Fraud Risk Management

Human nature dictates that fraud will always be an issue for corporations, and as long as there is fraud, there will be financial and reputational impact

BY MARTIN SAMOCIUK

Despite the enormous worldwide focus on corporate governance and risk management over the past couple of decades, we are still seeing major corporate collapses due to fraud.

Why? It is not as if we do not understand fraud risk, given the number of cases that have been analysed in great detail.

Maybe it is because the laws have not been tough enough. American legislators obviously think so, judging by the introduction of legislation such as the Sarbanes Oxley Act of 2002. But will new laws prevent corporate frauds in the future? This is unlikely, because people do not engage in fraud believing they are going to be caught and punished—they defraud because they believe they can get away with it. Laws have as little relevance for professional fraudsters as they do for dishonest CEOs.

So are there any lessons to be learnt from recent cases that can help a risk manager in implementing a fraud risk management strategy to prevent catastrophic frauds?

This paper examines two main areas where a fraud risk management strategy can be enhanced: analysing the risks from the fraudsters' viewpoint and implementing a detection strategy to act as a positive deterrent.

They are practical steps that are increasingly used by major multinational organisations and financial institutions.

What recent cases have shown is that an organisation can implement a good corporate governance and risk management framework, but when it comes to fraud, if there are loopholes in the controls, fraudsters will exploit them, sometimes with catastrophic results.

Standard risk self-assessment methodologies do not seem to have been of much use in identifying such loopholes.

So what can a risk manager do to gain an accurate understanding of fraud risks right across the organisation and raise them at the appropriate level?

One way is to look at the controls and procedures from the fraudster's viewpoint and ask whether they can be bypassed by using a particular method of fraud.

Many organisations require that line managers assess fraud risks based on a standard framework such AS/NZS 4360:2004. This is a powerful tool to ensure risks are analysed in a consistent manner across an organisation, based on an assessment of likelihood and consequence.

While the standard lays down some fundamental steps that should be followed in the risk analysis process, it does not specify any hard and fast rules as to how the likelihood and consequence should be calculated. Assessment can be either quantitative or qualitative.

Unfortunately, some organisations require line managers to assess the "likelihood" as the probability of a fraud occurring in a particular time frame, for example:

Likelihood	Description
High	Likely to occur within one year
Medium	Likely to occur within ten years
Low	Not likely to occur within ten years

This works when the organisation has a lot of statistics to support the assessment. For example, a bank that issues credit cards knows there is a high probability of fraud because credit card misuse occurs on a regular basis —losses can be quantified.

However, experience has shown when it comes to corporate fraud, asking honest line managers to self-assess the probability of a fraud occurring in their area can result in wildly inaccurate assessments for a number of reasons.

Firstly, the probability of a fraud occurring does not depend solely on the control framework; it depends on someone having the motivation to find or create an

opportunity and exploit it. An honest person will not attempt fraud, however weak the controls. A dishonest person may find ways to bypass even good controls.

Some honest managers cannot see a way around the controls and identify potential fraud opportunities. Fraudsters, on the other hand, are unpredictable, devious and always looking for an opportunity, and they certainly don't tell anyone when they have found a way around the controls.

Managers may be reluctant to admit there is a high likelihood of a fraud occurring in their work area.

Rather than assessing probability, the acid test for any organisation is to ask: "What is the likelihood of this method of fraud succeeding today if attempted either by an dishonest internal or external person?"

If a particular method will succeed, it has a "high" likelihood as shown below.

Likelihood	Description
High	The method will succeed given the current controls (we are sure there are no controls down the line which would prevent it)
Medium	The method may succeed (we are not sure about other controls down the line)
Low	We know the current controls would prevent the fraud succeeding

So instead of assessing the probability of a fraud occurring within a particular time-frame, the organisation's ability to resist fraud attempts is assessed.

Fraudsters, whether they are professional criminal groups or dishonest employees, do not have a limitless number of methods of fraud from which to choose.

There may be novel twists enabled by new technology, but the same basic methods appear year after year. Common examples include the submission of false documents, such as faxes, and the theft of passwords to payment systems.

There are usually no more than five or six methods that can affect any one job function. So managers should conduct a fraud profiling exercise to list as many of these as possible.

The vital element is to provide assistance to those honest managers who find it difficult see around the controls. For example, fraud investigators (who, similar to fraudsters, are not easily impressed by controls) can quickly identify the most common methods that can affect a particular operation.

Once honest managers understand the methods of fraud, they can readily evaluate the likelihood of success.

Each method identified can be analysed according to the likelihood (High, Medium or Low) and potential worst-case monetary loss as shown below:

Method	Likelihood	Worst Case $ Loss
An employee can create false payment instructions with authentic looking forged signatures. These would be input and authorised as normal by the payments team.	High	$200 m

It is widely accepted that the tone set at the top of an organisation regarding fraud prevention has a crucial effect throughout the rest of the organisation. As a result, most large organisations have issued a code of conduct and fraud and corruption policy.

- Unfortunately, sometimes that is the full extent of their fraud risk management strategy because:
- The directors may be focused on cost-cutting and efficiencies in order to improve cost to income ratios;
- The organisation may be focused on risk-taking rather than risk management, particularly where the CEO has a personality of a corporate psychopath;
- The directors may only want to put a gloss on their activities and not have difficult issues raised, such as their use of third-parties to make illicit payments to government officials in other countries to progress the business.

Where directors do want to introduce an effective fraud risk management strategy, there is a chicken and egg situation at the top of most organisations as far establishing the fraud risk appetite. The board has a responsibility to address this, but it needs an accurate analysis of the risks in that:

- an accurate fraud risk analysis is very difficult if using self assessment methodologies
- the risk assessment does not usually include the Executive Directors.

For example, those organisations affected by Sarbanes Oxley ("SOX") are expending a great deal of effort on process mapping and evaluating controls effectiveness in order to enable the CEO and CFO to sign the required management representations.

Yet this does not seem to have addressed the principal reason why SOX was brought into being i.e. fraudulent behaviour by dishonest board executives.

To our knowledge, very few organisations have profiled the frauds which a dishonest chairman, CEO or CFO could commit should they be acting solely or in collusion.

Clearly, directors should be included in the fraud profiling exercise by ranking the different methods which they could use. For example:

Method	Likelihood	Worst Case $ Loss
The CEO and CFO collude to acquire a "strategic" company at an inflated price, in exchange for a kickback to an offshore bank account.	High	$50 m

Experience has shown that when looked at from this point of view, most organisations that think they have low fraud risks usually find exactly the opposite, particularly when the question is asked of the executive directors.

Performing an assessment based on methods which have in fact been used on many occasions by fraudsters provides a practical evaluation of fraud risks.

After listing the likelihood and worst case monetary loss in a fraud profile, senior managers can evaluate the consequence based on the effect on reputation and loss of market share, and the legal and regulatory impact according to a standard risk matrix as shown below.

		Impact				
		Low	Medium	High	Severe	Catastrophic
Likelihood		↓	↓	↓	↓	↓
High	→	Low	Medium	High	Severe	Severe
Medium	→	Low	Medium	Medium	High	High
Low	→	Low	Low	Low	Medium	Medium

Based on the likelihood and impact, an overall risk rating can then be assigned to each individual fraud risk according to the matrix and listed in the fraud profile as shown below.

Risk Reduction

Once the risks have been ranked in the fraud profile, additional controls can be identified to reduce those risks that the business does not want to carry.

Some controls can be implemented quickly, but others may require board decisions on strategic policy changes or significant capital expenditure. It is vital for these issues to be included in a risk register and reported at the board level, for example, to the audit committee.

Fraud risks should also be re-evaluated whenever major change initiatives are introduced, for example, new or re-engineered products or processes.

It is important that where line managers believe that a change initiative has created unacceptable fraud risks, that there is a mechanism for them to report their concerns.

Proactive Fraud Detection

An important realisation for senior management is that however much they try and promote an honest, ethical culture throughout the organisation, they have little or no control over personal factors which may motivate an employee to commit a fraud. These can range from gambling or drug addiction, financial difficulties or resentment against the employer.

The other problem is that even if strong controls are in place, fraudsters are very plausible and can convince honest employees to bypass controls in the belief that they are assisting the "customer".

An organisation can significantly reduce the chances of large losses as a result of corporate fraud by putting in place a detection program either to prevent it succeeding in the first place or to catch it in its infancy.

There are some sound business reasons to embark on a proactive fraud detection program:

The longer a fraud is allowed to run undetected, the larger the losses which build up. For example, there have been at least three recent cases where managers who were addicted to gambling stole relatively small amounts each week, but which built up over a number of years to total losses of $22 million, $19 million and $10 million respectively. Stakeholders are now aggressively seeking answers from senior management as to why frauds were

Risk Level	Method	Likelihood	Worst Case $ Loss	Reputation	Legal & Regulatory Impact
Severe	The CEO and CFO collude to acquire a "strategic" company at an inflated price, in exchange for a kickback to an offshore bank account.	High	$50 m	Severe	Severe
High	An employee can create false payment instructions with authentic looking forged signatures. These would be input and authorised as normal by the payments team.	High	$200 m	High	High

allowed to run unchecked. The knowledge that there is active detection program is a very good deterrent to someone thinking of committing a fraud. Actively looking for fraud may expose potential loopholes which have been overlooked.

An active detection program comprises two elements, red flags and proactive fraud detection.

Red Flags

There are occasions when the behaviour of an individual, or something about the look of a document or transaction, raises a question mark in the mind of an employee. Depending on how astute or alert the person is, the incident may either be ignored and quickly forgotten, or followed up, sometimes to expose a potentially serious problem.

Many frauds have been prevented because an employee noticed something and reported the suspicion. Unfortunately, many more frauds succeed because of a reluctance by employees to report their suspicions and because organisations have tended to discourage reporting and to punish whistleblowers.

Employees are adverse to the personal risks associated with reporting fraud. Some positive initiatives are being taken to reduce the risks. For example, most publicly listed companies are introducing whistleblowing policies and procedures to provide a safe route for employees to report suspicions of potential fraudulent or corrupt behaviour.

However, having a whistleblowing policy is one thing; training employees in what to look for and encouraging them to look is quite a different matter—this requires an understanding of red flags.

Red flags can include changes in a person's behaviour, discrepancies or anomalies in the process or transactions, and alarms and warnings from systems monitoring.

All employees should be provided with fraud awareness training on potential red flags, how to respond to them.

Detection Routines

Once fraud risks have been identified, detection routines can be developed, comprising manual and automated tests. The internal auditor is ideally placed to develop such routines and integrate them into the audit program.

If there are 20-30 different methods in the fraud profile, then only the top 3 or 4 should be selected initially for proactive active detection. Any more than that and the internal auditor risks losing sight of the normal audit program.

The enhancements outlined in this paper are based on practical experience across a wide variety of organisations in Australia, UK and Scandinavia. They should contribute towards a stronger fraud risk management strategy for any organisation.

This article was orginally published in Risk Management magazine (www.riskmanagementmagazine.com.au)