FRAUD WATCH
FRAUD WATCH HELPS YOU TO FIGHT FRAUD
www.fraudwatchonline.com

Special features for Fraud Watch subscribers only **Posted May 10, 2010**

Fraud Risk Assessment: Hampered by Focussing on Controls?

There is a growing need to change from a bottom-up controls-based approach to a top-down risk-based strategy, say fraud risk management practitioners Martin Samociuk and Nigel Iyer.

Historically, many organisations have relied on detailed reviews of controls by internal and external auditors to reassure stakeholders that an effective fraud risk management strategy is in place. Today, there is a growing realisation of the need to change the focus from a bottom-up controls -based approach to a top-down risk-based approach. Rather than focusing on reviewing controls, organisations should first understand the potential fraudsters to which they are exposed and only then check if the controls would prevent frauds occurring. This article provides a fresh and 'uncluttered' approach to conducting a realistic fraud risk assessment and is based on the authors' recently published book, A Short Guide to Fraud Risk (second edition).

In 2003, when our first guide to fraud risk was published, the world was coming to terms with the aftermath of the huge financial scandals in the late 1990s and early 2000s. The shadow of the US Sarbanes Oxley Act 2002 was looming and corporate governance and risk management appeared to be gaining ground in corporate boardrooms. At last it seemed as if we were on the verge of finally cracking down on big-time fraudsters. Seven years on, we have witnessed a global financial crisis which has exposed unethical and fraudulent behaviour on a scale rarely seen before. Rather than preventing fraud, it seems as though the huge focus on risk management and corporate governance has actually provided a smokescreen behind which fraudsters have thrived.

So why is this so? Simply put, we believe that many organisations still do not understand their fraud risks. They have become overburdened with operational risk and audit requirements which focus on systems and processes and evaluating the effectiveness of controls, having lost sight of the fact that people commit fraud. This often results in an incorrect picture of fraud risk being presented at the Board level. In turn, organisations have been fighting an enemy about which they know very little, and even less about how to deal with. The fact that corporations and financial institutions can be blinkered by focussing on controls became very evident as they struggled to comply with the over-complicated requirements of the Sarbanes Oxley Act 2002.

Organisations devoted considerable resources to mapping processes and controls, and then even more to checking whether the controls were effective. It is ironic that of all the financial institutions and corporations that we have talked to which had gone through the process of complying with Sarbanes Oxley, not one had actually interviewed the Board of directors and other senior managers to list the potential frauds which they could commit. Yet, these are some of the very people the act was designed to prevent committing fraud.

Are we Hampered or Helped by Operational Risk?

Financial institutions normally place the responsibility for fraud risk assessment on business line managers as part of the operational risk framework. Yet historically, we have found that few organisations have given managers the basic elements to assist them to really understand fraud risks.

A very simple example is that few have actually defined what a fraud risk is.

Similarly, few organisations provide any training to their managers, who have had little or no experience of fraud, in how to assess fraud risks. As a result managers do not understand how controls can be bypassed by a fraudster and so woefully underestimate the level of fraud risks that they face.

It is unfair and impractical to ask managers to assess fraud risks when they don't know what a fraud risk is and have no knowledge of the methods that a fraudster might use. It is like asking a doctor to diagnose a patient without any training.

Furthermore, many organisations have a one-size-fits-all operational risk management framework which requires business line managers to analyse all risks by estimating 'likelihood' as the probability of the risk occurring within a particular time-frame, for example, the likelihood of a fraud occurring in one year or five years. However does it make sense to use 'likelihood of occurrence' when assessing deliberate acts such as fraud?

Ask yourself: do you really believe that a manager (who may have no experience of dealing with fraud) can accurately assess that a fraud risk has a 'high' or 'probable' likelihood of occurring, or believe that someone will commit a fraud in their department within say, one year or five?

This approach works for assessing accidental risks such as systems failure, where it is reasonable to estimate the likelihood of system failing in a particular time frame if routine maintenance is not carried out. But for fraud, the likelihood of occurrence depends on the method of fraud, plus the controls in place, plus the degree of dishonesty and skill level of the perpetrator.

For example, if there is a dishonest person in charge of the cash, there is a high likelihood of occurrence if they can see a way of doing it without being caught. There is a low likelihood of occurrence if an honest person is sitting in that seat. What managers cannot predict with any degree of accuracy is whether someone is dishonest or likely to become so.

When managers are asked to estimate the likelihood of a fraud occurring, they immediately look at their colleagues and wonder whether or not they are going to commit a fraud. As managers naturally want to believe that their employees are honest, it is common for them to assess the likelihood of a fraud occurring in their work area as low. Also, when managers have had little experience of fraud, they find it very difficult to identify how controls could be bypassed.

What makes matters worse is that is that in many cases the resultant fraud risk assessments have then been presented to top management together with other risks in a way that makes it appear that fraud risks have been assessed quantitatively using a mathematically accurate model. This is usually far from the truth; in fact some fraud risk assessments could be better described as pure guesswork.

An Unfettered Approach to Fraud Risk Assessment

At the end of the day, does an Executive Board really want to know when a fraud is likely to occur? Our discussions with Board directors indicate that is not what they want to know. What the Board wants to know is that if a fraud is attempted, will it succeed or not? And what will it take to prevent it? Also, what is the cost to prevent it? Or can the organisation carry the risk?

Answers to these questions are easier to provide by putting in the basic building blocks of an effective fraud risk management strategy which factors in the human element, rather than a rigid operational risk framework which cannot factor this in.

A vital element prior to conducting the assessment is to provide adequate resources and training to business line managers so that they understand how fraudsters work and how they seek to bypass controls. That way the managers will have a reasonable chance of assessing fraud risks and whether or not existing controls are effective. An increasing number of financial institutions have realised such resources training have to be provided by fraud prevention professionals rather than operational risk personnel.

Then the fraud risk assessment should be based on the following principles:

• Fraud is about people misusing the process and other people. The primary objective should be to understand the fraud risks in each job function across the organisation or external relationship.

• Fraud risk is defined as ‘the chance of a perpetrator (or perpetrators) committing a fraud which has an impact on the organisation’. The impact could be positive or negative.

• The fraud risk assessment should identify the methods which a perpetrator could potentially use, considering the existing controls i.e. today’s fraud risks. The current controls, and whether or not they are effective, should be identified for each method.

• Fraud risks should be analysed based on ‘likelihood’ and consequence.

• Likelihood is defined as ‘the chance of a particular method of fraud succeeding today’

• The consequence is the outcome or impact of an event, for example, the direct financial loss; other consequences of fraud may include adverse impacts on: brand image, reputation, market share, internal ethical culture, business operations, and employee morale, as well as costly legal proceedings or compliance issues.

• fraud risk should be rated in a way which allows management to prioritise them and decide whether or not they are willing to tolerate them.

• Having identified the method and associated controls in the risk assessment, treatment options can then be identified for specific methods of fraud in each job function or external relationship.

By making employees more aware and hence more resistant to fraudsters, the organisation will become both more resistant and resilient to fraud.

Executives who can build an organisation with a high resistance to fraud will be able to bridge some of the most significant gaps between theory and practice which still exist today, thereby adding significant value for shareholders and stakeholders alike.

Martin Samociuk and Nigel Iyer have worked as fraud risk management practitioners for many years. A Short Guide to Fraud Risk (second edition) was published by Gower in March 2010 (www.gowerpublishing.com/isbn/9780566092312).