



Using technology to fight fraud

“Although antifraud roles vary in business today, top management generally owns the antifraud responsibility, the audit committee oversees antifraud efforts, and internal audit provides a critical line of defense against the threat of fraud by focussing on risk monitoring in addition to fraud prevention and detection.”

- Internal Audit 2012, PricewaterhouseCoopers

Building a better mousetrap

Fraud represents a significant business risk that must be mitigated, and demand has increased for greater scrutiny and visibility into the effectiveness of internal controls. Effective fraud detection and prevention bolsters the bottom line by minimizing potential revenue leakage through unseen fraudulent activities. But, as any audit professional will tell you, finding fraud is an ongoing challenge that requires both skilled practitioners and specialized technology.

In the newly released 2008 Report to the Nation on Occupational Fraud and Abuse, the **Association of Certified Fraud Examiners (ACFE)** estimates that a typical organization loses 7% of its annual revenues as a result of occupational fraud and abuse. To illustrate the potential enormity of typical fraud loss, the ACFE applied the 7% figure to the estimated 2008 United States Gross Domestic Product — translating to about \$994 billion in fraud losses.¹

The losses are huge, and, according to a 2006 ACFE study, once the loss has occurred, the chance of recovering the funds in full is only 16.4%.²

The **KPMG** Fraud Survey 2006 reported that of the factors contributing to fraud in the organization, poor internal controls rated as the highest at 33%, and override of internal controls rated second at 24%.³ Continuous review of the internal controls is required to ensure that the controls that have been established remain in place and remain effective. In addition to having adequate controls, the challenge is for auditors and fraud examiners to look beyond the controls and find loopholes in the system where fraud could occur.

The responsibility for fraud detection and prevention is shifting increasingly to Internal Audit departments, who have the skill set to provide real-time fraud risk assessment and monitoring, and can report on areas of key risk to management.

To get started on building a fraud detection program, here are some guidelines on five key components that must be included:

- **Build a profile of potential frauds.** This profile includes a list of the many different areas in which fraud may occur and the types of fraud that are possible in that area. This can be developed as part of a risk assessment.
- **Test data for possible indicators of fraud.** A complete testing program should include ad hoc or random testing in addition to more formalized or regular tests.
- **Improve controls by implementing continuous auditing and monitoring.** Strengthen controls over transaction authorizations and use continuous auditing and monitoring to test and validate the effectiveness of your controls.
- **Review information from data testing and continuous auditing and monitoring.** Investigate patterns and fraud indicators that emerge from the fraud detection tests and continuous auditing and monitoring.
- **Repeat the steps.** This process of building a profile, testing data, improving controls, and reviewing information needs to be repeated on a regular basis.

¹ 2008 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

² 2006 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

³ Fraud Survey 2006: Fraud Risk Management, KPMG Forensic

Transactional analysis is one of the most powerful and effective ways of detecting fraud within an organization. KPMG's 2006 Fraud Risk Management report found that "Unlike retrospective analyses, continuous transaction monitoring allows an organization to identify potentially fraudulent transactions on, for example, a daily, weekly or monthly basis. Organizations frequently use continuous monitoring efforts to focus on narrow bands of transactions or areas that pose particularly strong risks."⁴

To maximize its effectiveness as a fraud detection system, transactional analysis ideally will:

- Allow easy comparisons of data and transactions from multiple IT operational systems.
- Work with a comprehensive set of indicators of potential fraud — taking into account both the most common fraud schemes and those that relate specifically to the unique risks a particular organization may face.
- Analyze all transactions within a given area and test them against the parameters that highlight indicators of fraud.
- Perform the analyses and tests as close to the time of the transaction as possible, ideally even before the transaction has been finalized, and preferably on a continuous monitoring basis.

Finally, a fraud detection and prevention program should incorporate a spectrum of analysis — ranging from ad hoc through to repetitive through to continuous. Based on key risk indicators, ad hoc testing will pinpoint areas for further investigation. Should this initial testing reveal control weaknesses of suspected instances of fraud, repetitive testing or continuous analyses should be considered.

By building a fraud detection program, organizations can catch frauds earlier, prevent greater losses, and quite often serve as a deterrent to other possible frauds.