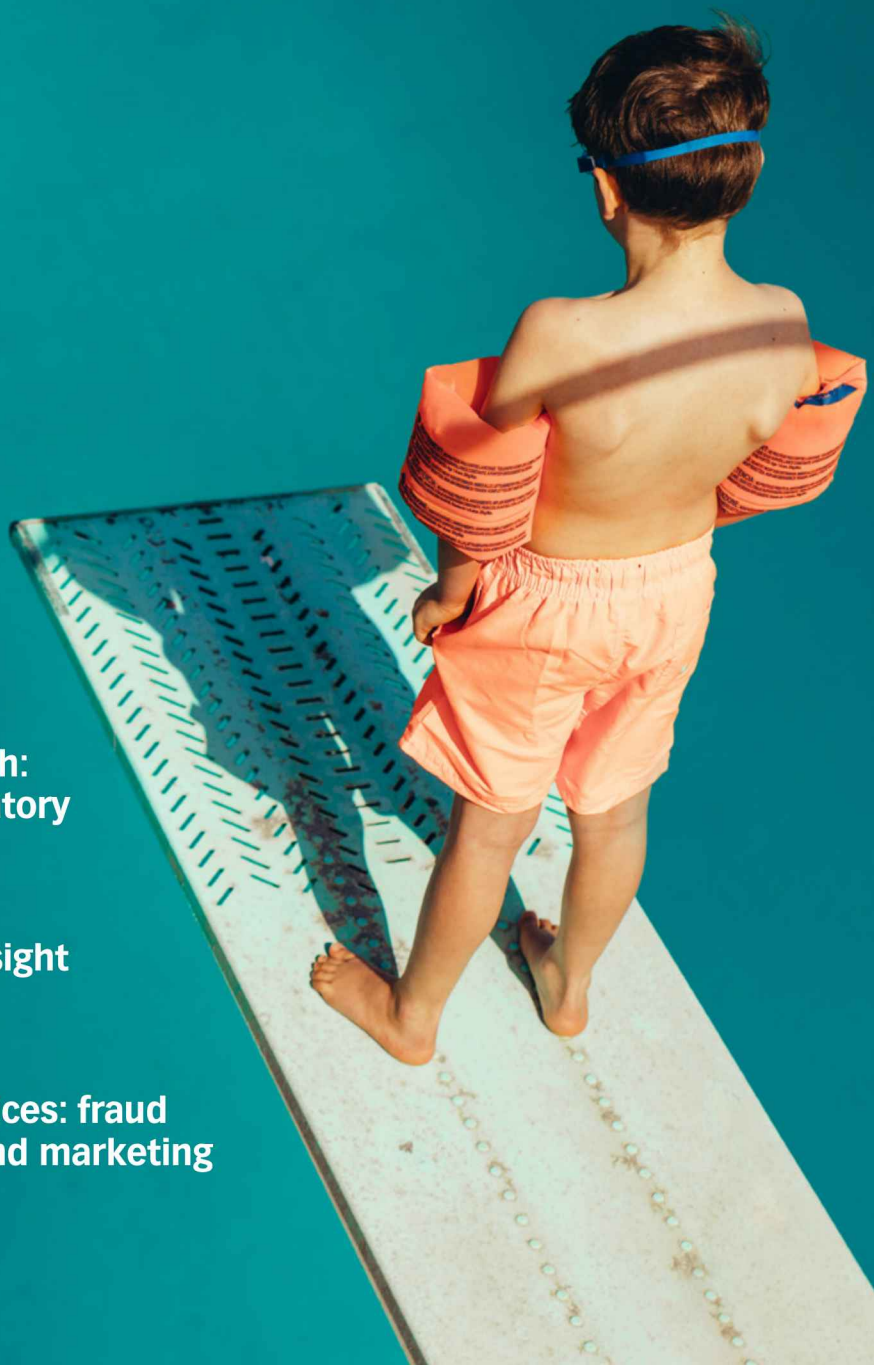
R&C risk & compliance

APR-JUN 2023

www.riskandcompliancemagazine.com



Inside this issue:

R&C

Editor: Mark Williams
Associate Editor: Fraser Tennant
Associate Editor: Richard Summerfield
Publisher: Peter Livingstone
Publisher: James Spavin
Production: Mark Truman
Design: Karen Watkins

Risk & Compliance
Published by Financier Worldwide Ltd
First Floor, Building 3
Wall Island, Birmingham Road
Lichfield, WS14 0QP
United Kingdom

+44 (0)121 600 5910
riskandcompliance@financierworldwide.com
www.riskandcompliancemagazine.com

ISSN: 2056-8975

PERSPECTIVES

KEYS TO PROACTIVE FRAUD RISK MANAGEMENT

BY **GERRY ZACK**
> SCCE & HCCA

On the surface, the management of fraud risk shares many characteristics with the management of other risks. At a high level, fraud risk management involves the following components: identification of fraud risks, assessment of the risks, evaluation and improvement of fraud-related internal controls, and monitoring and auditing of ongoing performance of the fraud risk management process.

While these components mirror those applied in other areas of risk management, there are several unique considerations in applying them to the management of fraud risks. Additionally, an investigative function is a critical component of a fraud risk management programme that may not be present in all other areas of risk management.

A detailed exploration of the many elements that comprise each of these components is not possible in a short article. Rather, the approach here will be to point out a few areas where improvements can often be made to strengthen the fraud risk management process.

Consider risk drivers

Risk managers often begin the process by identifying specific fraud risks that the organisation may be susceptible to and then immediately jump into assessing those risks. An extremely valuable

step to consider in connection with identifying risks, however, is to evaluate what drives fraud risk. Drivers of fraud risk impact both the nature of the frauds that a company is exposed to as well as the assessment factors, such as each risk's likelihood or impact.

What do we mean by risk 'drivers'? Drivers are events that give rise to new risks or changes in existing risks. Examples include: changes in technologies used by the organisation, changes in the people employed by the organisation and external developments such as changes in competition and economic factors.

Technology is one of the most obvious examples of a driver that can increase or decrease risk. Most of the time, new technology is implemented in order to gain operational efficiencies. But often, deployment of new software or other technology opens up new or different fraud risks, or changes some of the characteristics that impact a fraud risk assessment. Every time new technology is implemented, including things as simple as upgrades

to existing technology, fraud risks can change, and this must be considered.

Likewise, changes in other internal and external environmental factors can have a profound effect on fraud risks. For example, increased competition can increase incentives or pressures to engage in corruption or other frauds to gain or maintain competitive advantage. Similarly, increased pressures on employees can result in workers cutting corners, affecting vital internal controls.

Identify alternative fraud methods

One common mistake made in assessing fraud risks is to group frauds at an aggregated level. For example, an organisation might identify the payment of bribes in order to obtain new business as a fraud risk. While this is clearly a category of fraud, there are numerous manners in which a bribe can be paid, and the internal controls associated with each technique are vastly different. For example, the controls associated with preventing or detecting bribes paid through shell companies are very different from those needed to manage the risk of bribes paid by disguising them as payroll or expense reimbursements. Grouping them all together can result in an inaccurate picture of the level of risk and an incomplete consideration of internal controls.

Accordingly, the level of aggregation or disaggregation with which fraud risks are assessed is an important consideration. If the nature of the relevant internal controls associated with each method of perpetrating a fraud are vastly different, then consider them as different risks. Keeping them separate will facilitate a much better risk assessment and risk remediation plan.

Utilise data and quantify assessments wherever possible

Some organisations assess fraud risks based purely on judgment, sometimes assigning scores or levels like low, medium and high to assessment criteria such as likelihood and impact. These assessments are often based on interviews, surveys and similar methods. While this is better than not doing a risk assessment at all, it leaves room for improvement.

Starting with past history of fraud events, collect data to help in the evaluation of risks. Consider things like the number of people involved in a process, the number of steps and number of opportunities for something to go wrong.

To take a risk assessment to a more advanced level, use probabilistic models to refine and measure risk more precisely. Remember this: fraud risk assessment is a process with many opportunities for improvement. View the risk assessment as something that can be improved from year to year. Always look for ways to improve it by gathering and considering additional, relevant sources of data from internal and external sources.

Consider the relationship between fraud and compliance risks

Often, one type of risk has potential interactions with other risks. The nature of these relationships can vary. For example, sometimes the existence of one risk gives rise to another risk. In other cases, mitigating one risk may increase the likelihood or impact of another.

With fraud and compliance risks, the relationship is even more important, so much so that it makes sense to consider them together in certain respects. Not all frauds create compliance risk, and not all compliance risks involve fraud, but there is often a connection between the two.

Compliance risk can be defined as any legal or regulatory risk that can create liability for the organisation. Fraud risks involve intentional acts designed to achieve some inappropriate benefit, either for an individual or for an organisation.

Accordingly, the evaluation of compliance risks should consider the potential for intentional noncompliance for personal or organisational gain. Usually, intentional acts also involve steps taken to conceal, adding a layer of complexity to detection that is not present when noncompliance is accidental or the result of carelessness. Bribes paid with corporate funds are a good example of this. They represent frauds in that they are intentional acts and are an improper use of organisational funds that is misrepresented in the financial records. And they may also represent compliance risks, especially if the bribes are paid to government officials or otherwise to obtain business for the company.

> **"No matter how strong internal controls are, fraud or allegations of fraud will eventually occur. The importance of being prepared for these times cannot be overstated."**

Similarly, fraud risks should be evaluated for possible compliance ramifications. In many frauds involving theft from the organisation by an employee, no organisational compliance issues result. It is simply a risk of loss. However, some frauds may directly result in compliance issues for the organisation.

Monitor for signs of fraud

Internal controls need to focus on both prevention and detection of fraud. The key to minimising

damage from frauds that have not been prevented is early detection. This is where the use of data analytics can help immensely. For all critical fraud risks, identify which data would be affected if fraud is occurring, and monitor it on a regular basis.

The volume of data collected is immense. Determining which data is affected by fraud and monitoring it is not always an easy task. Most frauds have an impact on multiple data points. What data analytics focuses on is identifying anomalies in data that are indicators of fraud. Once anomalies are detected, further investigation is warranted to determine whether fraud is occurring.

Take the risk of using a shell company to funnel bribes as an example. Data analytics could be used to look for signs of shell companies. Examples of such indicators include incomplete vendor master file information, addresses that do not align with expectations, payment patterns and numerous other possible anomalies. Once such anomalies are identified, explore the transactions or activity further.

Invest in the investigative function

No matter how strong internal controls are, fraud or allegations of fraud will eventually occur. The importance of being prepared for these times cannot be overstated. And in today's environment, frauds are more complex, and the requirements of an investigative function are greater than ever.

For many years, surveys have shown that the top method of identifying fraud is through reports received from employees, customers and other third parties. And one of the most important factors leading to an individual's decision to report suspicious activity is the level of trust that person has in the investigative process. Quite simply, if a person does not think the investigative team will treat an allegation seriously or with the utmost professionalism, they will not bother reporting it.

This means that every organisation should have a plan for how it will handle each type of investigation (i.e., who conducts the investigation and whether external resources are used). Additionally, investigative procedures should be established and consistently followed. Knowing that allegations will be investigated in a consistent, thorough and impartial manner is critical to building trust.

There are dozens of characteristics that should be considered in developing and maintaining a fraud risk management programme. Those discussed here represent some of the most common opportunities for significant improvement. R&C

Gerry Zack
Chief Executive
SCCE & HCCA
T: +1 (952) 567 6215
E: gerry.zack@corporatecompliance.org