by Jill Barson Gilbert

ARTICLE COURTESY OF LEXICON SYSTEMS, LLC. • www.lexicon-systems.com • +1 281 280 8106

# Sustainable Compliance

Regulatory compliance encompasses complex, often interrelated issues. During my 25-year career in environment, health, and safety (EH&S), organizations have typically assigned compliance management to technical experts, lawyers, and public relations people, encouraging these extremely capable specialists to operate in isolation, rather than taking a holistic view of how regulation affects corporate strategy.

The Sarbanes-Oxley Act of 2002 (Public Law No. 107-204, 116 Stat. 745) has elevated the role of regulatory compliance, effectively placing corporate governance under a microscope. This law may actually be the catalyst for organizations to bring EH&S into the fold of overall compliance as an integral part of the business. In this column, we consider what compliance is, what is needed to sustain it, and how information technology (IT) can help.

## COMPLIANCE IS A PROCESS

Regulatory compliance is about managing business risk, and should not occur in a vacuum. Compliance is a business process that requires constant oversight, management, and continuous improvement. Organizations identify requirements, set goals and priorities, determine what management systems and information are needed to demonstrate compliance, and then assess whether employees actually apply the established controls.

No matter their mission, organizations face a growing mountain of regulatory obligations. When they assign the compliance domain to technical experts, lawyers, and public relations people, they unwittingly create "silos"—that is, isolated pockets of data storage and management processes—rather than an integrated compliance program. Managing compliance in silos is the antithesis of standardization and integration that helps to improve the business and reduce risk. Silos lead to inconsistent approaches that fail to consider the organization's strategy, the duplication of efforts, and isolated, fragmented, or outdated information.

## SUSTAINABLE COMPLIANCE

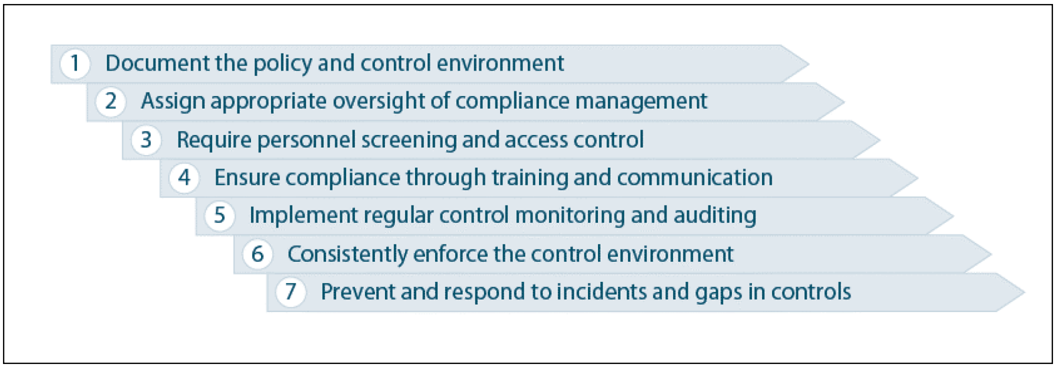
Organizations that embrace ISO or other environmental management systems are on the road to sustainable compliance. Yet, these approaches still tend to isolate EH&S issues and fail to consider the overall business. Michael Rasmussen of IT research firm Forrester Research has another approach. He suggests that effective compliance programs—whether they be EH&S, human resources, or corporate accounting—must cross business units or groups, since they impact the entire enterprise. Rasmussen contends that organizations must integrate seven habits to sustain compliance programs (see Figure 1). These seven habits support and augment the "Plan–Do–Check–Act" continuous improvement cycle. The key differences are the emphasis on controls—the business processes and deliverables that must be in place for compliance—and on auditing and enforcement.

## TECHNOLOGY'S ROLE

Technology alone cannot solve compliance problems. Discussions with corporate EH&S staff reveal that organizations must develop and continuously improve management systems, whether or not they use technology (see "Industry Insights on Commercial, Integrated EH&S Software Systems," *EM*, October 2004, p. 12). Research by management consulting firm McKinsey & Co. concludes that companies should beef up their management practices before focusing on technology. A study by McKinsey & Co. of 100 manufacturing companies in France, Germany, the United Kingdom, and the United States showed that IT expenditures had little impact on productivity unless accompanied by first-rate management practices (see "The Role of Regulation in Strategy," *McKinsey Quarterly*, 2004 Number 4; www.mckinseyquarterly.com). And IT analyst Mark Smith of Ventana Research further supports this position. Smith says that despite the increased buzz around business process management, organizations need to focus on assessing and improving their existing operational processes before automating and controlling them with new systems. Most organizations and IT suppliers have failed to take this easier path to process improvement, Smith adds.

Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. She helps organizations increase business value by designing and implementing EH&S management solutions that leverage technology. E-mail: JBGilbert@Lexicon-Systems.com.

Copyright 2006 Air & Waste Management Association



1. Document the policy and control environment
2. Assign appropriate oversight of compliance management
3. Require personnel screening and access control
4. Ensure compliance through training and communication
5. Implement regular control monitoring and auditing
6. Consistently enforce the control environment
7. Prevent and respond to incidents and gaps in controls

**Figure 1.** Seven habits of an effective compliance program.
*Source*: Rasmussen, M. *Seven Habits of Highly Effective Compliance Programs*; Forrester Research Inc., July 12, 2005.

A well-designed IT solution can help organizations document applicable requirements for regulatory compliance; identify potential gaps in compliance and address them in a timely manner; manage changing requirements; and consistently evaluate risk and performance. To be effective, a software-based compliance system must incorporate people, processes, and technology that fit with the organization's central strategy (see Figure 2).

When evaluating IT solutions for EH&S management, many organizations focus on EH&S features and functionality, taking only a cursory look at the IT infrastructure. Infrastructure and the business processes to sustain it are central to sustaining the compliance system. Active Reasoning, an IT compliance software firm, identifies five functional areas for the IT infrastructure (see "Sustainable IT Compliance for Financial Systems," February 2005; www.activereasoning.com):

1. **Change Management:** Manage the process for requesting, approving, evaluating, and implementing changes to the IT systems.
2. **Security:** Access control, perimeter security, password management, account management, user privileges.
3. **Data Storage and Recovery:** Data storage, backup, management, and recovery.
4. **IT Management and Governance:** Definition, administration, and enforcement of IT policies, and operational procedures.
5. **Segregation of Duties:** Defining roles and responsibilities for the IT organization.

Most organizations do a reasonable job of addressing data security, storage, and recovery, but can do a better job of documenting and enforcing change management and IT management, and defining IT roles and responsibilities. Compliance software itself typically has internal and external controls to ensure that casual users cannot access data through the "back door" or change the software configuration. And most commercial compliance software systems include audit trail capabilities to detect who logs on to the system, when they log on, and which data fields they change. Commercial software is also available to automate data backup and recovery. Tackling the change management process—not only documenting it and training stakeholders, but also enforcing it—is probably the most challenging of the five areas, with IT management, governance, and segregation of IT duties the next most challenging.

## CONTINUOUS COMPLIANCE

Compliance is an ongoing process, not a one-time event or a snapshot in time. The recent spotlight on corporate governance in the shadow of the Sarbanes-Oxley Act has caused both private and public companies to address the weaknesses in their business processes and management systems. Compliance management will evolve with changing regulations, and the IT systems that support compliance will continue to improve with advances in technology. Our challenge as EH&S professionals is to view compliance holistically, ensure that we implement the appropriate business and IT controls, and regularly evaluate the effectiveness of these controls. **em**

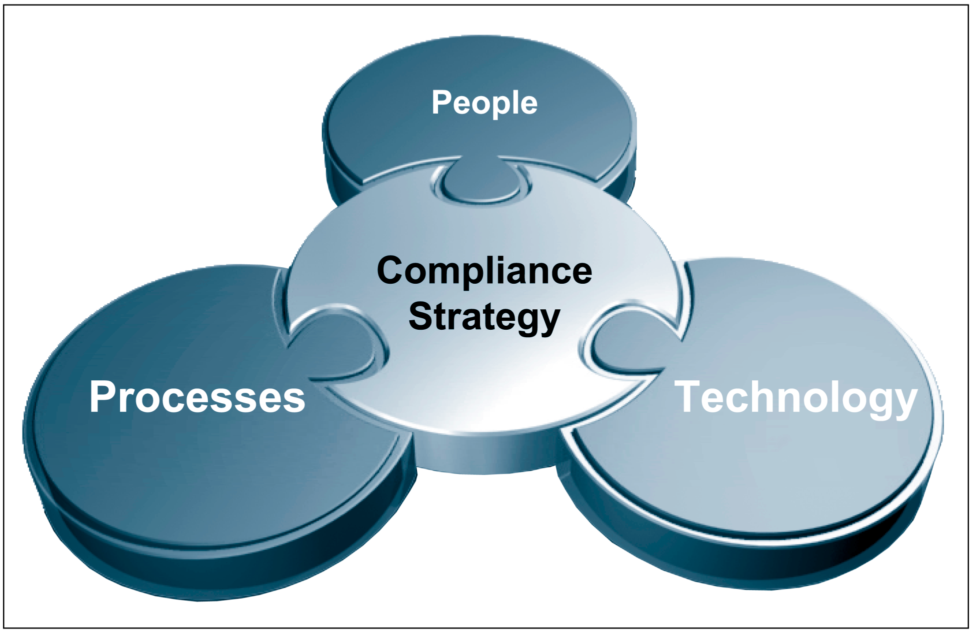


**Figure 2.** Technology is an integral part of compliance strategy.

Copyright 2006 Air & Waste Management Association