Preface

The current business environment is replete with governmental regulations and standards for best practices. In the United States, for example, the Sarbanes-Oxley Act of 2002 (SOX) contains new regulations for accounting practices of public companies, whereas the Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains regulations concerning access to health care as well as the use and dissemination of health-care information. There are also a number of voluntary standards, such as ISO 17799 from the International Organization for Standardization, which contains a code of practice for information security management. Because the costs associated with noncompliance can be significant, businesses are looking for ways to effectively manage their compliance requirements.

This issue of the *IBM Systems Journal* contains nine papers and a *Technical Forum* on compliance management, and they are grouped under four major topics: 1) risk management, 2) privacy and data protection, 3) development, and 4) auditing and reporting. The *Technical Forum* section contains a paper on the role of WORM (write once read many) devices in trustworthy record keeping. We thank the issue coordinators, Charles Palmer and David Medina, for their leadership in planning and producing the issue.

The first two papers of this issue focus on risk management. In “Seeing is believing: Designing visualizations for managing risk and compliance,” Bellamy et al. argue that visually oriented user interfaces can facilitate the management of complex, distributed processes. Their paper shows the application of this idea to compliance management by describing the design and pilot deployment of a visualization tool to support SOX compliance in IBM. In “Optimized enterprise risk management,” Abrams et al. discuss the concept of enterprise risk management (ERM), a process that is integrated (spans all lines of business), comprehensive (includes all types of risk), and strategic (is aligned with the overall business strategy). They present a framework for implementing ERM in which the enterprise and its environment are captured by a five-layer model; the enterprise spans the three middle layers (strategy, deployment, and operation) and reaches into the events layer, whereas the environment is represented by the jurisdiction layer and in part by the events layer.

The next two papers cover privacy and data protection. In “Best practices and tools for personal information compliance management,” Kudo et al. describe two tools they developed to support compliance with regulations concerning the handling of personal data, such as the Japanese Personal Information Protection Act of April 2005. Whereas aDesigner scans an entire Web site and determines whether each Web page complies with IBM’s privacy guidelines, the Personal Information Detection tool (PID) is capable of automatically identifying “named entities,” such as names, addresses, or telephone numbers, in Japanese documents. The authors also present statistics from the personal information gathered through the deployment of these tools. In “Compliance with data protection laws using Hippocratic Database active enforcement and auditing,” Johnson and Grandison describe an integrated set of technologies, known as the Hippo-

0018-8670/07/$5.00 © 2007 IBM

cratic Database (HDB), that enable compliance with security and privacy regulations without impeding the legitimate flow of information. HDB allows fine-grained disclosure policies to be defined, transparently enforces these policies by transforming user queries in a middleware layer to ensure that the database returns only policy-compliant information, and efficiently tracks all database accesses for monitoring and auditing.

The next two papers relate to software development. In "A survey of static analysis methods for identifying security vulnerabilities in software systems," Pistoia et al. cover three areas that have been associated with sources of security vulnerabilities: access-control, information-flow, and application-programming-interface (API) conformance. For each type of security vulnerability they present their findings in two parts: first, they describe recent research results, and then, they illustrate implementation techniques by describing selected static analysis algorithms. In "Ariadne: An Eclipse-based system for tracking the originality of source code," Luo et al. introduce Ariadne, describe its architecture within the Eclipse framework, the originality metadata that it keeps track of, and the data structure used to implement the tracking mechanism. They demonstrate the tool's functionality in two typical scenarios: tracking of software bugs and generating Certificate of Originality reports.

The next three papers deal with auditing and reporting. In "Role of an auditing and reporting service in compliance management," Ramanathan et al. describe a technology for handling audit data. They describe mechanisms to submit, collect, store, archive, restore, and create reports on audit data. They demonstrate the benefits of this technology through scenarios in which they show how reports created by this service, embedded in an IBM product, can be used to establish compliance. In "Addressing the data aspects of compliance with industry models," Delbaere and Ferreira focus on the problems encountered by enterprises when the data required for compliance with regulations are generated in incompatible formats or at the wrong level of detail, or when data requirements of overlapping regulations are inconsistent. They propose an approach to this problem based on establishing enterprise-wide data standards, and they illustrate this approach with examples from the banking industry. In "A static compliance-checking framework for business process models," Liu, Müller, and Xu investigate the possibility of automatically verifying that a business process complies with a set of requirements. Business process models expressed in the Business Process Execution Language are transformed into pi-calculus and then into finite state machines. Compliance rules captured in the graphical Business Property Specification Language are translated into linear temporal logic. Then, process models can be verified against the compliance rules by means of model-checking technology for finite state systems.

In the *Technical Forum* paper "WORM storage is not enough," Hsu and Ong argue that simply storing records in WORM storage is not sufficient for trustworthy record keeping and that more research is needed for developing a holistic approach to the problem that covers not only storing, but also discovery and delivery of data.

The next issue of the *IBM Systems Journal* is devoted to IBM Service Management.

Alex Birman, Associate Editor

John J. Ritsko, Editor-in-Chief