

Enforced Integrity

The underlying precept of the Sarbanes-Oxley Act of 2002.

David B. Sidon, CPA
The Navis Group

What's the lead story on tonight's news? Probably another integrity lapse, I bet. Who's the celebrity business man or woman headed off to the clink this week? Has our President (past or present) been square with us about relationships; foreign, domestic or personal? How about certain members of another of the integrity industries, the priesthood? And then there's the steroids issue – but, "we're not here to discuss the past", as a formerly respected slugger has suggested.

So it has come to this – enforced integrity. You wouldn't think that you'd have to put this in writing as Senator Sarbanes and Representative Oxley have. But then again, early on it was important to get the "thou shalt not kill" concept cast in stone, albeit another fairly obvious rule.

Some have asked if this is really necessary, or if this more akin to all of us being kept after school because one idiot in the back of class mouthed off. It doesn't matter. Apparently in the eyes of the folks in charge, it is indeed necessary, therefore we all have some work to do to assess our own integrity and honesty.

I work as a project management consultant in the banking industry and am currently involved with Sarbanes Oxley (a/k/a SarbOx; a/k/a SOX) compliance efforts on the part of my client banks. SarbOx may be a new set of compliance rules, but banks, at least those with assets exceeding \$500 million, have been subject to similarly strict standards as prescribed by the Federal Deposit Insurance Corporation Improvement Act of 1991 ("FDICIA"). In complying, the industry has adopted guidelines established in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"). The project parameters for full compliant documentation and testing are daunting, and the costs significant. But this is not about appeasing regulatory expectations; this is about looking inward and considering how we do business with each other. This is a process that should be embraced as an extensive analysis of best practices, with the scribing of those practices representing an exercise in business analysis and clarity. This is a golden opportunity that should not be missed by assigning a committee or the Compliance Department the task of achieving a passable level of compliance.

A sampling of the questions listed in COSO's "Overall Internal Control System Evaluation" reveals the integrity search and assertion process. Certainly no management team wants to answer any of the following questions other than with enthusiastic, confident affirmation. Here's the sampling:

"Does management adequately convey the message that integrity cannot be compromised?"

"Is the competence of the entity's people commensurate with their responsibilities?"

"Are the internal and external risks that influence the success or failure of the achievement of the objectives identified and assessed?"

“Are control activities in place to ensure adherence to established policy and the carrying out of actions to address the related risks?”

“Does communication of relevant information take place?”

“Is it [communication] clear with respect to expectations and responsibilities of individuals and groups, and reporting of results?”

“Are deficiencies reported to the right people?”

And so on; seemingly basic and simplistic questions. Welcome to SOX compliance, where “no”, “perhaps”, “sometimes” and “maybe” are not appropriate answers. But still, how do you prove that there are no hands in the proverbial cookie jar?

The daunting documentation process stems from policies and procedures regarding the safekeeping of the cookie jar and its contents, setting firm controls and recognizing the many risks involved. Who has access to the cookie jar? What are the procedures governing the removal (and eventual reinstallation) of the lid? Are there dual controls in place? Who counts the cookies? Who audits the count? Who authorizes the taking and re-stocking of cookies? What quality standards are applied to the cookies? How do we dispose of old cookies? Do the cookie jar rules apply to everyone? At night, is the cookie jar locked up? Remember, cleaners and security guards love cookies, too.

Therefore, what is necessary are clear, unambiguous policies, procedures, and rules of conduct that comprise an overall system of philosophical and financial integrity.

The FDICIA / SOX compliance flow that I’ve described to client banks follows:

The control of BANKING PROCESSES which satisfy BANK & CUSTOMER REQUIREMENTS is governed by CONTROL OBJECTIVES based on INTERNAL PROCEDURES considering RISKS & CONTROLS.

This flow begs the question of the documented and tested existence of well defined processes, requirements, objectives, procedures and risk controls as part of an overall integrity system. It’s no longer “good enough” to assume integrity. A formal system that documents and communicates management’s business philosophies must be created, affirmed at year-end by management, and verified by external, independent audit.

In the end, only two questions really count: Got integrity? Can you document it?

This article was published in Banker & Tradesman, July 25, 2005.

This article was published by Vitex, Inc., The Alliance Newsletter, October, 2006.



David Sidon, CPA (sidon@navis-group.com) is principal of The Navis Group, a risk management consulting firm based in Gloucester, Mass., specializing in enterprise risk and business continuity planning – www.navis-group.com.