Deloitte.

Fraud, bribery and corruption
Protecting reputation and value

An investor's choice

Imagine two similar companies that are alleged to have engaged in a significant incident of fraud or corruption.

Company A takes a proactive approach to managing fraud and corruption risks, has world-class — but not infallible, anti-fraud and anti-corruption processes ingrained in its control processes; has a good relationship and strong record with its regulators; has robust plans in place to investigate potential wrongdoing and is capable of implementing crisis communications to help protect the company's reputation.

Company B takes a reactive approach, is confident in its ability to deal with issues as they arise, and is a follower rather than a leader in implementing risk management and anti-fraud and anti-corruption processes.

As an investor, which company would you believe better protects your investment? As a senior executive, or audit committee member, which entity would you judge to be better able to demonstrate that you have fulfilled your responsibilities?

Of course, there is no guarantee that a better-prepared company will experience a more favourable outcome than one that chooses a reactive approach. However, experience suggests that companies that manage their risks proactively or use predictive technology may be less vulnerable to having their reputations harmed by allegations of wrongdoing, falling behind in the news cycle of reactions, and losing the support of regulators, customers, suppliers, investors, the general public, and even politicians.

Global media and the Internet enable news to travel faster and reach more people than ever before. The international nature of business and growing collaboration among regulators worldwide can expose companies to a greater number of regulatory regimes. These factors may increase both the likelihood and the potential impact of alleged wrongdoing on a company's reputation and shareholder value. Executives and audit committee members should consider how their company manages its risks of fraud and corruption and whether today's risk environment merits a more proactive approach.

.

"Protecting your entity's reputation, value, and sustainability requires a paradigm shift from the traditional reactive approach of fraud and corruption strategies to predictive detection, not only theoretically but in practice."

Dave Kennedy
Leader, RA Forensic, Southern Africa
Managing Director, Risk Advisory, Africa

Ten areas that executives and the audit committee should evaluate to help mitigate reputational risks of fraud, bribery and corruption

There are many ways that management, assisted by the audit committee and internal auditors or advisers, can seek to help audit committee members and the board of directors mitigate reputational risks that could arise from alleged fraud, bribery, or corruption. Below, we outline ten items that can help executives and audit committees to gauge the company's sophistication in this area and assess the scope for improvement.

Integrating risk and strategy

When risks and rewards are considered separately, it may be easier for those pursuing growth to omit or diminish consideration of reputation and compliance risks. Holding senior and operational management responsible for considering risks and balancing them with potential rewards can foster wise risk-taking. Does management consider risks holistically in developing and implementing the company's strategies and business plans?

Crisis management planning

Has the company developed a crisis-management plan to react to allegations of major fraud or corruption? Does that plan include assigned responsibilities for management and advisers to help drive actions and communications that will sustain confidence? These plans can be valuable in implementing a robust response to allegations under severe time pressure and intense scrutiny from the media, regulators, investors, and law enforcement agencies.

Comprehensive risk assessment

Risk assessment is the foundation upon which effective anti-fraud and anti-corruption processes are built. Does management conduct, document, and update an assessment of fraud and corruption risks periodically (typically annually)? Can management explain key fraud and corruption risks that may affect the company's reputation? For example, are the organisational systems, processes and financial reporting appropriately assessed to prevent fraudulent activity?

Risk tolerance and mitigation planning

Does the board understand management's level of overall risk tolerance and its level of risk tolerance for fraud and corruption specifically? Has the board determined its level of risk tolerance for these matters? Having the board determine risk tolerance is not easy, and the practice is not yet widespread, but if the board has done so, to what extent does it correspond to management's level? Are efforts to mitigate these risks designed to bring them within the risk tolerance level? Incidents of major fraud and corruption may indicate a gap between the risk tolerance level of the board and that of management, or between that of executive management and line personnel.

Managing performance and compensation

Is effective risk management an explicit element of performance assessment and compensation for executives and managers? Holding senior executives and line management accountable for managing ethics, compliance, and the fraud and corruption risks within their area of responsibility is likely to be more effective when it influences their compensation. This can be evaluated using objective measures, such as the results of an assessment by the internal audit function.

Evaluating the tone at the top

Does management evaluate employees' perceptions of the tone at the top periodically (leading practice is annually), using techniques such as an employee survey? A professionally designed and independently administered survey should serve as an early warning system, alerting the audit committee to a tone that falls short of its expectations.

To understand and to be able to detect fraudulent activities, employees should be aware of the behavioural aspects of individuals and organisations. The behavioural aspect of individuals assists in profiling a typical fraudster while that of organisations typifies the risks that make the organisation susceptible to fraud.

Ten behavioural aspects of individuals and organisations that are typically "red flags" or "fraud indicators" that all employees within an organisation should be aware of in their daily functions:

- Staff under stress without heavy workload or always working late.
- Staff engaging in other activities requiring funding, such as gambling or extra-marital relationships.
- Always being anxious and defensive when asked routine questions.
- Reluctance to take leave.
- High staff turnover, with new staff resigning quickly.
- Desire to "beat the system".
- Defendant in a civil suit.
- Rationalisation for conflicting behavioural patterns.
- No signs of a code of personal ethics.
- Undisclosed conflicts of interest.

Indicators that the organisation or department may be a target for a fraudster:

- Does not enforce clear lines of authority and responsibility, especially for authorisation of transactions.
- There are a lack of adequate documents and records within the entity.
- Lack of segregation of duties
- Inadequate physical security in departments, such as locks, safes, fences, keys, cards, etc.
- Inadequate personnel policies and human resource management systems.
- Inadequate process for disclosure of income from external remunerative work and undisclosed conflicts of interest.
- Operating on a crisis basis and without budgetary control.
- Inadequate communication and awareness regarding disciplinary codes, fraud policies and codes of conduct.
- Inadequate background and reference checks before hiring decisions are made.

Whistle-blower system benchmarking

Do management and audit committees review an evaluation of the whistle-blower system that benchmarks its performance against industry-specific statistics? A benchmarking analysis may help to identify an underperforming whistle-blower system, enabling remediation. In our experience, below-average use most often arises in hotlines that are not effectively communicated to employees and other potential users, or where users lack confidence that reports will be addressed appropriately without retribution.

Leveraging transaction monitoring and data mining

Has the company implemented computer-assisted transaction monitoring and data mining targeted at its key fraud and corruption risks? These tools are especially valuable in entities with a large volume of transactions and potentially high-impact fraud and corruption risks, such as violations of the Prevention and Combatting of Corrupt Activities Act, the Foreign Corrupt Practices Act or the U.K. Bribery Act. Today's technology, combined with skilled evaluation of anomalies, can enhance deterrence and detection capabilities in this area significantly.

Regulatory relationships

Does the company have a good relationship with regulators, such that regulators may be more supportive if the company has to investigate alleged wrongdoing? Companies of all sizes are vulnerable to additional costs, restrictions on operations, or potential shutdown if regulators decide they cannot be trusted to investigate themselves. A cooperative relationship and a strong record with regulators can help to avert turning a serious allegation into a regulatory crisis.

Investigative resources and protocols

Financial investigations often involve locations on the other side of the world, involving a different language, different laws, and a different culture. Predetermining investigative resources and protocols can speed an investigation and also help reduce the risk of ineffective investigations. Have management and the audit committee identified in advance the legal, computer forensics, and forensic accounting resources needed to conduct internal investigations into serious allegations that may arise wherever the company operates? Has it approved a set of investigation protocols to help avoid reputational risks that can arise from inappropriate investigation methods? Do the company and its whistleblower system operator have a process to identify the correct parties to notify internally for different types of allegations? Does this process set forth investigation roles and responsibilities depending on the nature of an allegation?

Conclusion

The audit committee can be valuable in probing management's decisions regarding the appropriate level of sophistication of the processes to help mitigate the reputational and financial risks of alleged fraud, bribery and corruption. Management, the audit committee and the board may have different views on the cost/benefit trade-offs involved and the appropriate balance, given the risk environment. Asking the questions set out above may help to better define and mitigate reputational or financial risk in the event of allegations of fraud, bribery or corruption.

Contacts

Dave Kennedy
Leader, RA Forensic, Southern Africa
Managing Director, Risk Advisory, Africa
Direct: +27 (0)11 806 5340
Mobile: +27(0)82 780 9812
Email: dkennedy@deloitte.co.za

Tommy Prins
Director, Risk Advisory, Forensic
Mobile: +27 (0)82 824 2815
Email: tprins@deloitte.co.za

Navin Sing
Director, Risk Advisory, Forensic
Direct: +27 (0)31 560 7307
Mobile: +27(0)83 304 4225
Email: navising@deloitte.co.za

Clayton Thomopoulos
Director, Risk Advisory, Forensic
Direct: +27 (0) 21 427 5680
Mobile: +27 (0)82 749 4638
Email: cthomopoulos@deloitte.co.za

Gregory Rammego
Director, Risk Advisory, Forensic
Direct: +27 (0)11 806 5255
Mobile: +27 (0)82 417 5889
Email: grammego@deloitte.co.za

Marc Anley
Director, Risk Advisory, Forensic
Mobile: +27 (0)79 893 8191
Email: maanley@deloitte.co.za

Praveck Geeanpersadh
Director, Risk Advisory, Forensic
Direct: +27 (0)11 806 5437
Mobile: +27 (0)82 450 7387
Email:
pgeeanpersadh@deloitte.co.za

Graham Dawes
RA Leader – Rest of Africa
Mobile: +254 719 892 209
Email: grdawes@deloitte.co.ke