Managing Fraud Risks Without Good Guidance

By Melissa Klein Aguilar

While the ‘F’ word has always been an ever-present threat in Corporate America, one particular type of fraud—financial-statement fraud—has taken center stage since the corporate scandals of the first half of the 21st century put Sarbanes-Oxley into motion.

Since the Securities and Exchange Commission’s rules for implementing Section 404 of SOX took effect, companies have had to assess the risk of fraud in their financial statements to meet their internal controls reporting requirements. Trouble is, no comprehensive guidance on how to conduct a fraud risk assessment is readily available in one place.

“The challenge is that in the U.S. there’s no single fraud risk standard to measure against,” says Pam Verick Stone, a director at risk management consulting firm Protiviti.

Toby Bishop, a partner at Deloitte Financial Advisory Services, agrees that “a lack of extensive or authoritative guidance” on the subject has left auditors and financial reporting executives vexed. Most of the methodology developed over the last few years, he says, arose “through practical experience.”

That has frustrated some internal auditors, such as Bill Stepaniuk, director of internal audit for the Public Company Accounting Oversight Board to revamp the rules that apply to auditors. The public comment period on both proposals ended in late February.

The SEC’s plan aims to fill a void of guidance for management; even though the Commission has published guidance on the topic, large companies that have complied with Section 404 since 2004 have long complained that they have no choice but to rely on the far more exacting Auditing Standard No. 2 that the PCAOB expects external auditors to follow. The new guidance is also intended to allay fears of smaller companies not yet

Continued on Page 54
# Compliance Week

## Table of Contents

### Rules & Regulations
- 404 Reform Ideas Get Mixed Reaction .......................... 1
- Foreign Issuers Glean SEC Insights On IFRS Filings .......... 6
- Plaudits, Mostly, For Foreign Issuer Exit Strategy .......... 10
- News Briefs .................................................................. 12

### Special Report: Foreign Corrupt Practices Act
- FCPA Enforcement Has Record 2006; Expect More .......... 16
- Overseas, Nations Slow To Follow The FCPA Path .......... 20
- Guest Column: Enforcing An Ethical Line Against Bribery .. 22

### FCPA Compliance
- An overview of the risk assessments and data analysis necessary to build a foundation for FCPA compliance. SPONSORED BY Deloitte Financial Advisory Services LLP. Page 18

### Enforcement & Litigation
- Court Rulings Set Stage For Backdating Lawsuits .......... 24
- GCs Wary Of ‘Scienter’ Idea In New Evidence Rule ....... 26
- Perils GCs Can Face In Backdating Actions ................. 28

### Accounting & Auditing
- PCAOB Gets An Earful On Proposed Audit Standard ....... 30
- Audit Inspection Reports: Does Anyone Care? ............. 34
- Can ESOARs Cure Option-Expensing Pains? ............... 36
- Accounting Industry Briefs ........................................ 37

### FIN 48 And Local Taxes
- How FIN 48, which requires companies to disclose uncertain tax strategies, is applied to state and local taxes. SPONSORED BY UHY Advisors SALT, LLC. Page 32

### Executive Compensation
- Top Option Grants, Stock Awards In February 2007 ....... 39
- How To Structure Pay-For-Performance Packages ....... 40

### GRC Illustrated Series
- How Automated Controls Can Help Manage Risks ....... 42

### Boards & Shareholders
- The Fine Art Of Settling Shareholder Resolutions .......... 47
- Companies Try Taking Action Via No-Action Letter ....... 48
- New Forum Lets Investor Groups Plot CSR Fights .......... 50
- Amid Fewer Lawsuits, D&O Premiums Tumbling .......... 51

### ERM & Internal Controls
- Managing Fraud Risks Without Good Guidance .......... 1
- New, Slimmer Guidance For IT Controls Unveiled ....... 52
- How To Check, And Block, Management Overrides ....... 53

### Compliance & Technology
- How A $47B Giant Put XBRL To Good Use (Cheaply) ....... 56

### Global Compliance
- EU Calls For Opinions On Auditor Liability Caps .......... 58
- J-SOX Hits Japan, And Few Know What Comes Next ....... 60

### Remediation Center
- Delegating Approvals; Listing Your Pay Disclosure ....... 64

### Columns, Q&A
- Editor’s View: Death To Audit Standard No. 5, Long Live The PCAOB! 4
- Davis & Lukomnik: ‘B-List’ Activism Portends New Challenges For Cos. 66
- Dan Swanson: Business Continuity Plans: Auditing Your Resiliency 68
- Louis Thompson: Angry Investors At The Gate; Do You Let Them In? 70
- Richard M. Steinberg: Where Responsibility For ERM Needs To Reside 92
- Donna Boehme, Formerly BP: Building A Compliance Function 1

### Crossword Puzzle
- Our First Ever Crossword Puzzle (In Honor Of April Fool’s Day) 82

### Conferences & Events
- Compliance Week Webcast Series ............................ 83
- 2007 Compliance- And Governance-Related Events ....... 84

### Personnel Moves
- Who’s Coming & Going In Corporate Governance ....... 86

### Help Wanted
- Compliance-Related Job Listings ............................. 88

### Data & Disclosures
- Investigations, Restatements & Class-Action Lawsuits .... 90

### Advertiser Index
- List Of Advertisers & Editorial Calendar ...................... 94

---

Compliance Week (ISSN: 1549-957X) is distributed monthly by Financial Media Holdings Group, Inc., 77 No. Washington Street, Boston, Massachusetts 02114. Copyright ©2007, Financial Media Holdings Group, Inc. All rights reserved. Neither this publication nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of Financial Media Holdings Group, Inc. Requests for reprints and permissions should be directed to Compliance Week at the address noted above, or by calling (888) 519-9200. Subscriptions to Compliance Week include a weekly email newsletter, full access to resources at ComplianceWeek.com, and this monthly print magazine. To subscribe, go to http://subscribe.complianceweek.com. To change your address or order back issues, email Compliance Week at info@compliance-week.com or call (888) 519-9200.

Important Notice: Compliance Week does not provide legal advice. Content is for general information and discussion only, and is not a full analysis of the matters presented. The information provided by Compliance Week may not be applicable in all situations, and readers should always seek specific advice from lawyers, auditors and/or appropriate governance and compliance experts before taking any action with respect to any matters discussed herein. In addition, columns and opinion articles solely reflect the views of their respective authors, and should also not be regarded as legal advice.
Risk Assessment & Data Analytics
Building the Foundation for FCPA Compliance Programs

By Nina Gross and Dan Krittman
With contribution from Michele Cross and Samir Hans

As if growing customer demands for innovation, strained resources, globalization and regulatory requirements aren’t enough, companies now face increased government enforcement of the U.S. Foreign Corrupt Practices Act (FCPA). As a result, and in the wake of recent high-profile corporate corruption scandals, many multinational companies are reassessing their framework for evaluating FCPA risk.

 Newly developed FCPA risk assessments include a focus on exposure from overseas operations, joint ventures and acquisitions in countries considered high risk for potential corruption, and business partners, including consultants, agents, and distributors. Such tailored assessments have revealed vulnerabilities involving interactions with foreign governmental entities and employees. Increasingly, technology and the use of data analytics are part of these assessments, assisting companies with their evaluation and monitoring of FCPA risk—a growing challenge given the complexity of decentralized corporate structures and the pace of global mergers and acquisitions.

Implementing a formal FCPA risk assessment process that integrates technology and data analytics can aid legal counsel, compliance officers, internal audit, executive management, and, ultimately, board and audit committee leaders in the early detection of FCPA red flags. It can also support the fine-tuning of their FCPA compliance programs and the prioritizing of their FCPA compliance monitoring efforts.

FCPA Risk Factors and Considerations

A robust FCPA risk assessment process can lay the foundation for an overall FCPA compliance program. In designing and implementing an FCPA risk assessment process, management should seek to develop a framework that is flexible, adaptable and gives consideration to a variety of complex risk factors, including:


» International sales. Management should track the level of international sales to government entities, including to state-owned enterprises and through joint ventures, and consider future government sales resulting from acquisitions.

» International sales channels and channel partners. Channel partners, consultants, agents, distributors, joint venture partners and other third parties may be critical to a company’s market penetration and distribution strategies. But they can also expose the company to additional FCPA risks, particularly given the lack of transparency into third-party business activities. In refining their FCPA risk framework, companies should move aggressively to identify and document the wide range of third parties and channel partners that liaise with foreign government officials (e.g. customers, regulatory entities, and tax and customs authorities) and the portion of sales or other business activities that are handled by those third parties and channel partners.

» Industry-specific considerations. Companies should assess potential FCPA risks with respect to industry-specific processes, such as government procurement, product regulatory approval and licensing processes (e.g. pharmaceuticals, medical device manufacturing, technology and telecommunications), and practices such as the provision of “trial equipment” (e.g. technology and telecommunications). In assessing risk, management should seek to understand the various parties involved with securing foreign government business and approvals.

Companies should consider beginning the assessment process by carefully evaluating their exposure from operations in countries perceived as having significant levels of potential corruption. Information garnered through internal audit activities, employee feedback (informal or through whistleblower hotlines), competitors’ disclosures, and reported government investigations into corruption activities can aid in assessing the overall business climate within the countries of operation, as well as FCPA risk exposure.

The ability to proactively identify and respond to FCPA exposure rests largely on a robust risk assessment, enabled by data analytics and sustained through focused monitoring.

Deloitte.
Implementing a Formal FCPA Risk Assessment Process

When implementing a formal risk assessment process, management should consider several critical success factors, including:

» Who will perform the assessment? Designating specific owners of the risk assessment can help promote consistent performance of the assessment on a regular basis. Such owners should have experience in assessing FCPA risks and a strong understanding of the FCPA’s requirements. This approach may warrant a cross-functional and global team comprising members from internal audit, sales, accounting, compliance, and legal.

» To whom will the assessment be reported and how?

» How can technology and data analytics be used in support of the risk assessment process and ongoing monitoring, investigation, and due diligence efforts?

» How will assessment results be integrated into the company’s overall ongoing compliance-monitoring efforts?

» How will the assessment results be used to fine-tune FCPA compliance programs, including potentially identifying the need for additional training and monitoring?

Performing a broad FCPA risk assessment and leveraging technology and data analytics can help build a foundation for an effective FCPA compliance program and aid management in their efforts to identify and respond proactively to FCPA exposure.

Leveraging Technology and Data Analytics

Relatively recent technological advances have resulted in companies increasingly migrating more of their detailed transactional data to electronic systems. One of the results of this migration has been a fundamental shift in the approach to FCPA investigations and associated data analytics. Companies and their legal counsel not only need to consider implementing legal, compliance and investigative strategies now, but they also should consider creating a plan to deal with massive amounts of related electronic transactional data.

For example, identifying potential FCPA violations or red flags can be complicated, time-consuming and expensive. Typical technology challenges include differences in accounting systems; differences in foreign languages; the sheer volume of data involved; coordinating multiple globally based teams of employees, lawyers and consultants; issues related to security, confidentiality and privacy; and shortages of essential technical resources in key locations.

Technological innovation is playing a key role in overcoming these challenges. With the standardization of accounting systems, forensic accountants and technology professionals are building tools designed to facilitate necessary data extraction and the analysis of large amounts of data. Tools with multilingual search engines and advanced linguistic features can enable forensic accountants to work with systems in different languages without losing functionality. Technology also now permits forensic accountants to analyze entire accounting tables, reducing or in some cases eliminating the need for sampling exercises that might result in missed anomalies. And location-neutral utilities, accessed via secure Internet sites, can provide quick, reliable access and functionality to globally dispersed teams responding to alleged FCPA red flags or violations.

Technology is no longer a tool used solely to track leads on a reactive basis. Rather, it is now implemented to identify anomalies proactively. Using these tools, companies in many industries can easily and inexpensively extract data from accounting systems on a regular schedule, such as at the end of a fiscal quarter, and run it through various anomaly tests with adjustable thresholds to flag potential FCPA problems.

Tools incorporating the aforementioned technological innovations—FCPA Analytics from Deloitte Financial Advisory Services LLP is one example—can help simplify the identification of suspicious accounting transactions. In addition, these tools can help users assess whether a company’s clients, vendors, agents, employees, and other associates are on a list of Politically Exposed Persons (PEPs). Transactions with PEPs may warrant further analysis. Such analytical tools point the way to a future where technology will likely be central to almost all FCPA compliance programs.

Nina Gross and Dan Krittman are directors, Samir Hans is a senior manager and Michele Cross is a manager in the Forensic & Dispute Services practice of Deloitte Financial Advisory Services LLP.


The views expressed in this article are those of the authors and do not necessarily represent those of Deloitte Financial Advisory Services LLP.