

# Cost-effective controls

How to achieve segregation of duties with limited resources **Interviewed by Leslie Stevens-Huffman**

**F**raud can be financially and emotionally devastating for any CEO, whether the company is publicly traded or privately held. While most chief executives would agree that segregation of duties (SOD) provides the best prevention and may even be the ultimate cure for a slew of fraud-related problems, they often don't think the problem can happen to them.

The most frequently asked questions about fraud are: Does *my* business really face risk? And does that risk justify the expense of segregating duties and instituting controls? The answer to both of those questions is "yes." All CEOs face the risk of fraud-related loss, yet it is possible to institute a cost-effective control system by applying a pragmatic approach to the segregation of duties review process.

"For many CEOs, it's hard to justify the time and resources needed to go through a formal SOD analysis because they don't believe their business is at risk when they are surrounded by tenured, loyal associates," says Lee Buby, SOX 404 practice leader for Haskell & White LLP. "But it takes incentive and opportunity to commit fraud, and, unfortunately, it's the more tenured employee that has the greatest opportunity."

*Smart Business* spoke with Buby about how CEOs can achieve tight controls through a cost-effective SOD analysis.

## Why is the risk of fraud greater with tenured employees?

Tenured employees know the aspects of the company's accounting system and how to cover their tracks, so they have the know-how to commit fraud. Also, long-term associates are often not only loyal employees but also friends with the CEO, so it's hard for any executive to imagine such a betrayal of trust. So those kinds of losses are not only the most likely, they are emotionally devastating for CEOs when they occur.

## What's the first step in a cost-effective SOD analysis?

Perform an appropriate SOD assessment that will actually identify and define every



**Lee Buby**  
SOX 404 practice leader  
Haskell & White LLP

existing issue. Then evaluate each issue against the organization's tolerance for risk. If the risk of loss is small, the CEO may choose to accept it, or he or she may be satisfied that an existing control is sufficient. Having the knowledge will allow the CEO to make cost/benefit decisions for each issue. The best assessments are customized, but to save money and resources, start with an industry template and adapt it by actually performing walk-throughs of each activity. Not every issue is equal, so you can create mitigating controls for higher-risk areas.

## What is the next step?

To truly assess the risk, review employees' access to information, not just their job description. A good analysis should include what each employee can access, physically or via technology. Assume that if an employee is able to access a function or asset, it *will* be accessed. This is especially important in organizations with tenured employees who have know-how of the different aspects of accounting. Once again, management can apply the cost/benefit test before instituting new controls, but at least the information is there to make an informed decision.

## Doesn't the IT audit evaluate SOD?

Management and audit teams have historically relied on IT auditors to evaluate the accessibility of an IT control environment, but this has been limited to determining whether those who have access also have a valid business purpose for it. This, by itself, does not take into consideration whether various combinations of access or assigned duties presents an SOD issue. Management and auditors must work closely with IT professionals to define and gain an understanding of access rights in order to perform the SOD analysis. This is an area where traditional SOD assessments and IT stewardship has fallen short.

## How can CEOs identify the best areas for SOD?

Identify critical areas and hold the related SOD design or mitigating controls to a higher standard. For highly liquid assets that are easily convertible to cash, such as access to a line of credit or the issuance of shares of company stock at a public entity, management should always attempt to design preventive controls before settling for after-the-fact detective ones. This is one of those areas where SOD just absolutely makes sense. And don't forget about terminated personnel when designing controls. This includes everything from protecting assets to preventing share price manipulation, bad press and disclosure of confidential information or trade secrets.

It's not always an easy task, and it can be time-consuming, but a pragmatic approach to SOD and control decisions, based on knowledge and risk tolerance, will help reduce risk using a cost-effective methodology. Also, once the initial analysis has been performed, the maintenance time is minimal, and it can be used every time a shift in accounting duties is required or new staff is hired. It may just be the best time and money a company will ever spend because not only will it add value to the organization, it will also give the CEO peace of mind. <<

**LEE BUBY** is the SOX 404 practice leader for Haskell & White LLP. Reach him at (858) 350-4215 or lbuby@hwcpa.com.

**Insights Accounting** is brought to you by Haskell & White LLP