



Fraud risk analysis: do you understand the risk?

Martin Samociuk points out some home truths in the frequently misunderstood process of fraud risk analysis.

Looking at the corporate collapses caused by fraudulent behaviour, it is natural to wonder how effective a fraud risk analysis the victim organisations had in place prior to the event. Was there a fault in the risk management process or is it too difficult to predict when such events may occur?

In all likelihood, the problem lies in the way that fraud risks have been analysed. A consistent feature of victim organisations seems to be that they had not understood their actual fraud risks.

Understanding such risks is dependent on the way the organisation defines the terms used in the fraud risk analysis.

Fraud risk

In order to define the term “fraud risk”, we will first define “fraud” as stated in the International Standard on Auditing 240: “*An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.*”

In other words, fraud involves a perpetrator committing a deceptive act; the key point being that a fraud risk is the chance of a perpetrator using a method of fraud which has an impact on the organisation.

This point seems to be ignored by some organisations. They regard fraud risk as some sort of amorphous entity lurking in the company’s systems and processes which can be statistically analysed in the same way as non-human risks, such as the risk of production of a defective component. As a result they focus on the method of fraud, not the act.

Prior to commencing a fraud risk analysis, participants draw up a universe of fraud risks (when they really mean methods) that might be applicable to the organisation. For example, the list may be drawn up using a standard taxonomy, such as misappropriation of assets, financial misreporting and corruption. Fraud risks are then mapped to the relevant controls and people and/or departments that may be impacted.

This approach seems to be back-to-front when one considers how fraudsters, be they internal or external, actually work. Fraudsters do not need a universe of generic fraud risks; they are in a particular job function, or they establish a relationship as an external party. They need to identify a method of fraud applicable to that area, either bypassing existing controls or by manipulating honest employees.

“Fraudsters do not need a universe of generic fraud risks; they are in a particular job function, or they establish a relationship as an external party”

Preparing a generic organisation-wide fraud risk map encourages a checklist mentality and does not encourage thinking about how a perpetrator might be able to bypass controls. A generic list of methods may be useful to provide initial training, but it will not help to identify a unique method applicable to a specific job function.

FRAUD

To identify potential fraud risks you have to put yourself in the mind of a potential fraudster or “think like a thief”.

Instead of first trying to map generic fraud risks, an organisation should identify job functions and external relationships and then identify potential perpetrators and methods of fraud in order to evaluate the fraud risk.

Inherent and residual risk

The term “inherent risk” is widely used in operational risk management and auditing. For example, audit risk models define inherent risk as the risk of a material misstatement in the unaudited information, assuming the absence of internal control procedures.

Some fraud risk assessment methodologies also suggest that inherent risks should be identified at the start of the process. The output is a list of fraud risks which the organisation would have faced had no controls been included in the business process. The controls are then mapped to the identified inherent risks. “Residual risks” are the risks remaining without appropriate controls, or before any treatment action; ie today’s risks.

There is considerable difference of opinion among risk managers regarding the above approach, with some claiming it is a valid method to identify key controls, and some saying it is unnecessary.

I share the second view when it comes to analysing fraud risk. First, because fraudsters do not care which methods would have been possible with no controls; they want to know what method will bypass controls today. Second, business line managers often struggle to identify inherent fraud risks in the absence of controls and as a result think it is a waste of their time.

Given this, inherent fraud risks should mean the fraud risks which a business is carrying today. As such, a fraud risk analysis should identify those methods which a perpetrator could use today and identify whether or not the current controls would stop the act. If the existing controls would not stop the perpetrator and management does not want to carry that risk, then the risk needs treatment, which may mean additional controls or other action.

The “residual risk” is then the risk which the organisation is willing to carry after treatment (this is in line with standards such as Australia/New Zealand Standard AS/NZ 4360: 2004 Risk Management.)



“A fraud risk analysis should identify those methods which a perpetrator could use today and identify whether or not the current controls would stop the act”

prescribe any hard and fast rules as to how the likelihood and consequence should be calculated; assessment can be either quantitative or qualitative.

It is unfortunate that many organisations insist that business line managers analyse fraud risks alongside other operational risks, in one short session, by estimating “likelihood” as the probability of a fraud occurring within a particular timeframe. For example:

- High – likely to occur within one year
- Medium – likely to occur within 10 years
- Low – not likely to occur within 10 years.

Alternatively, they use terms such as “remote”, “reasonably possible”, or “probable”.

However, when managers assess that a fraud risk has a “high” or “probable” likelihood of occurring, do they really believe that someone will commit a fraud in their department within one year – or that one of their employees is probably likely to commit fraud? Not when we have phrased the questions in these terms.

They could make such an assertion when the organisation has a lot of data to support the assessment. For example, a bank that issues credit cards knows there is a high likelihood of fraud occurring because it knows a lot about the perpetrators; criminal groups regularly commit credit card fraud and losses can be quantified.

However, it does not work where the organisation does not have statistics. An organisation does not know if a

FIGURE 1

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

Likelihood

Risk management frameworks and standards usually state that risks should be analysed in terms of likelihood and consequence and lay down some fundamental steps that should be followed in the risk analysis process. They do not

particular director, employee or external party is dishonest or likely to become so. Therefore, it is difficult to predict the likelihood of a fraud occurring at any level in an organisation. In fact, fraud usually comes as a complete surprise to management and auditors.

Also, in practice, managers naturally believe that all their employees are honest and so assess the likelihood of a fraud occurring in their work area as low. This means that they generally under-rate the risks.

A better definition of likelihood and an acid test for any organisation would be to ask: "What is the likelihood of this method of fraud succeeding today if attempted either by a dishonest internal or external person or group of people?"

If a particular method will succeed, it has a "high" likelihood as shown in Figure 1.

Managers and employees are much more comfortable assessing the risks of fraud by imagining that a theoretically dishonest person is sitting in their seat and attempting to use a particular method. There is no link to the perceived honesty of any existing employees.

Once managers list the methods of fraud, they can readily evaluate the likelihood of success (high, medium or low) and potential worst-case monetary loss as shown in Figure 2. Senior managers can then evaluate other consequences, for example the effect on reputation and market share, or compliance impact according to the organisations' standard risk matrix.

FIGURE 2

Method	Likelihood of Success	Consequent \$ Loss
An operator creates false payment instructions with authentic looking forged signatures. These would be input and authorised as normal by the payments team.	High	\$200 million

Conclusion

A fraud risk analysis using generic inherent fraud risks, likelihood of occurrence and consequences may satisfy the requirements of a standard risk framework. However, the resulting fraud risk maps have limited value in understanding where frauds are possible or in preventing them (as some victim organisations have discovered).

If you want to understand your fraud risks, the analysis should be based on understanding the potential methods of fraud applicable to each job function or external relationship and evaluating the likelihood of a perpetrator succeeding given the current controls. **R**

Martin Samociuk is the author of several books and papers on fraud risk management. The above is based on material drawn from an upcoming publication, co-authored with Nigel Iyer, titled A Short Guide to Fraud Risk due to be published by Gower in the UK later this year.

Looking for a way to realise essential time savings and accomplish a streamlined approach to risk management?



Some of the many benefits of our system are:

- The capability to track risk reduction activities and report on progress.
- Risk Register creation and maintenance tools.
- The ability to automatically generate your organisations' risk reporting for board or regulatory consumption.
- Make management decisions based on flexible risk analysis.

We're so confident in our software that we offer an initial on site or web based demonstration, followed by a FREE, NO OBLIGATION evaluation period. You have nothing to lose so contact us today! Online request at: www.pentana.com/demorequests Email: info@pentana.com Call +61 3 9754 4500

Then discover the pioneering software from Pentana today!

Pentana software has been created and developed by our team of industry experts to reflect the needs of our international clients. Ensuring that you get a commercially proven, comprehensive toolset configured to your requirements.



 **Pentana**
Innovative software - integrated services
www.pentana.com