Find the problem before it finds you

By the Financial Forensic Investigation Team of the Attorneys Fidelity Fund

Allowing events to destroy the vision you have of your firm can be managed and limited, but how?

When you decide to open a firm, irrespective of size, you have taken a decision to run a business. Wikipedia defines a business as 'an organisation involved in the trade of goods, services, or both to consumers [or clients]' (http://en.wikipedia.org/wiki/business, accessed 25-5-2015). Legal firms are mainly involved in providing professional services to clients. While you may have thought through what you would like to achieve in running a business, there could be opportunistic events that may affect the realisation of your goals.

Before getting excited about owning and running a business, and before counting the chickens before they hatch, take a step back and ask the following questions:

- Have you taken the time to find the problem before it finds you?
- Do you know and are you keeping watch of what can destroy your vision?
- Do you know and are you conversant with challenges that may be posed by Information Technology (IT) in your firm?
- Do you keep abreast of developments in the industry?
- Are you employing the right calibre of staff?
- Are you compliant with the legislative and regulatory environment?
- Have you identified your stakeholders whose expectations you need to fulfil?

These are some of the areas you need to visit and understand, and the list is not exhaustive, in order for you to find the problem before it finds you.

Figure 1 below depicts some of the stakeholders that a firm may have to consider, as well as how they overlap, which requires a balanced response to their needs and interests.

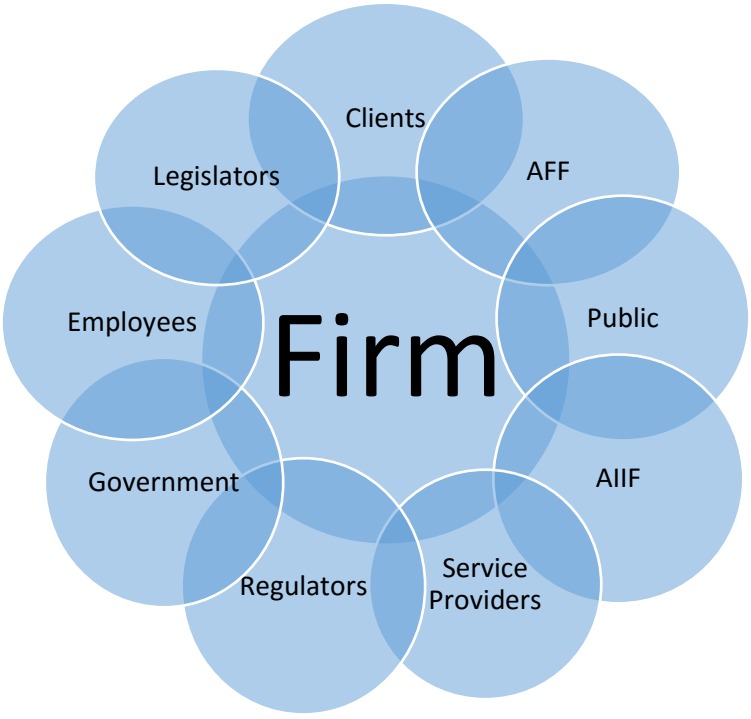


Figure 1: Overlapping stakeholders

This article seeks to address Enterprise Wide Risk Management (ERM) and revealing its benefits for business, a concept that should be at the forefront of each practitioner's mind. This process should involve everyone in the firm irrespective of their position.

What is ERM?

ERM is sometimes viewed as a way of aggregating, managing and reporting on all of the risks facing an organisation – a way to consolidate the information within the individual risk silos. That is a necessary and desirable goal, but it is not specifically ERM. There are many definitions of ERM, but the definition provided by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (the five sponsporing organisations are: American Accounting Association; American Institute of Certified Public Accountants; Institute of Internal Auditors; Institute of Management Acounts; and Financial Executives International) as outlined in COSO's Enterprise Risk Management – Integrated Framework, published in 2004 (www. coso.org/documents/COSO_ERM_ExecutiveSummary.pdf, accessed 25-5-2015) has gained prominence and acceptance by many organisations.

COSO defines ERM as 'a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives'.

This definition reflects certain fundamental concepts. ERM is:

- 'A process, ongoing and flowing through an entity
- Effected by people at every level of an organisation
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories' (see COSO Enterprise Risk Management – Integrated Framework op cit).

According to the framework (op cit): 'This definition is purposefully broad. It captures key concepts fundamental to how companies and organisations manage risk, providing a basis for application across organisations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining ERM effectiveness.'

Although risk management is a business process, it is not a process that functions in isolation. Risk management is also not a once-off activity but is performed on a daily basis as part of ongoing operations. For risk management to be effective, it needs to be linked and integrated with all business processes, from strategic planning to operational processes. There are eight key components of the ERM process and these are discussed below:

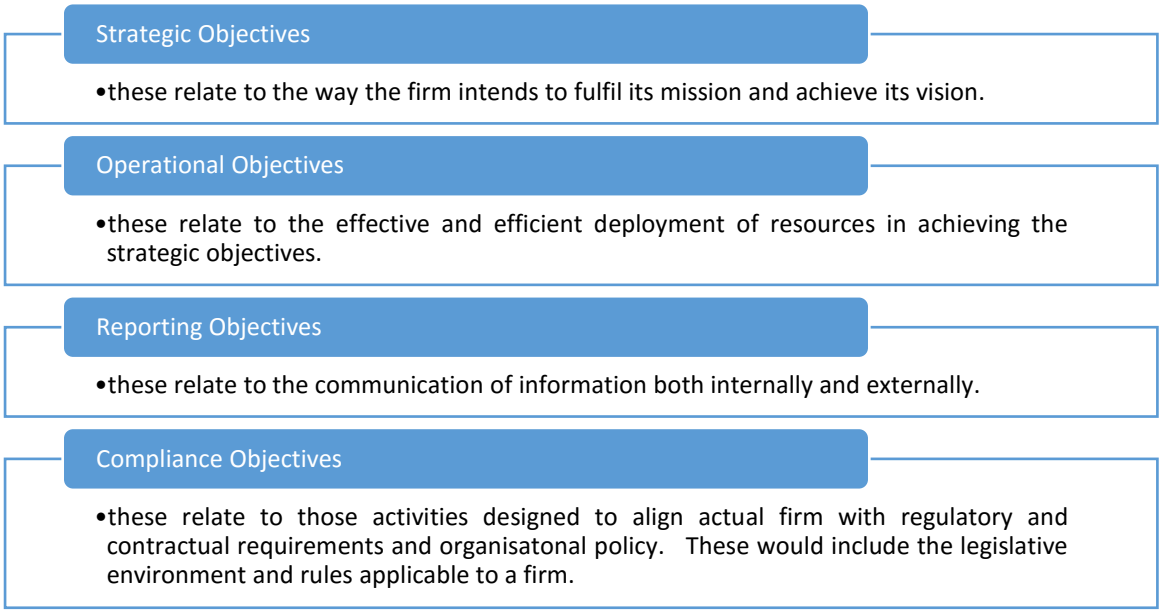
1. Internal environment

This encompasses the tone at the top and sets the basis for how risk is viewed and addressed by the organisation's people. It would include defining the risk appetite of the organisation, integrity and ethical values, and the environment in which they operate. Practitioners should always keep in mind

that their stakeholders, both internal and external, want to know what the firm stands for – its ethics, values and intentions. They want to know that it can be trusted to do the right things in view of increasing concerns about – among other issues – bribery, corruption, fraud, failures in data security, etcetera. An example of how a practitioner could set a tone around its lack of tolerance for fraud perpetrated by staff against the firm could be by exposing such individuals through various forms, including, laying criminal charges against such employees.

2. Objective setting

It is important and necessary to define the direction that the firm should take. There should be a process to set objectives of the firm, which objectives should support and be aligned with the firm's vision and mission and consistent with its risk appetite. It is also important to document the objectives that the firm should achieve. Documenting the set objectives assists in keeping watch throughout risk management to ensure that whatever processes/interventions take place they remain in line with the set objectives. Objectives may be set at various levels of the firm. The diagram that follows depicts the four main types of objectives:



3. Event identification

Once the objectives have been set, internal and external events that could potentially affect the achievement of those objectives should be identified. These could arise from sources such as key business processes, technology, people, economic factors and client demographics and behaviours. Potential events with a negative effect on the firm represent a risk to the firm and these should be managed, while events with a positive effect represent opportunities, which should be channelled back to the strategic objectives. This step is crucial as proper identification can protect a firm from possible downfall, while poor event identification can leave room for a downfall. Of importance is that risks are identified at different levels in the organisation, at both strategic and operational levels. Risks identified at strategic level should be taken down to operational level as the actual management takes place through day-to-day activities at operational level.

4. Risk assessment

The identified risks need to be assessed for their impact and likelihood in the achievement of the objectives. In assessing the risks, both the inherent and residual risks should be assessed. The inherent risk refers to that risk that exists with the mere existence of the business and/or activity, before any controls are put in place. The residual risk refers to the risk that remains (residue) after controls have been put in place, and this is the risk that the practitioner should mainly be concerned with. The risk remaining after the controls (residual) should not be greater than the defined risk appetite of the firm. The outcomes of the risk assessments should be documented in a risk register, which should be reviewed and updated as frequently as required by the firm.

5. Risk response

Once risks have been assessed, the practitioner should evaluate various strategies to respond to the assessed risks. Below are the various strategies that the practitioner can decide on:

- **Tolerate** – the risk is known and accepted by the firm.

- **Transfer** – the risk continues to exist, but it is passed on to a third party to manage, for example an insurer or outsourcer.

- **Terminate** – the firm has no appetite for the risk and will, therefore, stop the process, activity, etcetera.

- **Treat** – introduce controls and continuity strategies in order to reduce the impact and likelihood of the risk materialising.

These response strategies are at times referred to as the 4T's. Value creation is one of the principles in ERM. It is, therefore, important that in responding to a risk, the cost involved should not exceed the benefit to be derived.

6. Control activities

These are part of the process by which a firm strives to achieve its business objectives. They are policies and procedures that help ensure risk responses are properly executed. It is best practise to have both the policies and procedures documented. The Business Dictionary defines 'policies and procedures' as 'a set of principles, rules, and guidelines formulated or adopted by an organisation to reach its long-term goals and typically published in a booklet or other form that is widely accessible' (www. businessdictionary.com/definition/policies-and-procedures.html, accessed 25- 5-2015). It is common for small firms not to have documented policies and procedures, and practitioners are encouraged to have and maintain these documents irrespective of the size of the firm.

7. Information and communication

Information is needed at all levels of an entity to identify, assess and respond to risks, including emerging risks. Information can be obtained in various forms from various sources, in qualitative or quantitative form. The information obtained allows ERM to respond to changing conditions in real time. Without information around developments in, for example, the legal fraternity, the tax legislation, the basic conditions of employment, the economic conditions, etcetera, the firm may find itself exposed to a number of risks that it did not anticipate. Should you be caught off guard, you may find yourself out of business. Communication should raise awareness about the importance and relevance of effective ERM.

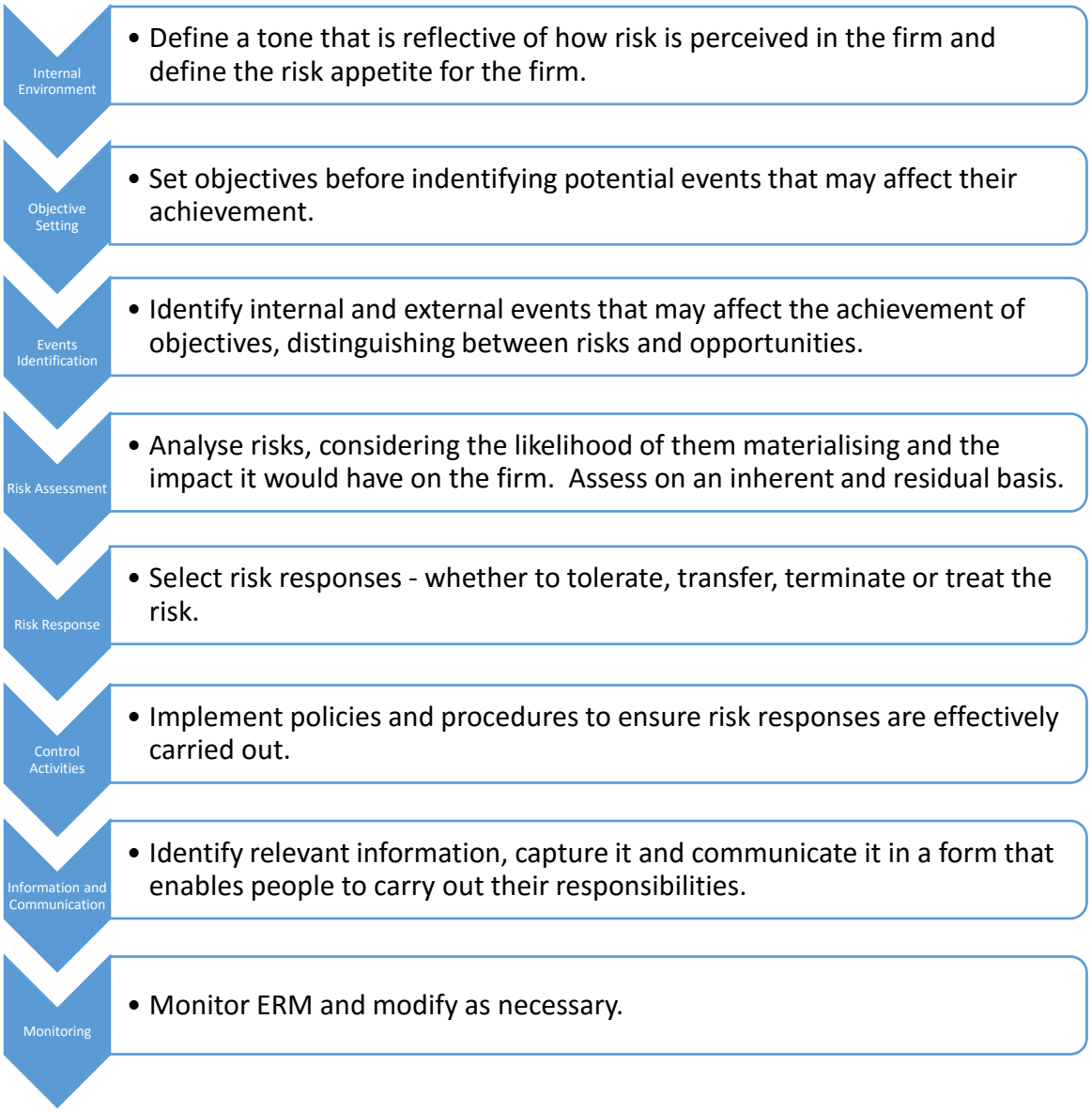
8. Monitoring

Monitoring of ERM involves the assessment of both the presence and effectiveness of its components and the quality of their performance over time. It can take place through ongoing activities or separate evaluations.

An example of a risk that a firm may face could be stakeholder dissatisfaction. The likelihood and impact of this risk for the firm could be catastrophic as it could lead to a collapse of the firm. The risk could be managed by the firm understanding the expectations of its various stakeholders and ensuring that there are measures in place to address these. As a measure, the firm may explore ways to involve some of the stakeholders in the development of the risk management processes and keeping people informed. Putting these measures in place should reduce the residual risk. Ensuring that measures remain effective throughout the life of the firm would further require ongoing monitoring, obtaining feedback and reviewing those measures so as to ensure they remain relevant in managing the risk.

Conclusion

The eight components of ERM are summarised in the diagram below:



The risk identification and assessment activity can happen as often as the firm deems necessary, but it is advisable to conduct it at least on an annual basis. It may be costly, time consuming, frustrating and probably impossible to reverse the damage that may be caused by a problem if it finds you.

So, go on and find the problem before it finds you and enjoy the rewards of that investment.