

# GUIDELINES FOR COMPLIANCE WITH SARBANES-OXLEY

VASANT RAVAL

*SOME OF THE MEASURES ONE MIGHT SELECT TO COMPLY WITH THE LETTER OF THE LAW MAY TURN OUT TO BE AD HOC, ISOLATED PATCHWORKS RATHER THAN INTEGRATED SOLUTIONS THAT YIELD LONG-TERM BENEFITS.*

Over the past few years, cases of miserable failure in corporate governance have shocked the financial world. Enron and WorldCom are just two examples of how a few people in a position of power can cause unprecedented damage to hundreds of thousands of people, including investors, employees, and retirees. Lessons thus learned created a wave of regulations, the most significant being the Sarbanes-Oxley Act of 2002, the first major overhaul in the area of securities since the Securities Exchange Act of 1934.

A reading of piles of pages of the act and its numerous interpretations does not reveal any explicit links between information resource management and corporate governance. After all, how you comply with the act's provisions is not dictated. However, a careful study of the act and its requirements suggests that, in the absence of information technology's involvement, some of the measures one might select to comply with the letter of the law may turn out to be ad hoc, isolated patchworks rather than integrated solutions that yield long-term benefits.

Information executives are used to their role in compliance of regulations. HIPAA (Health Information Portability and Accountability Act) is a recent legislation that requires systemic steps to ensure data security and information privacy by covered entities. Aside from regulations, information executives have seen the transition to Euro as a force behind system-wide revisions for some, and Year 2000 (Y2K) compliance to ensure that systems are viable in 2001 and beyond. Such changes impact many systems and applications in various organizations, and to accommodate them is a part of the role of information executives.

The Sarbanes-Oxley Act (SOA) applies to those corporations (in the United States and abroad) whose securities are publicly traded on the U.S. financial markets (e.g., NYSE and NASDAQ). The spirit of the provisions of the act is to require the issuer of securities to create a risk management model for its stakeholders, mainly the investor. In this regard, even for a non-publicly traded organization, some of the provisions of the act might be helpful to review and, if appropriate, implement.

## CORPORATE GOVERNANCE AND INFORMATION SYSTEMS

In simple terms, corporate governance has to do with managing the risks of doing business, and thus protecting the stakeholders of the corporation. A comprehensive, enterprisewide risk management is the main purpose of corporate governance. Aside from the inherent risk implicit in the nature of business, a business firm's risks can be identified with its systems, both manual and automated. A corporation comprises many systems, two of which are the most significant: operational system and information system. The two are more like two sides of the same coin. Operations are supported by information and at the same time, operations are a source for data. Risks emerge from operations, information systems, or from the relationship between the two. To manage the risks, one needs to control the corresponding system. Consequently, there is a link between risk management and systems management.

AMRResearch recently released results of a survey of Fortune 1000 companies ([www.Amrresearch.com](http://www.Amrresearch.com)) concerning compliance with the SOA. The results revealed that "85 percent of companies are planning for changes to their IT systems to support compliance efforts, and Fortune 1000 companies will spend \$2.5B this year both in planning and executing SOA-related efforts." For most companies, the SOA compliance requirements are also an opportunity to improve their systems and processes, increase systems reliability and data security, and enhance technology's productivity.

## FINANCIAL AND NON-FINANCIAL SYSTEMS

Although the overwhelming emphasis of the SOA is on financial systems — their inputs, processes, and outputs — the reality is that these financial systems are neither manual nor stand-alone in almost all cases. Consequently, financial — or accounting — systems are a part of the portfolio of information systems intertwined with each other, such as customer relationship management, human resource management, and supply-chain management. Increasingly, business information systems have moved to net-centric environments, where operational or non-financial transactions are likely to flow seamlessly to financial transactions. Because of this, for all practical purposes, whatever impacts the operational systems and processes is likely to cause an exposure to financial transactions as well.

The reality of integrated operational and financial systems is that business operations risks should be managed in tandem with financial risks, both of which would be present in the information systems in use. For example, for a Web-based business such as Amazon, business continuity planning should be an integral part of the enterprise risk management, because any disruption in, or non-availability of, the customer

---

*THE SOA COMPLIANCE REQUIREMENTS ARE ALSO AN OPPORTUNITY TO IMPROVE THEIR SYSTEMS AND PROCESSES, INCREASE SYSTEMS RELIABILITY AND DATA SECURITY, AND ENHANCE TECHNOLOGY'S PRODUCTIVITY.*

Web site will likely result in a loss of revenue, which is clearly a financial exposure. Under the SOA, an entity covered by the act should report material events, financial and non-financial, on a real-time basis, currently interpreted as within 48 hours.

### SEEKING COMPLIANCE SOLUTIONS

Although deadlines for certain requirements of the act have been extended under certain conditions, the timeline for compliance with the SOA is rather short. Consequently, there is a flurry of activity currently underway. According to AMRResearch, nearly 52 percent of the companies surveyed are already implementing their compliance plans, another 33 percent are evaluating issues on hand, and the remainder have not begun. The amount of work necessary to reach compliance depends on the degree of sophistication of existing systems in terms of business process documentation, risk assessment, and relevant control measures in place. Generally, even for those that are well organized in the matter of financial systems, there is a great deal of work that needs to be done, especially in the first year. In the rush to reach compliance, it is likely that patchworks might be put in place where, given sufficient time and study, a holistic solution can be implemented. In this regard, the situation is much like the Y2K problem: some got by with a temporary fix and others streamlined their systems and processes.

With regard to SOA compliance, there is a great deal of discussion of issues, mostly in the context of marketing of products and services by public accounting firms, law firms, software vendors, and consultants. However, not much is available to organize the process of developing a compliance solution. The following guidelines can help in getting started.

#### **1. Work closely with executives who understand financial accounting and reporting; for example, the chief financial officer and the internal auditor.**

Typically, a content expert should be involved from the very beginning. After all, the owner(s) of the accounting information systems (AIS) are accountable for the processes, controls, and outputs of the system. They are primarily responsible for SOA compliance and have an in-depth understanding of the system from a content perspective. A most helpful candidate for this role is the internal auditor. In all likelihood, the internal auditor would be responsible to work with the audit committee of the board of directors in putting together a compliance solution.

*THE SITUATION IS MUCH LIKE THE Y2K PROBLEM: SOME GOT BY WITH A TEMPORARY FIX AND OTHERS STREAMLINED THEIR SYSTEMS AND PROCESSES.*

## 2. Assess the nature, role, and context of your AIS.

This exercise allows us to determine the present state of AIS. The issue here is not content (transactions and account balances), but rather processes. What are the subsystems within AIS, who is accountable for each, what technology platform are we using, what are the major risks in each subsystem, and what specific controls exist in each? Also, it is important to identify if the AIS is relatively decoupled from or integrated with the rest of the systems. If integrated, what is the interface between AIS and the linked system(s)? Finally, it would help to determine if the AIS is homegrown, vendor-supported, or a hybrid. Because external auditors have audited financial accounting systems and financial statements over the years, it would help to solicit their counsel. Although external auditors are subject to certain constraints in terms of their participation in this step, they have, over time, developed insights into the AIS that can save time and effort, and help avoid any missteps.

## 3. Identify and evaluate relationships between accounting and operations.

To develop a meaningful understanding of the AIS and its relationships with other systems, it is important to take a close look at the interfaces between the AIS and other systems. If the AIS is practically stand-alone, it affects other systems the least. At the other extreme, if the AIS is a part of an ERP (enterprise resource planning) system, it affects and is impacted by other systems.

A related dimension to explore here is the nature of business and its life-cycle stage. The nature of business and the way it is organized will determine the degree of closeness of the AIS with other systems. For example, in a private, for-profit college, academic computing systems can be separated from financial systems. This will ease the burden of risk management. On the other hand, an online bookstore such as Amazon or an online brokerage firm such as Ameritrade would have its AIS closely linked to its operations, requiring much greater care in SOA compliance.

The life-cycle stage of the business (initiation, contagion, control, and maturity) also provides additional insight. A growing business may require considerable additional effort to develop the SOA solution, because the growth may have kept people busy with other immediate concerns, and away from risk management. A mature business is likely to have an in-depth understanding of its processes, including accounting and finance; its stability affords yet another advantage because you can focus on the long-term solution rather than take a shortcut.

---

*EXTERNAL  
AUDITORS HAVE,  
OVER TIME,  
DEVELOPED  
INSIGHTS INTO THE  
AIS THAT CAN SAVE  
TIME AND EFFORT,  
AND HELP AVOID  
ANY MISSTEPS.*

---

*UNDERSTANDING THE EXISTING SYSTEMS WITHIN THE CONTEXT OF THE SOA REQUIREMENTS IS THE FIRST STEP, A STEP THAT MAY NOT REQUIRE ONE TO MAKE IMMEDIATE DECISIONS ON FUTURE TECHNOLOGY OR SYSTEMS.*

#### **4. Determine and review the maturity stage of your systems and business, and future plans.**

An understanding of the life-cycle stage of the information system helps in assessing the direction to take in finding a compliance solution. You cannot fit an isolated accounting software package in an ERP system. Similarly, an offshore software developer may not be able to help you with an integrated accounting system without a complete understanding of the networked operations. While considering possible scenarios, it is important to project the state of the systems a year or two from now rather than their present state. A planned change to an existing system may be modified to accommodate the compliance and retain the cost savings or productivity gains targeted in the plan.

#### **5. Examine the role of software vendors.**

If the accounting software systems you use are from a particular vendor, it might prove helpful to ask that vendor about any upgrades or improvements made in the software currently in use, or its substitutes. Most software developers are cognizant of the SOA requirements and have anticipated the need to modify or calibrate their systems to better meet the new regulatory requirements. For example, Oracle's Internal Controls Manager Solution uses features and functionality of Oracle E-Business Suite to meet the requirements, including document management, continuous auditing, whistleblower protection, application configuration risk assessment, and embedded business process workflow. Last year, PeopleSoft launched Financial Management blueprint. Companies using the blueprint to automate key business processes and financial controls can create the foundation for a process-based approach that would ensure that financial reporting and disclosure requirements are defined clearly, performed consistently, and managed effectively.

#### **6. Continue to do research on how others are solving the same problems.**

There is some benefit in staying behind the "bleeding edge." More options and alternative solutions are announced almost every day. While these are emerging, some of the "homework" can be accomplished that does not yet require the selection of information technology or software. Understanding the existing systems within the context of the SOA requirements is the first step, a step that may not require one to make immediate decisions on future technology or systems.

#### **7. Find a value-added solution.**

A typical stigma attached to risk management is that it is all about cost and no real benefit. Sure enough, preventive measures help avoid disasters and thwart security compromises,

and thus save potential losses; but these are opportunity costs that are never booked. No one seems to disagree with the statement that the costs of SOA compliance will be significant and the external audit costs will also rise substantially in the coming years. However, a solid case should be made for all system modifications, although regulatory requirements may dominate the justification for spending. Whereas the legal needs take away the stress of justifying the outlays, it is important to see that the opportunity to make changes is seized in making the most in terms of process streamlining, restructuring, improving efficiency, and enhancing productivity. Perhaps the incremental costs of additional benefits (beyond just compliance) might be marginal compared to the minimum costs of a compliance solution. Finally, a holistic solution to the compliance needs might even lower the external audit costs by the second year of its implementation.

### **8. Make a case for a technology committee at the board level.**

Information technology and information systems are central to today's businesses. Their role is as critical — perhaps even more critical — as that of the other factors involved in the success of an enterprise. Consequently, it is appropriate to think of IT governance while working on the corporate governance. The issue of IT governance overlaps, and may even dominate in some cases, the whole idea behind governance, the risk management. Powerful arguments can be made to the CEO and board members to seriously consider the first step in IT governance: appoint a technology committee of the board.

### **CONCLUSION**

The most important task in achieving compliance is to set expectations: expectations among the CEO, CIO, audit committee, the management, external auditors, and the internal auditor. When properly set, expectations can lead to better solutions to the compliance issue. Also, there must be a balance between being compliant and creating a risk management resource within the company. Although the immediate concern is to be compliant within the timelines given, all work should be mapped into the longer-term objective of creating a risk management culture for the company. Over time, it is essential to rise above the rituals and consider compliance, with regulation only as an incidental benefit. This means that we should use a framework that eventually brings all related aspects of risk management into a unified whole. It does not matter if these aspects belong to operations, systems, accounting, or management.

Going forward, the experience will be somewhat choppy, uncertain, and chaotic. If things are ever clear to a point where rules can govern, we might as well computerize the

---

*THE ISSUE OF IT  
GOVERNANCE  
OVERLAPS, AND  
MAY EVEN  
DOMINATE IN SOME  
CASES, THE WHOLE  
IDEA BEHIND  
GOVERNANCE, THE  
RISK MANAGEMENT.*

compliance. This is never going to happen, for judgment will remain an important element of the process. In this sense, enterprise risk management will always remain a journey, not a destination, and continuous improvement would be a goal. ■

Vasant Raval is a professor of accounting at the College of Business Administration, Creighton University in Omaha, Nebraska. He can be contacted at (402) 280-5518 or varaval@creighton.edu.

United States Postal Service  
**Statement of Ownership, Management, and Circulation**

1. Publication Title  
 EDPACS The EDP Audit, Control, and Security News

2. Publication Number  
 0 7 3 6 - 6 9 8 : 1

3. Filing Date  
 October 1, 2003

4. Issue Frequency  
 Monthly

5. Number of Issues Published Annually  
 12

6. Annual Subscription Price  
 \$245.00

7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4)  
 CRC Press, LLC 2000 NW Corporate Blvd., Boca Raton, FL 33431 - 7835

Contact Person  
 Nubia Moreno  
 Telephone  
 561-361-6072

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer)  
 CRC Press, LLC 2000 NW Corporate Blvd., Boca Raton, FL 33431

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)  
 Publisher (Name and complete mailing address)  
 Auerbach Publications 29 West 35th Street, 7th Floor, New York, NY 10001  
 Editor (Name and complete mailing address)  
 Beldon Meikus Auerbach Publications 29 West 35th Street, New York, NY 10001  
 Managing Editor (Name and complete mailing address)  
 Christian Kirkpatrick Auerbach Publications 29 West 35th Street, New York, NY 10001

10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)  
 Full Name Complete Mailing Address  
 Taylor and Francis Group 11 New Fetter Lane  
 London, England EC4P4EE

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities. If none, check box  None  
 Full Name Complete Mailing Address

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)  
 The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes  
 Has Not Changed During Preceding 12 Months  
 Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form 3526, October 2003 (See instructions on Reprint)

13. Publication Title  
 EDPACS

14. Issue Date for Circulation Data Below  
 October 2003

Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)	783	700
(1) Paid/Requested Outside-Country Mail Subscriptions Stated on Form 3541 (Include advertiser's proof and exchange copies)	501	389
(2) Paid In-Country Subscriptions Stated on Form 3541 (Include advertiser's proof and exchange copies)	0	0
(3) Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	0	0
(4) Other Classes Mailed Through the USPS	0	0
b. Total Paid and Requested Circulation (Sum of 15b(1), (2), (3), and (4))	501	389
c. Free Distribution (15c)		
(1) Outside-Country as Stated on Form 3541	43	42
(2) In-Country as Stated on Form 3541	0	0
(3) Other Classes Mailed Through the USPS	0	0
d. Free Distribution Outside the Mail (Carriers or other means)	0	0
e. Total Free Distribution (Sum of 15c and 15d)	43	42
f. Total Distribution (Sum of 15b and 15e)	544	411
g. Copies not Distributed	239	289
h. Total (Sum of 15f and g)	783	700
i. Percent Paid and Requested Circulation (15b, divided by 15g, times 100)	92%	90%

16. Publication of Statement of Ownership  
 Publication required. Will be printed in the October 2003 issue of this publication.  Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner  
 Signature: [Signature] Title: VP Production Date: 9/29/03

Instructions to Publishers  
 1. Complete and file one copy of this form with your postmaster annually on or before October 1. Keep a copy of the completed form for your records.  
 2. In cases where the stockholder or security holder is a trustee, include in items 10 and 11 the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check the box. Use blank sheets if more space is required.  
 3. Be sure to furnish all circulation information called for in items 15. Free circulation must be shown in items 15d, e, and f.  
 4. Item 15b. Copies not distributed must include (1) newspaper copies originally stated on Form 3541, and returned to the publisher; (2) estimated returns from news agents; and (3) copies for office use, leftovers, spoiled, and all other copies not distributed.  
 5. If the publication had periodic authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or, if the publication is not published during October, the first issue printed after October.  
 6. In item 16, indicate the date of the issue in which this Statement of Ownership will be published.  
 7. Item 17 must be signed.  
 Failure to file or publish a statement of ownership may lead to suspension of Periodicals authorization.

PS Form 3526, October 1999 (Revised)

Start (or extend) my subscription to EDPACS. Your subscription includes access to EDPACS OnLine, a searchable archive.

- 1 year (12 issues), \$245
- 2 years (24 issues), \$327 Best Deal — Save \$93
- Bill my purchase order # \_\_\_\_\_ attached
- Check for \$ \_\_\_\_\_ enclosed, payable to CRC Press LLC
- Charge my:  Visa  Mastercard  Amex
- Card No. \_\_\_\_\_ Exp. Date \_\_\_\_\_
- Signature (required) \_\_\_\_\_
- Phone your order to: 1-800-272-7737
- Fax: 1-800-374-3401
- Mail: CRC Press LLC, 2000 NW Corporate Blvd.  
Boca Raton, FL 33431
- E-mail: orders@crypress.com

Name \_\_\_\_\_  
 Title \_\_\_\_\_  
 Company \_\_\_\_\_  
 Street Address \_\_\_\_\_  
 City, State, ZIP \_\_\_\_\_  
 Country/Postal Code \_\_\_\_\_  
 Phone \_\_\_\_\_  
 E-mail address \_\_\_\_\_

Customers in CA, DC, FL, GA, IL, MA, MO, NJ, NM, NY, and TX, please add applicable sales tax. Canadian customers, please add GST.