



## Compliance Becomes A Top Concern

In the arena of corporate governance and compliance, the Sarbanes-Oxley Act (SOX) has commanded considerable attention, and deservedly so. Developed in response to accounting scandals that rocked the corporate world, SOX is aimed at improving the transparency and accuracy of financial accounting and record keeping of U.S. publicly traded companies.

But SOX is just one of many federal mandates facing U.S. companies. In the healthcare industry, there's the Health Insurance Portability and Accountability Act (HIPAA). In the financial services industry, regulations now require T + 1 ("transaction date plus one") settlement of financial transactions. And the energy sector was targeted in recent legislation, with a number of new mandates from the Federal Energy Regulatory Commission, the Nuclear Regulatory Commission and the EPA.

Many organizations are now developing compliance strategies that will enable them to meet their statutory obligations while also minimizing the disruption of day-to-day operations and the impact on employees. Companies are also looking for ways to keep the costs of compliance to a minimum, and this is where technology has a role to play.

Organizations can use technology to meet compliance demands in a cost-effective way. Software products have emerged in several technology segments in response to emerging regulatory requirements.

## The Fit Between Compliance and Technology

Corporations have been put on notice: Government agencies and industry self-regulatory bodies will be adamant in enforcing new regulations and have set strict deadlines for organizations to meet the requirements. While some deadlines have already passed, such as HIPAA privacy safeguards (impacting all but the smallest health care providers) and provisions of the Gramm-Leach-Bliley Act (affecting financial institutions), others are still to come.

The compliance deadline for Sarbanes-Oxley section 404 has been extended to the first statements of a company's fiscal year ending after June 15, 2004. Some HIPAA deadlines applicable to small health-care providers go out as far as 2006. But failure to act within the timelines can mean hefty financial penalties as well as possible imprisonment. Failure to comply with HIPAA can cost up to \$250,000 and 10 years in prison (ouch!). And the SOX penalties are even greater — up to \$5 million or 20 years in prison. Similarly large fines have been imposed for not following regulations such as SEC rule 17a-4, which applies to e-mail management within broker-dealer organizations. The imperative is clear: comply, or else.

To avoid penalties, it is important to understand the specifics of requirements. For example, SEC Rule 17a-4 states that broker-dealers must preserve all electronic records "exclusively in a nonrewritable, non-erasable format." (It almost goes without saying that these, and all other corporate records, be retained only as long as legally required, after which time they are destroyed.) The rule also requires, however, that broker-dealers be able to produce those records in a timely manner in the event of an audit or regulatory investigation. This combination of requirements places enormous demands on a financial institution that can only be met with specific technologies.

Other regulations, such as Sarbanes-Oxley sections 404 and 409, involve monitoring and reporting on content as well as the process of managing information. Although some of the technology requirements overlap, there are additional capabilities needed. Specifically, these regulations require process management and monitoring of the information, not just storage and retrieval.

SOX was enacted to ensure that U.S. publicly owned companies establish and maintain internal controls, as outlined in Sections 103-a and 404-b of the regulation.

## The Silver Lining

While organizations may regard the ever-growing (and ever-changing) list of regulatory requirements as a daunting challenge, the ECM and BPM technologies that can ease compliance can also provide a range of significant business benefits. For starters, any organization that undertakes a strategic compliance initiative will realize many other benefits that come from effective management of information and a better understanding of business processes.

BPM solutions allow an organization's processes to be fully documented and accompanied by transaction audit trails, putting business managers in a better position to make decisions. BPM also documents the policies that state exactly what needs to be done as well as the procedures that specify how policies should be implemented. Organizations can use this information to continuously improve their processes through the adoption of a full life-cycle process management practice (along the lines of Six Sigma), which, in turn, helps maintain competitive advantage.

Another incremental benefit of implementing technologies for compliance is often improved support for litigation discovery. It's not uncommon for companies to settle litigation out of court rather than defend against it because settling is likely to be less time-consuming, less resource-intensive and, therefore, less costly. But companies using ECM effectively can be more assured of being able to access information requested in a legal discovery process. ECM also provides an advantage for gathering information needed for audits or for ensuring business continuity in the event of fire, flood or other disasters.

Finally, the combination of organized content and enhanced and automated business processes provides improvements in operational efficiency by reducing manual processing and routing, reducing paper storage and providing faster access to key documents for customer service. These gains can bring not only millions of dollars in savings for large organizations, but also increased revenue through improved customer satisfaction and retention.

## Looking Ahead

With deadlines for compliance fast approaching, organizations clearly need to take action now. Surprisingly, however, a recent poll by the Business Process Management Institute indicated that only 27 percent of those organizations polled are taking steps to comply with SOX, and only 11.5 percent are taking action to do something about HIPAA. Here are some basic recommendations:

- Know your regulations. This includes both those related to public and private companies in general, and those that are specific to your industry.

- Develop your enterprise strategy and plan for compliance. Make sure your strategy encompasses both processes and content, since both are necessary to ensure compliance.

- Document your retention policies, procedures and schedules. This is important not only to prove to the regulatory bodies that you have them, but also to communicate these policies, procedures and schedules to your employees so they can follow them.

- Determine your specific requirements for a technology solution to enable you to implement your enterprise compliance plan and support your retention policies and your processes.

- Assess your current technology to determine if it meets your requirements and where gaps may exist.

- Research the additional technology needed and procure and implement it as required.

With risk reduction now a business requirement, it's likely that these organizations will find good reason to take another look at these technologies. Eventually, most laws will have test cases that provide further enlightenment by showing what the regulator considers a violation. The goal is to make sure that your company isn't the test case.

\* Sources used Transform Magazine, AIIM EDoc Magazine and DocumentIQ.

LEADING COMPLIANCE STANDARDS, LAWS & REGULATIONS

Item	Definition	Affects	Highlight	More Info/Comments
SEC 17a-4	Store Electronic Records on non-rewritable, nonerasable format. Records retention; ability to capture, store and manage correspondence/communications regarding business transactions	Financial services such as brokers, dealers, exchange members	Gives retention periods for securities broker/dealer records; stipulates requirements if electronic record-keeping systems are used	Does not make technology use mandatory; Mentions imaging but does not stipulate it as the only usable technology
Sarbanes-Oxley 404	Monitoring of the process involved in producing and changing financial records	All publicly traded companies, public accounting firms, auditors, brokers, securities analysts	For public companies, provides requirements for audit committees, financial reporting, insider trading, executive loans, change disclosure and management's assessment of controls	Final rules for particular sections emerging, for example, Section 404 now requires assessment of financial controls rather than internal controls; Deadlines extended to 2004 for large companies, 2005 for small companies.  More information: <a href="http://www.sarbanes-oxley.com/">http://www.sarbanes-oxley.com/</a> <a href="http://www.sec.gov/news/press/2002-128.htm">http://www.sec.gov/news/press/2002-128.htm</a>
Sarbanes-Oxley 409	Disclose information on material changes in the financial condition or operations of the issuer on a rapid and current basis	All publicly traded companies, public accounting firms, auditors, brokers, securities analysts	"Same as Sarbanes-Oxley 404"	Library services on content with the ability to track changes  More information: <a href="http://www.sarbanes-oxley.com/">http://www.sarbanes-oxley.com/</a> <a href="http://www.sec.gov/news/press/2002-128.htm">http://www.sec.gov/news/press/2002-128.htm</a>

HIPAA	Protects "Individually identifiable health information" that is, any data identified by name, social security, address or birth date whether it is electronic, paper or oral. Also requires patient notification of privacy policies.	Health plans, including employer-sponsored health and all healthcare providers that transmit patient information electronically for claims, benefit eligibility, referral authorizations, etc.	Security rule, effective April 21, 2005, requires best practices for assuring that electronic patient data is confidential, available as needed and maintained with integrity intact.	For more information: <a href="http://www.hep-c-alert.org/links/hippa.html">http://www.hep-c-alert.org/links/hippa.html</a> <a href="http://www.hhs.gov/news/press/2002pres/hipaa.html">http://www.hhs.gov/news/press/2002pres/hipaa.html</a>
Check 21	The law facilitates check truncation by creating a new negotiable instrument called a substitute check, which would permit banks to truncate original checks, to process check information electronically, and to deliver substitute checks to banks that want to continue receiving paper checks.	Banking Institutions	The Law was signed into law on October 28, 2003, and will become effective on October 28, 2004. The law does not require banks to accept checks in electronic form nor does it require banks to use the new authority granted by the act to create substitute checks.	For more information: <a href="http://www.federalreserve.gov/paymentsystems/truncation/default.htm">http://www.federalreserve.gov/paymentsystems/truncation/default.htm</a>

<p>IRS Rev. Proc. 97-22</p>	<p>Provides guidance to taxpayers that maintain books and records by using an electronic storage system that either images their hardcopy (paper) books and records, or transfers their computerized books and records, to an electronic storage media.</p>	<p>Financial Services</p>	<p>An electronic storage system must ensure an accurate and complete transfer of the hardcopy or computerized books and records to an electronic storage media The electronic storage system must also index, store, preserve, retrieve, and reproduce the electronically stored books and records.</p>	<p>For more information: <a href="http://www.recapinc.com/irs_97-22.htm">http://www.recapinc.com/irs_97-22.htm</a></p>
<p>Gramm-Leach Bliley Act</p>	<p>Requires financial services companies to implement safeguards for customers' current and legacy information.</p>	<p>Financial services such as brokers, dealers, exchange members</p>	<p>In essence, the act makes it illegal for a financial institution to share customers' "nonpublic personal information" with third parties unless the company first discloses its privacy policy to consumers and allows them to opt-out of that disclosure.</p>	<p>For more information: <a href="http://www.senate.gov/~banking/conf/">http://www.senate.gov/~banking/conf/</a> <a href="http://www.ftc.gov/privacy/glbaact/">http://www.ftc.gov/privacy/glbaact/</a></p>

21 CFR 11	Defines the recommendations for managing audit trails, access control and electronic records retrieval.	Healthcare and Pharmaceuticals	On February 20, 2003, the FDA released a new draft--Draft Guidance for Industry; Part 11, Electronic Records; Electronic Signatures - Scope and Application which changes the requirements for electronic records. It also withdraws many previous guidance documents on maintenance of records, e-copies of records, timestamps and validation.	For more information: <a href="http://www.21cfrpart11.com/">http://www.21cfrpart11.com/</a> <a href="http://www.fda.gov/ora/compliance_ref/part11/">http://www.fda.gov/ora/compliance_ref/part11/</a> <a href="http://www.fda.gov/cber/gdlns/prt11elect.pdf">http://www.fda.gov/cber/gdlns/prt11elect.pdf</a>
Dept. of Defense 5015.2, version 2	Defines the basic requirements based on operational, legislative and legal needs that must be met by records management application (RMA) products acquired by the Department of Defense (DoD) and its Components	Vendors of electronic records management software and document management products paired with RM software	Testing and certification program for software products	Many gov't entities require RM software to comply with this standard. For a register of DoD certified products, see <a href="http://jitc.fhu.disa.mil/recmgt/">http://jitc.fhu.disa.mil/recmgt/</a>

Government Paperwork Elimination Act	Requires federal agencies to accept electronic information and transactions. It also requires that they maintain electronic records	Federal Agencies	This work must be completed by October 21, 2003.	For more information: <a href="http://www.whitehouse.gov/omb/fedreg/gpea2.html">http://www.whitehouse.gov/omb/fedreg/gpea2.html</a> <a href="http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html">http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html</a>
NASD 3010 & NYSE 342	Requires member organizations to establish and maintain a system of supervision, demonstrate that their system is complete, evaluate it on a regular basis and ensure that it remains effective	Members of the National Assoc. of Securities Dealers (NASD) and New York Stock Exchange (NYSE)	Record-keeping requirements concerning e-mail communications	More information: <a href="http://www.sec.gov/news/press/2002-173.htm">http://www.sec.gov/news/press/2002-173.htm</a>