FOCUS

Compliance

A Requirements Primer

GEORGE W. BEELER, JR.,
BEELER CONSULTING
and DANA GARDNER,
INTERARBOR SOLUTIONS

Many software engineers and architects are exposed to compliance through the growing number of rules, regulations, and standards with which their employers must comply. Some of these requirements, such as HIPAA (Health Insurance Portability and Accountability Act), focus primarily on one industry, whereas others, such as SOX (Sarbanes-Oxley Act), span many industries. Some apply to only one country, while others cross national boundaries. To help navigate this often confusing world, *Queue* has assembled a short primer that provides background on four of the most important compliance challenges that organizations face today.

SOX

The Sarbanes-Oxley Act of 2002 can be tidily summed up as trying to answer the not-so-simple question, “Says who?” when it comes to proper corporate financial reports. Because of a spate of major corporate and accounting scandals at the turn of the century—perhaps best punctuated by the collapse of Enron and Arthur Andersen—Sarbanes-Oxley, or SOX, was designed to shore up public and investor confidence in financial reporting.

Yet the sometimes-unanticipated consequences of the act’s 11 sections, which range from stepped-up responsibilities for corporate governance boards to criminal penalties for violators, have been far-reaching—and not always considered productive. Costs associated with SOX compliance have been blamed for muting the market for IPOs (initial public offerings), quelling the venture capital climate for incubating start-ups, as well as causing at least a short-term drag on the U.S. gross domestic product.

Named for Congressional sponsors U.S. Sen. Paul Sarbanes (D-Md.) and U.S. Rep. Michael G. Oxley (R-Ohio), the act was overwhelmingly approved by a vote of 423-3 in the House and 99-0 in the Senate. It marks the most sweeping change in corporate governance regulations since the aftermath of the Great Depression of the 1930s.

SOX mandates new or enhanced standards for all U.S. public company boards, management, and the public accounting firms that service, audit, and advise them. In essence, the act defines proper corporate governance, who should monitor such governance and how it should be monitored, and sets up the means to enforce proper standards for compliance and establish culpability for noncompliance.

As part of that good governance umbrella, the SEC (Securities and Exchange Commission) has gained new strength through SOX to make rulings on corporate behavior that does or does not comply with the new law. SOX also established a new authority, the PCAOB (Public Company Accounting Oversight Board), which oversees and, when needed, disciplines accounting firms as they audit public companies.

In addition to creating the PCAOB, the law requires public companies to evaluate and disclose the effectiveness of their internal financial reporting controls, as well as to have independent auditors “attest” to the validity of these measures. Companies must also have their chief

executive officers and chief financial officers regularly certify the financial reports.

As a reform measure, the act more purely defines auditor independence by excluding certain types of work between clients and auditors. To obviate even the appearance of conflicts of interest, SOX requires that public companies have committees just to oversee the relationship between the company and the auditors. SOX disallows most personal loans to executive officers and directors, any nonreporting of stock trades by insiders, and insider trades during pension-fund blackouts.

Those caught improperly dipping from the well of inside knowledge or knowingly and willfully misstating financial results face stiff criminal and civil penalties, including jail time and fines, for violating securities laws under SOX.

Although SOX is sometimes derided for causing an economic penalty through significant additional levels of regulation, tracking, and monitoring, it has also juiced up the industries around products and services to assist in defining and implementing corporate governance and achieving SOX compliance. For example, vendors supplying computing systems and software to track, update, and manage reporting processes and data have benefited. Systems in hot demand have included those for document management and financial data access, as well as storage systems for archiving additional financial information.

These SOX-related costs have amounted to millions of dollars for large corporations. Ironically, among the biggest beneficiaries, at least during the opening years of SOX, have been the accounting firms themselves, the result of a spike in demand for audits and governance-related services.

Companies that may have assumed that SOX compliance was a one-shot affair or a project-based activity may be in for a surprise. Studies and recommendations from management consulting firms are pointing to a long-term effect from SOX: the necessity to create an ongoing SOX-compliance layer that becomes a fixture of large publicly traded companies—that is, until some future concentration of corporate scandals forces yet another reevaluation and remediation of the status quo. —DG

SARBANES-OXLEY

BASEL II

Although full implementation of the international Basel II accord for improved banking capital management is not due until 2008, its impact is already being felt. Aimed at preventing international banking crises and reducing the risk from a highly fractured approach to banking across many countries, Basel II (officially known as the International Convergence of Capital Measurement and Capital Standards—A Revised Framework) augments the first Basel accord, adopted in 1988.

The 13 countries that make up the Basel Committee on Banking Supervision have been working since 1999 to revise the international standards and methods for jibing banks' capital expectations with economic reality. The risk of banking missteps has increased in recent years along with globalization. Markets are no longer defined by borders but in fact consist of many countries, with many banking systems and regulatory definitions.

By creating more consistency in how banks and regulators in as many as 100 countries manage risk in terms of capital and demands, Basel II is designed to forestall and prevent unanticipated failures—and the harmful domino effect of additional failures that sometimes follow one bank's or region's failure. Basel II is also aimed at preventing regulators from finding ways around banking best practices and making the global approach to banking systemic rather than spotty in definition, measurement, or enforcement.

Designed to encourage stability in the international financial system, Basel II is tasked with reducing risk by making sure capital is allocated prudently. The accord also fosters better measurement and management of credit risk and isolates it from a bank's operations. Furthermore, Basel II makes aggressive regulatory oversight imperative in more instances and in concert with regional and international best practices. Specifically, Basel II's "three pillars" consist of minimum capital requirements, improved supervisory review, and greater market discipline. For example:

- Pillar one aims to better calculate the proper capital requirements for banks' credit risks, operational risks, and market risks, and encourages the use of advanced data collection and sophisticated risk management techniques.
- Pillar two gives regulators additional means over Basel I to manage banking risk issues and expands the scope of

what regulators can enforce under such residual risks as liquidity and legal risks.

- Pillar three mandates far greater disclosure from banks to provide markets with warnings or assurances on how the banks are actually faring.

It was only in June 2006 that a comprehensive version of all Basel II accords, based on the June 2004 final framework, was published. Preliminary work is already under way on Basel III, with these early goals: better defining what constitutes bank capital, further quantifying types of risk, and mandating the use of additional tools to manage and measure banking missteps.

The Basel accords are not without critics. By joining many banks together in a timed and mandated risk evaluation process, critics fear that Basel II will exacerbate economic downturns because many more banks will simultaneously squeeze credit in like fashion, based on similarly perceived risks and regulatory mandates. Smaller banks cry out that the new system favors larger financial institutions, because they are better able to absorb the costs of change. Developing economies object that the Basel II requirements, in effect, make credit more expensive than when today's mature economies were in a similar state of growth.

By working to eliminate regional crises and rapidly escalating failures, however, Basel II should ultimately reduce the long-term ill effects of a Swiss cheese approach to banking regulations. Developing countries will face less severe crashes, and credit access should improve because of far less overall risk and more transparency in the global system. —DG

DANA GARDNER (dgardner@interarbor-solutions.com) is president and principal analyst at Interarbor Solutions of Gilford, New Hampshire, an IT industry market research and consulting firm. A prolific blogger and podcaster, Gardner covers application development and deployment strategies, services-oriented architecture, and software infrastructure. He also advises clients on RSS, viral marketing, and podcast content creation strategies. He is a former Yankee Group analyst, and a former editor at large of *InfoWorld*.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (affectionately known as HIPAA) dealt with several issues surrounding health insurance. As its name suggests, one issue was the ability of persons who had health coverage through an employer to maintain that coverage (“port” it) when they changed employment.

In the computing industry, HIPAA is better known for its Administrative Simplification section. This section mandated that the information for managing health-care financial claims and reimbursement be communicated with EDI (electronic data interchange) using data interchange standards recognized by ANSI (the American National Standards Institute). The objective was to enhance the speed and effectiveness of the claims process, thereby reducing the back-office costs of providing and financing health care.

Data interchange standards specify the structure and content of messages or data sets being sent from one computer system to another. These standards are implemented in software that assembles the messages from data sources (files and databases) in the originating system, and in other software that parses the message and places the data in the files and databases of the receiving system. Data stores on the originating and receiving systems rarely have identical structure. As a consequence, data interchange commonly requires that the data be transformed twice: once when the message is assembled at the originating site, and again when it is parsed at the receiving site.

The ASC X12N (the Accredited Standards Committee’s subcommittee for insurance) developed and approved core standards specified for HIPAA Administrative Simplification during the early 1990s. Supporting standards were those of the Dental Content Committee of the American Dental Association, Health Level Seven, the National Council for Prescription Drug Programs, the National Uniform Billing Committee of the American Hospital Association, and the National Uniform Claim Committee of the American Medical Association. These six organizations are listed in the HIPAA regulations as the designated standards maintenance organizations supporting HIPAA. They maintain and operate a transaction change request system for receiving and reviewing publicly proposed changes for the sets of standards that are mandated for HIPAA (see <http://www.hipaa-dsmo.org/>).

The original legislation called for implementation in summer 1999. The actual process took more than twice as long, with the first compliance deadlines occurring in fall 2002. Standardized data interchange is now largely complete.

As the delayed schedule suggests, the course of implementation has not always been smooth. The thorniest issues surround rules for data privacy and security. Today more people know of HIPAA for its privacy and security rules than for its EDI impact. (Indeed, a Google search on the single term *HIPAA* will take you to a Department of Health and Human Services Web page whose primary title is “Medical Privacy—National Standards to Protect the Privacy of Personal Health Information.”)

Detailed, individual health data has always been part of the paper trail needed to support health insurance claims. The requirement to communicate this data electronically between the computers of independent corporations (health-care providers, insurers, and intermediaries) raised questions of who owns and controls the data, and who is ultimately responsible for it. The government took several years to create privacy and security regulations, then get them approved and implemented. From the consumer’s perspective, these regulations are just a new set of forms that health-care providers ask them to sign authorizing the release of information for claims purposes.—GB

HL7

HL7 (Health Level Seven) is a not-for-profit organization formed “to create standards for the exchange, management, and integration of electronic healthcare information.” HL7 consists of both individual and corporate members, including health-care providers, software developers, medical informaticists, and consultants.

When HL7 was founded in 1987, its members needed data standards to link multiple computer systems within large hospitals or medical centers. These systems were introduced to help manage the laboratory and patient administration functions of those institutions. The first HL7 standards, known as HL7 Version 2, have grown and matured. Today they are used in more than 95 percent of large health-care institutions in the United States and are broadly implemented in other countries.

In 1994, HL7 modified its consensus practices to meet the criteria of ANSI (the American National Standards Institute). HL7 then sought and received accreditation from ANSI as a standards developing organization. All HL7 standards developed since then have been registered as American National Standards.

As early as 1992, organizations in other countries sought accreditation as HL7 International Affiliates so that they could use and publish the standards and create implementation guides appropriate to their regions. This program has grown dramatically in the last decade. Today there are affiliates in more than 26 countries, with participants from every continent except Antarctica. The affiliate members have taken active, important roles in defining and developing new HL7 standards that meet the needs of a broader range of health-care computing environments.

About 10 years ago, HL7 recognized the need to create a more stable and durable foundation for the standards it was developing. It began working on HL7 Version 3, which is a family of data interchange standards based on a single RIM (reference information model) and a common set of vocabulary (terminology) specifications.

To support Version 3 development, HL7 created a formal methodology for defining these model-based standards. The methodology is similar to modern software development methodologies. The standard data structures are defined as abstract UML-compliant static information models derived from a single semantic model of health information. This model is the HL7 RIM adopted

as an HL7-ANSI standard three years ago and will become an ISO standard in the near future.

Every year, HL7 publishes a Normative Edition of all Version 3 specifications that have been balloted and reached normative status. The 2006 edition includes all of the core specifications for the RIM, vocabulary, data types, and communication wrappers, plus detailed specifications for patient administration, accounting, claims personnel management, scheduling, records management, public health, clinical genomics, and clinical trials.

The challenge in creating standards for communication of clinical data is to assure that the standard data structure can convey the complete clinical context for the data. Context not only includes who observed what about whom, but may also involve why the observation was made, what other conditions affect the subject, where the observation was made, etc.

HL7 Version 3 expresses this contextual information by providing explicit data relationships as part of the structure and encoding the nature of each contextual relationship in HL7-defined vocabulary terms. This contrasts with HL7 Version 2 (and similar early standards) where the contextual relationships were implicit rather than explicit, and thus were at risk of being misinterpreted. As a result, the Version 3 structures can communicate a complete health record, whereas the Version 2 structures are more appropriate for communicating record fragments.

Because HL7 Version 3 can support the complete representation of clinical data and because of the efficiencies seen when implementing model-driven standards, Version 3 has been designated as the primary standard for national health-record projects in a number of countries, including England, Canada, Germany, the Netherlands, Japan, and Korea. —GB

GEORGE W. BEELER, JR., PH.D. (woody@beelers.com) is president of Beeler Consulting LLC. He is a member of the emeritus staff of Mayo Clinic, Rochester, Minnesota, where he held leadership roles in clinical computing and medical informatics. He has been active in HL7 for the past 13 years. He served on the HL7 board for nine years, was board chair for two years, and is currently a co-chair of the Modeling and Methodology Committee that oversees Version 3.

© 2006 ACM 1542-7730/06/0900 \$5.00