possible, consequences have ranged from court-imposed fines and sanctions to regulatory inspectors' desire to "dig" through data stores to find what's needed. Records management capabilities are an important aspect of compliance, providing controls governing what to keep, what to safely discard and what to hold in the face of imminent enforcement or legal actions.
3. **Effective compliance is strategic, not tactical.** The case-by-case approach to compliance has resulted in complicated, redundant systems that don't interoperate, require scarce resources to update individually and incur separate maintenance costs year after year. Furthermore, multiple repositories and duplicate search services actually hamper the ability to prove compliance. As corporations realize the need for integrated compliance efforts, they also recognize the need for architecture

that provides capabilities across all compliance requirements, simplifying infrastructure and bringing much needed consistency while lowering costs.

4. **Processes are the heart of compliance efforts.** Becoming compliant required mapping and documenting them; remaining compliant – particularly doing so at reasonable cost – involves automating and monitoring them. All BPM tools provide the ability to automate workflows, incorporating input from different sources. One differentiator for compliance-oriented BPM is the ability to automatically capture and control records made during transactions and to preserve them in context. Another is the ability monitor processes in real time, sending alerts when a questionable event transpires instead of simply reporting on it after the fact.

5. **Email is inherently part of business processes.** It's hard to think of any transaction these days that is not done via email, including SOX 404 authorizations for process control changes. Simply put, emails are records and retention policies apply. The real challenge is how to associate the retention rule to the record. Email systems that rely on user intervention for capture and control are not likely to succeed, in part because of staggering volumes and because experience shows user reluctance to spend time on after-the-fact activities. Email that can be captured automatically based on business processes has particular appeal – no messages lost, all messages consistently handled, all messages searchable and producible within the context of the transaction or process. Compliance is one of the reasons industry analysts advocate using email solutions from content management vendors. One content repository for process flows, controls and records trumps relying on multiple back-up tapes when trying to reconstruct what occurred.

6. **People have different ideas about "their" information.** Proof of compliance, albeit critical in the current environment, is only one use of information. Other requirements exist, and proponents are likely to be vocal regarding their needs. The legal department, for example, has to respond quickly to litigation discovery requests, produce irrefutable evidence in the company's own defense, and assure that "smoking guns" don't lurk in uncontrolled repositories. IT, pressured to show solid evidence of control and reduce costs, legitimately raises issues with total cost of ownership, a point underscored by the fact that every dollar spent on storage requires $3 to $8 in administrative costs. Records managers' concerns cover authenticity and reliability of information maintained only in electronic form – a particular challenge for records that require retention over decades. Users just want access to the information they need to do their jobs. The point is to consider all uses of information – for compliance and beyond.

7. **Standards (and products based on them) can help.** Standards provide guidance for meeting regulatory requirements. In the U.S., the COBIT standard is a collection of management principles aimed primarily at IT functions; in the UK, the Conduct of Business (COB) standard provides useful guidance for complying with Financial Services Authority regulations. Standards also provide frameworks and best practices that can be useful in resolving internal differences of opinion. ISO 15489 is a widely adopted international standard that takes a process approach to managing records, providing a framework to ensure that adequate records are created, captured and stored. Software applications developed to manage records should adhere to either the Department of Defense's 5105.2 standard or the Model Requirements of the European Union.

8. **ROI is possible.** Benchmarking analysis by the General Counsel Roundtable shows that each dollar of compliance spending saves, on average, $5.21 in avoidance of legal liabilities, reputation damage and lost productivity. Other studies show annual savings of nearly $250,000 from automated records capture and management for as little as 100 users. Reduced legal

discovery costs are also possible. DuPont, in a five-year study of discovery response, found that it could have avoided $12 million in review and processing costs for documents that were past retention – if they had complied with their own internal policies. In some industries, significant advantages are possible: Compliance with Basel II, a guideline for international banking, allows reduction of loan reserves – currently about $.08 on the dollar – for banks that can demonstrate control over operational risk.

9. **Balance controls and risks.** In the last round of compliance, lack of regulatory interpretation resulted in uncertainty about what was really required. The result was an overabundance of controls aimed at mitigating all risks great and small. Many CIOs now realize that controls put in place must be sustained, checked and measured - some through manual efforts such as examining audit trails – and they are looking for ways to streamline these tasks. Eliminating unnecessary controls and automating others will help somewhat, but practical reductions in reporting time will only be possible through real-time monitoring of key processes and controls. Aside from using fewer resources, pro-active monitoring reduces risk by catching potential problems before they worsen – something that can't be done from audit trails.

10. **Cost-conscious compliance and enforcement requires an integrated framework.** At its core, compliance requires the ability to govern processes, monitor controls, capture content, attach retention rules, search for and produce reliable evidence, and report as required. Each capability involves fundamental elements that must be tweaked according to each regulation's current and future provisions. Compliance today is difficult because businesses are forced to retrofit capabilities to systems originally acquired to enhance productivity, a focus based on access to information rather than control of it. What's needed is an architecture that delivers services for both production and control. Best bets are solutions that offer integrated content repositories, records and email retention, process management capabilities and active monitoring features.

The compliance net is widening. U.S. companies with less than $75 million market capitalization and foreign firms registered to trade securities in the U.S. face a July 2007 Sarbanes-Oxley deadline. Transparency of corporate governance has also crossed the pond, with European Union firms facing compliance with International Financial Reporting Standards by January 1, 2006. Government agencies must comply with Office of Management and Budget Circular A-123, which defines responsibilities for agencies' control over financial reporting by August 15, 2006.

Whether just starting out or midway through the race, one thing is clear: Rather than a quick sprint to the deadline, compliance is a marathon run over changing terrain. Those who win know how to conserve effort, reduce cost and position their companies over the long haul.

References:

Martinez, Barbara and Joann S. Lublin, "Why a Lawman Wields Authority Over Drug Maker," The Wall Street Journal, 20 June 2005.

"24-Hour Turnaround of E-Mail Requests Poses Problems for Investment Advisers," Digital Discovery & e-Evidence, Pike & Fischer, 9 March 2005.

Worthen, Ben. "How to Dig Out from Under Sarbanes-Oxley," CIO Magazine, 1 July 2005.

CEO Agenda 2006: New Realities for Global Leaders, August 2005. Publication details available at http://www.nyse.com/about/publication/1112010226998.html?sa_campaign=/internal_ads/midhomepage/0916ceoagenda

"FEI Survey: SOX 404 Compliance Costs Up 39%," at http://www.fei.org/404_survey_3_21_05.cfm

Stephens, David O. and Roderick C. Wallace. Electronic Records Retention: Strategies for Data Life Cycle Management. ARMA International, Lenexa, KS, 2003.

"Integrity-driven Performance," PriceWaterhouse Coopers white paper, 2004.

"Risk Reduction with Cost Reduction: A New Perspective on Cost Justifying 'Best Practices' ERM Programs," presentation by J. Michalowicz at Managing Electronic Records, Chicago, September 2002.

"Review of FileNet Records Manager," Cohasset Associates, May 2004.

Brewer, Cass, "One More Year: New SOX Deadline for SMBs and Foreign Filers," available at http://www.itcinstitute.com

Martin, Steven, "Sarbox Redux," Compliance Pipeline, 1 September 2005, available at www.compliancepipeline.com.

IBM Corporation
3565 Harbor Boulevard
Costa Mesa, CA 92626-1420
USA

Printed in the USA

07-07

For more information, visit **ibm.com**/software/data/cm.

IMW12875-USEN-00