The Dark Side of Ethics and Integrity

Mark Boult, Nigel Iyer and Richard Minogue

Reputational damage and even corporate collapse can result from reckless risk taking, fraud, corruption and greed.

Traditional risk management copes poorly with the dark sides of human behaviour. A new, more human approach is needed to deal with fraud, corruption and other integrity risks. By integrity risk, we mean this: the likelihood of someone inside of the organisation committing an integrity violation which impacts the organisation.

Organisations face innumerable integrity risks, at every level and division, affecting every asset, person and objective. Imagine convincing management to approve a traditional programme to identify these risks for every person and asset! Would there be endless questions and boxes to tick? There is an easier way.

Integrity risk assessment

Traditional risk assessment starts with classification of assets or objectives, analysis of threats and determining factors, and of mitigating controls. Fraud opportunities are difficult to spot while attention is focused on the adequacy of existing processes and controls. The likelihood of occurrence is difficult to assess, because it depends not only on what can occur but on the willingness of individuals to break rules, and the level of internal tolerance to unethical acts. In mid-2008 most Britons would probably have minimised the likelihood of mass expense fraud among Members of Parliament. A year later, they would say it was "a certainty".

Assessing integrity risks involves looking at each position associated within the organisation and what the person could do if he or she were dishonest, as shown in Figure 1.

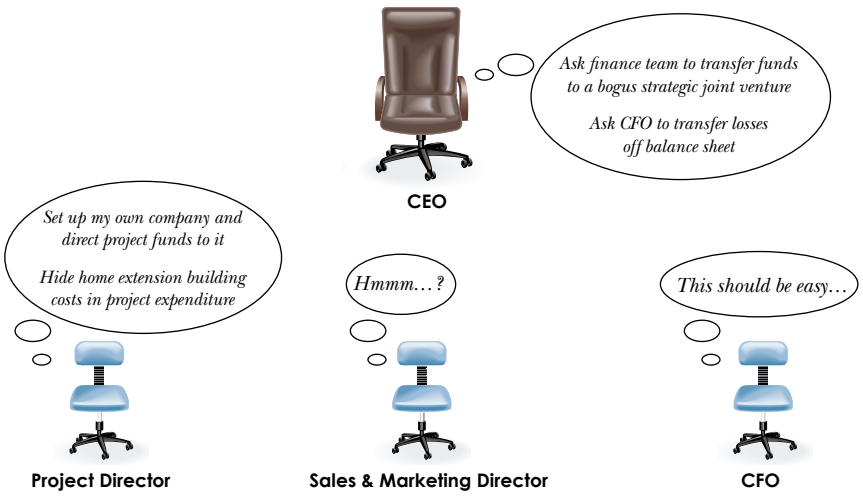

Figure 1 Brainstorming technique – think like a thief

"You have five minutes to think how to get £100,000 out of your organisation by any means. You can be whoever you like. All you need is motivation, greed and imagination to find a loophole in the system. Don't get caught!"

Facilitated brainstorming with employees is an effective, cost efficient and motivating solution for integrity risk assessment. Employees know which rules are followed or broken, and which integrity breaches are common. The trick is getting them to see the implications, and to speak up. To provide the necessary motivation, brainstorming is often combined with integrity training.

While assessing risks, you also raise participants' awareness. Properly prepared, the technique works with employees from top management to the factory floor, exposing integrity risks at every level. The grass roots approach, which might replace or complement the top down risk assessment, follows these basic principles:

- Integrity risk is a function of both people and processes. The objective is to understand risks in each job function or external relationship.
- Integrity risk is the likelihood of someone inside the organisation committing an integrity violation which impacts the organisation.

The brainstorming session identifies methods a perpetrator might use, and reviews existing controls. Identified threats are then assessed, based on likelihood and consequence, and weighted to help management establish priorities and countermeasures.

This brings us back to the human factor. When someone deliberately behaves unethically, they are anxious to avoid detection and punishment, even if that means working against the organisation's interests. The most damaging consequences of integrity failure come not from the incident itself, but from an abdication of responsibility.

Next steps

Once integrity risks are identified and assessed, management decides its response, and how to create an environment where they are prevented or detected promptly.

Preventive controls are designed to avoid undesirable events altogether. This reveals an important difference between unintentional error and deliberate incidents. The outcomes might be identical; an invoice might be accidentally or deliberately paid twice. Accidental errors are, however, much easier to prevent than intentional violations where trusted persons actively seek to defeat controls.

Strong prevention is expensive, and the strongest measures would outweigh the value of protected assets. Managers must accept that controls alone cannot reasonably prevent integrity violations.

Early detection routines can compensate for the limitations of prevention. While a detection control will typically not provide conclusive evidence that integrity has been violated, it will identify an unusual event that merits further investigation. Increasingly organisations perform integrity health checks

designed specifically to detect red flags that would otherwise go unnoticed. Detection programmes are only useful if somebody does the follow up-work, but even a modest project will help deter greedy opportunists.

The likelihood of unethical acts is determined by opportunity, the propensity of individuals to break rules and the way the organisation accepts or resists such behaviour. Good internal controls reduce opportunities, while an active integrity programme strengthens internal culture, making it more resistant to inappropriate behaviour. A successful programme requires sincere commitment and the active support of management.

How good are you at managing integrity risks?

Integrity risk management is challenging. Before embarking on a project, management might want to evaluate its current state of preparedness. Below shows 12 factors which influence integrity in an organisation.

Sample assessment

Here are 12 factors that influence the level of integrity risk management in an organisation:

1. Tone at the top
2. Risk assessment
3. Risk treatment
4. Implementation of controls
5. Training and awareness programmes
6. Risk follow-up
7. Internal audit process
8. Monitoring by executive board
9. Monitoring and detection
10. Management of incidents
11. Learning from events
12. Results and review of action

Organisations can perform a comprehensive assessment, complete with interviews and detailed protocol. A less vigorous approach, sometimes used as a first step, is a quick assessment based on employee perceptions, using the same 12 point model. These two tools provide a means to measure, benchmark and monitor integrity risk management maturity in a simple (perception) and robust (assessment) manner.

Many organisations have yet to start managing integrity risks in a structured way, let alone measure progress. For those who would like to start, a survey among managers with the results presented to the board can raise management awareness.

This so-called lightning assessment of resistance to unethical behaviour, fraud and corruption is perhaps subjective, but it does provide top management with participants' perceptions of how integrity risks are handled, and an introduction to a structured approach to integrity management.

Managers anonymously complete questionnaires containing carefully structured scenarios and multiple choice questions, selecting the most appropriate answers. Responses are complied into a model which aggregates and allocates scores to each of the 12 elements. An example question, and complete survey results are shown below.

Sample lightning assessment question

Which answer best represents the general attitude in your organisation regarding fraud prevention?

A. We trust each other. Internal controls are only a secondary line of defence against fraud.

B. People are very unlikely to try anything as they are sure to get caught and penalised.

C. We have improved in recent years but we still have some way to go.

D. Our management controls are much more effective than before in creating an effective deterrent.

E. We are always trying to understand better the risks of fraud facing our organisation and taking innovative steps to bring this risk down to zero.

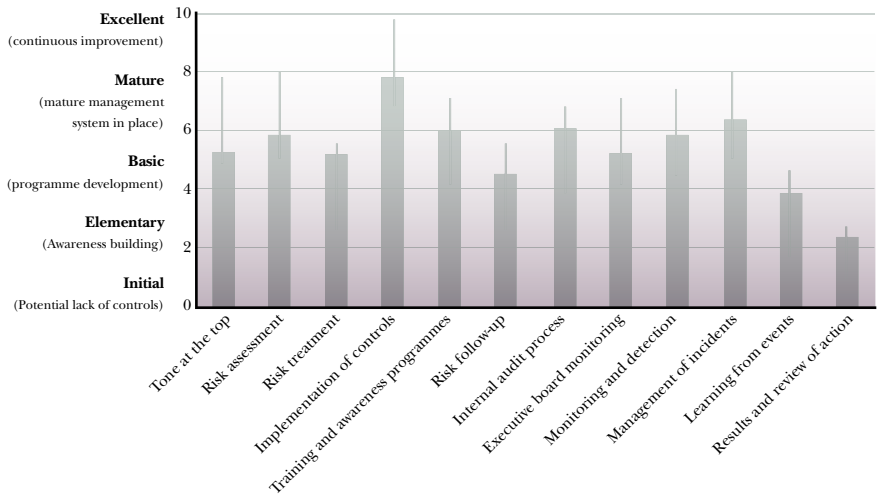

Figure 2 Lightning assessment results

The results paint a picture of an organisation which focuses on internal controls and dealing with incidents. However, it has some work to do in learning from events and implementing improvements. The wide variety of responses for tone at the top suggests that management may have not succeeded in communicating a strong ethical tone. Risk assessment also shows a wide response spread, indicating that people are not as aware as they should be about what fraud risks are and how they should be managed.

Management can define the maturity level it would like to achieve in the short, medium and long term, and derive actions to achieve this maturity. Development of actions can be achieved by drawing on the details of the full rating tool in the areas where improvement is most needed.

Once improvements are underway, the full assessment tool can be used to get a robust and detailed assessment of the organisation's maturity. It can form the basis for specific improvement actions, benchmark the organisation (or parts of it) and measure and demonstrate improvements over time.

Summary

Every day we hear how people, organisations and governments can have their reputations shattered when their actions are regarded as unethical. In extreme cases this can bring them down and create hardships for many innocent people. We all need to act proactively to manage these risks and ensure the integrity of ourselves and our organisations.

Tools are available to help us identify weaknesses and strengths in our management of integrity risks, and to support the development of improvement actions to minimise the potential for and the magnitude of integrity incidents on our organisations.

When employees understand integrity issues and are convinced of management's sincerity about them, they will be that much more proud, loyal and alert.

Mark Boult MIRM is Principal Consultant with DNV. Richard Minogue and Nigel Iyer are Partners with Septia Group.

They welcome comments and criticisms at richard.minogue@septiagroup.com, mark.boult@dnv.com and nigel.iyer@septiagroup.com.