Executive fraud: Five questions the board should be asking

By Mike Roos, Barnstone, and Jonny Frank, StoneTurn Group

When serious misconduct occurs in a company, the media, investors and regulators inevitably ask, "Where was the board?" What questions should directors be asking to ensure an effective defence against fraud and corruption?

Fraud and corruption pose serious business, as well as legal, risks—particularly, it seems, in Africa. A 2011 Economist Intelligence Unit survey of corporate executives reports that Africa has the 'highest incidence of fraud among any region, with 85% of respondents falling victim of fraud in the last year'. The survey found that African companies lose, on average, 3.1% of revenue to fraud.[1] Transparency International's Corruption Perception Index shows that sub-Saharan Africa is one of the most corrupt regions in the world.[2]

A recent KPMG study finds that the 'typical corporate fraudster' is a senior finance executive, and that CEOs are the fastest-growing group of fraudsters—26% of those committing fraud are chief executives, up from 11% in 2007.[3] While these are global statistics, there is no reason to suspect that South African executives are not as susceptible to the same pressures or have the same opportunities as their peers overseas to commit fraud.

This trend should be a wake-up call for boards and their audit committees because they are so reliant on these very executives to help combat fraud. Boards depend on management for the reports and information they need to ascertain whether the company's systems and processes are sufficiently geared to prevent fraud—and to detect it timeously if it does occur.

Weakening controls environment

An added cause for alarm is the economic downturn, which is likely to have two main impacts on corporate fraud. The first is general: in a bid to reduce costs, companies may curtail spending on the control environment, which could be affected by staff lay-offs and general lack of investment. The KPMG report suggests that the control environment is weakening: the exploitation of weak internal controls jumped from 49% in 2007 to 74% in 2011. Losses from collusion, by contrast, declined from 15% to 11%.2.[2]

A second impact of the economic downturn is that the CFO and the CEO are likely to find themselves hard-pressed to turn in the 'right' numbers at a time when it is important to do so. Pressures like these, coupled with a weakened control environment, can provide just the right sort of conditions to provoke a little creative accounting.

Since the new Companies Act came into existence earlier this year, board members have found themselves facing dramatically increased responsibilities, including potential personal liability for the consequences of their decisions. In other words, if serious fraud and corruption takes place in a company, its board members are at risk of severe damage to their reputations and also of financial liability if it is found that they did not discharge their fiduciary duties adequately.

The challenge for board members—and the audit committees they appoint—is to make sure that they have taken the necessary measures to prevent and detect fraud. We will devote the rest of this article to suggesting five questions directors should be asking of the relevant company executives: the CEO, the CFO, the company secretary, the head of internal audit, the ethics compliance officer and the legal officer. We will also suggest a technological solution that uses advanced analytics.

1. What is the process for identifying the risks of significant fraud and corruption?

The essential point here is that a fraud prevention programme can only be developed if the potential risks are thoroughly understood. The board needs to make sure that there has been a comprehensive assessment of the fraud risk, including criminal risk. This assessment should look at the entire system, use scenarios and include active involvement by business unit and function leaders.

2. What are those risks?

At the conclusion of the assessment, the company must identify the various types of risk it faces. We advise distinguishing between liability and leakage risk. Liability risk includes financial reporting, unauthorised receipts and unauthorised expenditure, while leakage risks include revenue and expenditure leakage as well as asset misappropriation.

3. What are the programmes for mitigating and controlling risk?

The elements that make up the control environment are an organisational culture of integrity reinforced by the tone of executive and middle management. Mechanisms such as training, code of conduct certifications and channels for anonymous whistleblowing are also important elements.

High-impact risks require specific preventive and detective controls in addition to a strong control environment.

Boards and audit committees need to pay particular attention to monitoring how effective the processes actually are. This goes beyond operational effectiveness: directors must also ensure that the company evaluates the design of the control processes to establish that there are safeguards against circumvention through override, collusion or unauthorised access.

Front-line employees are the first line of defence—it's only a minority who actually

become fraudsters. Fraud awareness is not enough: they need to be equipped with the knowledge, skills and tools to prevent and detect fraud. This means training employees about the schemes prevalent in the areas in which they work, preventive measures and red flags to ensure early detection.

4. How are loss and fraud reported?

It is very important to keep a register of all the fraud and loss that have been detected. The reporting should include an analysis of the root causes, and must distinguish between operational loss and loss from fraud. It must be apparent that the company learns from what has gone before, so the same kinds of fraud are not repeated—loss reporting must never just be a statistical exercise.

The same point should be made of the anonymous whistleblowing tip-off line that should be in place.

As part of this whole process, we believe it is very important to identify losses that were prevented as a result of the processes in place. For example, recording that a R10 000 fraud was prevented is good, but it might be more valuable to note that a certain actions prevented a R10 million fraud. This kind of near miss helps the board and company executives see the value of the work they are doing, and concentrates the mind most effectively!

All in all, we advocate that loss reporting is much more granular in order to make analysis both easier and more valuable.

5. How is technology being used?

Asking the first four questions is critical, particularly when it comes to identifying weaknesses and strengthening them. But it's not enough. Relying on compliance and the internal audit is not adequate for mitigating the risks companies face or for demonstrating that board members have adequately discharged their duties—especially given the increased propensity of senior executives to themselves commit fraud.

Technology could just save the day. Business now runs almost entirely on its IT systems, and advances in analytics have now made it possible for those systems to be monitored—and monitored intelligently—virtually in realtime. This means that organisations can detect fraud as it occurs and not just after the fact.

All in all, we advocate that loss reporting is much more granular in order to make analysis both easier and more valuable.

This is why the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[4] strongly endorses the continuous monitoring of transactions, with the aim of ensuring operational effectiveness and efficiency, reliability of financial reporting, and regulatory compliance.

Think of analytics as the 21st Century's version of a smoke detector for fraud. Continuous monitoring keeps the stable door on a hairspring, ready to alert management every time it moves—and not only when the horse has bolted. Traditional monitoring via internal audit and so on is retrospective, and so recovery of the identified losses becomes both difficult and expensive.

Continous monitoring is a huge breakthrough because it uses sophisticated analytics to monitor financial transactions across all systems in realtime—exception reports could be produced every three minutes, for example. Because it's automated, there's much less dependence on (or vulnerability to) humans. In addition, these new analytics systems are intelligent enough to spot trends and then report on deviations from them. Humans don't need to think of everything!

In our experience, this kind of software takes something like three months to implement, and also detects operational inefficiencies and compliance issues. But, best of all, the investment is usually recouped within two or three months.

Board members have an important role to fulfil in combating fraud. By asking these questions, and insisting on the right answers, they can help to keep their companies financially healthy—while protecting their own reputations and assets.

[1] *The Economist Intelligence Unit, 2011/2012 Global Fraud Report.*

[2] *Transparency International, Corruption Perception Index 2010—www.transparency.org.*

[3] *KPMG, "Who is a Typical Fraudster," 2011—www.kpmg.com.*

[4] *Originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, COSO is a voluntary private sector organisation dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO comprises the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).*

Mike Roos CA (SA) is a Director at Barnstone Corporate Services and leads the Fraud & Risk Services group. His experience includes complex investigations, litigation support and conducting fraud risk assessments. He can be reached at mroos@barnstone.co.za.

Jonny Frank is a partner in the New York office of The StoneTurn Group. He retired from PwC, where he led and founded Fraud Risks & Controls and is a former Federal prosecutor in the U.S. Department of Justice. He can be reached at jfrank@stoneturn.com.