

A Panacea of the Profession

**Is segregation of duties
a useful control, or
is it the snake oil of
internal auditing?**

BY BRUCE MCCUAIG

RECENTLY, THE COMMITTEE of Sponsoring Organizations of the Treadway Commission (COSO) announced a new project, "Implementing the COSO Control Framework in Smaller Businesses," to address the widespread, mistaken belief that it is difficult for small companies with less ability to achieve segregation of duties to have effective internal control. There is not a shred of definitive proof in the audit literature that segregation of duties is generally effective or worth its often significant cost. In fact, the preponderance of evidence in my experience indicates that segregation of duties is the most overrated and often least cost-effective control design option available.

Segregation of duty breakdowns are usually symptoms of bad control design, not root causes of control failure. The real problem is lack of risk assessment, lack of a control environment that places emphasis on ethical standards and competence, and lack of monitoring when conflicting duties exist. Reliance on segregation of duties has become a ritual based on a self-serving belief. That reliance has caused harm to clients and, worse, blinded the profession to better tools.

Needless, inappropriate segregation of duties, recommended by auditors and accountants, has snarled business in a staggering amount of red tape and useless bureaucracy. It seems intuitively obvious that two people sharing custody and ownership of an asset or responsibility for the authorization and recording of a transaction will improve control. However, the laws of human psychology, the social and cooperative nature of human beings, and the realities of the workplace will, in most cases, prevent segregation of duties from being an effective control.

There are situations where segregation of duties is appropriate, responsible,

and effective, but they are unique, specific, and strategic. In financial institutions, for example, a huge risk of fraud exists when trading and back-room activities are not segregated. The nature of trading activities makes other forms of monitoring an ineffective option. Because the risk is material, segregating conflicting duties in different departments makes sense. Other valid applications exist. However, every other use should be cost justified. It's time the audit profession began to look to the underlying causes of control breakdowns and governance failures and develop the tools to treat the disease and not the symptom.

As a category of controls, segregation of duties is intended specifically to prevent fraud and error and to safeguard assets. In an operating environment, a foreman may requisition the purchase of materials. They are purchased from an approved supplier by a purchasing agent. The result is often chaos — purchasing orders from the lowest bidder, the foreman does not get the material specified, or gets it late. What really happens? The foreman picks up the phone and orders the material directly from the supplier, and purchasing prepares the paperwork after the fact, often when the invoice arrives. In an accounting department, journal entries are supposed to be approved by a person other than the one entering the transaction. What really happens? Employees sign a month's worth of their colleague's transactions after the fact, or, even worse, sign bundles of blank journal entries for convenience, or even photocopy signatures onto the required forms so only one additional signature is required.

Time and time again, honest, well-meaning employees, in the pursuit of legitimate business objectives, find themselves hopelessly encumbered

by these controls while trying to do their jobs. Thus, they simply bypass or subvert and violate them.

Unsubstantiated belief in — and obsessive reliance on — ineffective practices is bad for clients. But even worse is the effect it has on the audit profession. The progress made by the medical profession in diagnosing and treating illness could not begin until old, primitive beliefs and practices were abandoned, and science and knowledge began to prevail. Bad practices get imbedded in professional literature, professional standards, laws, regulations, and tools. They block innovation and learning and impede progress. And that is what has happened with segregation-of-duties practices. Accepting lack of segregation of duties as an excuse for poor controls is simply wrong. Recommending segregation of duties inappropriately is irresponsible. Relying on segregation of duties where the control environment, monitoring, or risk assessment is weak is negligent. The answer lies not in an obsession with a control whose effectiveness is suspect, but in the balanced application of all the elements of control outlined in COSO's 1992 *Internal Control-Integrated Framework*, or better yet, the 2004 COSO *Enterprise Risk Management-Integrated Framework*.

By all means, let's rewrite the COSO framework, but let's make it far more useful for analyzing risk and control in specific processes and work groups, for teaching managers and work groups about control practices, for cost effective control design, and for forming a reliable opinion on control effectiveness. But don't rewrite it for small companies.

As audit practitioners, we must learn to give at least equal weight in our analysis of controls to the qualitative or, as some of my colleagues ironically call them, "soft" controls. Control environment, monitoring, risk assessment, and information and communication are much more important elements of control than segregation of duties or many other control activities. Doubters need only look at the kinds of control breakdowns described in the hundreds of significant deficiencies and material weaknesses reported to the U.S. Securities

and Exchange Commission (SEC) in 2004. Most of those material weaknesses related to breakdowns in the control environment or in monitoring. Breakdowns in the broad, pervasive COSO categories are the real root cause of financial reporting fraud. These control elements are not particularly costly to develop and implement, and small companies, if anything, are at an advantage in relying on them.

Techniques, technologies, and good management practices now are available to compensate for any loss of control, real or perceived, as we relinquish our attachment to segregation of duties. A new research study by The IIA's Research Foundation, "Changing Internal Audit Practices in the New Paradigm," describes how FedEx Kinko's, an office and print services company, is using data mining as a control to detect fraud. Thousands of Kinko's employees are authorized to make cash refunds of up to US \$100 on their own authority. Sophisticated data mining techniques developed by Kinko's detects abuses for follow up and quick resolution. The same research study describes how information technology giant IBM uses a similar technique for analyzing employee payables. Imagine how much wasted time is spent reviewing and approving employee expense accounts. By their nature, employee expense accounts should be easy to track and analyze for patterns indicating fraud or waste. Purchasing departments spend countless hours acquiring routine supplies or equipment. Business activities would proceed much more smoothly, productivity would increase, and customers and other stakeholders would benefit greatly from these new techniques.

Clear and unequivocal codes of conduct and ethical standards send a powerful and positive message. Companies should expect occasional error, fraud, or abuse and deal with it. The organization will be healthier as a result. "Trust but verify" can be a powerful and cost-effective strategy.

Many companies use powerful risk management databases to assess and manage risks and controls related to business processes and financial disclosures. These databases

are linked to data-mining or continuous-monitoring software and to internal audit management systems to achieve even greater synergies.

Other companies are using ongoing Web-based surveys based on COSO criteria to seek direct employee input on sensitive soft control issues such as integrity and business conduct. Companies must demonstrate, for example, that communication of relevant information takes place, that management adequately conveys the message that integrity cannot be compromised, or that the competence of the entity's staff is commensurate with their responsibilities.

Huge potential exists to expand these techniques. Many software companies are building survey capability into their risk management databases. Several Web survey products are on the market to allow cheap, efficient polling of employees to gather information on the level and nature of soft controls. Survey results require verification, but they are a valuable, efficient, and underutilized tool to gather and analyze information on many of the most important elements of internal control. Those being the elements with some predictive ability of a company's capability to achieve reliable financial reporting and U.S. Sarbanes-Oxley Act of 2002 compliance and those pervasive elements that credit rating agencies, among others, have signaled are the most important determinants of a company's credibility.

Professional auditors and advisors need to be far more clever in helping clients design high-impact, cost-effective internal controls; far more sophisticated in their diagnostic and monitoring tools; and far more balanced in their assessment and use of all of the COSO criteria. They need to provide far better advice on control design. There is no reason large and small companies can't share the same COSO framework. What need to change are the profession's beliefs and outmoded practices.

BRUCE MCCUAIG, CIA, CCSA, CA, is principal consultant, Collaborative Assurance & Risk Design, at Paisley Consulting in Cokato, Minn.

To comment on this article, e-mail the author at bmccuaig@theiia.org.