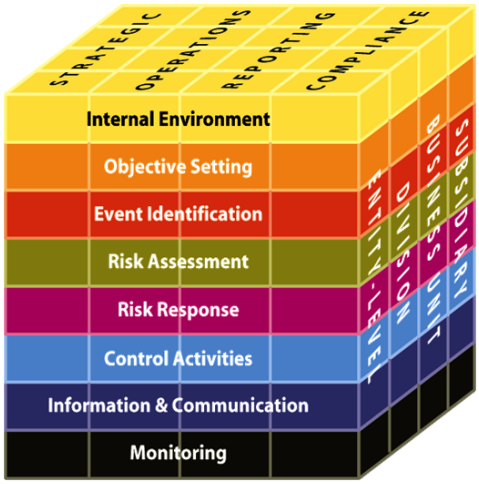
Enterprise Risk Management Process

Last week we explored the minimum capital requirements under Pillar 1 of Basel III. This week, we will focus on the firm-wide risk management process and the role of supervisors, under Pillar 2, to ensure that regulated entities develop and implement adequate risk management practices.



Source: COSO

Enterprise risk management

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) defines enterprise risk management 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of the*

According to COSO, enterprise risk management is:

- "*A process*" - which indicates that it is ongoing and does not have a definitive deadline.
- "*It is effected by an entity's board of directors, management and other personnel*" – enterprise risk management is the responsibility of all employees, although the board of directors has ultimate responsibility for managing and monitoring the key risks impacting the entity. It is important for firms to promote a risk culture and establish a

risk governance structure that clearly delineates the roles and responsibilities of everyone in the organisation. Firms may follow the three lines of defence. The first line of defence is employees and managers, ***the risk owners***. Employees and managers are responsible for identifying, assessing and managing the risks inherent in their day to day activities. The second line of defence is the risk management or ***compliance function*** which is responsible for overseeing risk management within the organisation. The third and final line of defence is ***internal audit***, which is responsible for providing an independent assurance of the effectiveness of the firm's risk management processes and internal controls.

- "*Applied in strategy setting and across the enterprise*" – enterprise risk management applies a holistic approach to risk management rather than a "silo" approach. Traditionally, firms managed risk within respective units or "silos." For example, the Chief Financial Officer would be responsible for assessing and managing financial risks while the Chief Operating Officer would be responsible for managing operational risks. While business units might be better positioned to manage the risks associated with their activities, the "silo" approach suffered from many limitations, such as the non-identification of some risks (especially those external to the organisation) until it was too late, and the adoption of inappropriate risk responses.
- "*Designed to identify events that may affect an entity*" – such events may pose either a threat or an opportunity for the organisation.
- "*Manage risks to be within its risk appetite*" - risk appetite is an integral part of the enterprise risk management process as it articulates the level of risk the organisation is willing to accept in pursuit of its mandate.
- "*Provides reasonable assurance*" – reassurance to management, clients, and regulators that the firm's risk management processes and system of controls are adequate.
- "*Achievement of the entity's objectives*" – the strategic objective of most companies is to create or maintain value for their shareholders. The enterprise risk management process should begin with an understanding of the key drivers of shareholders' value such as revenue growth and operating efficiencies.

Enterprise Risk Management Process

With an understanding of the key drivers of shareholders' value, management is better able to identify those internal and external events that may either threaten the achievement of the organisation's strategic and operational goals or create a viable opportunity for the firm. The goal of enterprise risk management is to capture the full range of risks - whether it be strategic, operational, regulatory, or reporting risks – that may affect the company's success. The earlier these risks are identified, the sooner firms can implement plans to reduce their effects, should they materialise.

Once a risk has been identified then it must be evaluated to determine the likelihood of occurrence and its impact or the anticipated severity of its consequences. Risk events are then prioritised based on the magnitude of their likelihood and impact. Those risks that have a high chance of occurring and a severe impact on the organisation will be prioritised over those that have a very low probability of occurring and a very low impact on the organisation's core objectives. The main reason for prioritising risks is to form a basis for allocating the organisation's limited resources.

Management then determines the most appropriate response for a risk event given the organisation's risk appetite. Risk can either be avoided, reduced, accepted, or transferred to a third party such as an insurance company. When determining the risk response, it is important to consider both responses that will prevent a risk event from occurring and those that will minimise the impact of the event should it occur. The risk response should bring the priority level of a risk within the acceptable limit.

While risk identification, evaluation and response are core elements of the enterprise risk management process, communication and monitoring are also important. Risk information must be captured and communicated in an appropriate form and in a timely manner that would enable persons to respond accordingly. Some firms monitor and produce periodic reports on key risk indicators for executive management and the board of directors.

Enterprise Risk Management within Securities Firms

Risk management is especially important for firms handling clients' monies and assets. Ineffective risk management could lead to firm failure, financial losses for clients, a lack of confidence in the securities sector, and instability in the financial system. Accordingly, the

Trinidad and Tobago Securities and Exchange Commission (TTSEC) has always encouraged its registered entities to develop and maintain risk management practices that are appropriate for their business. Pursuant to By-Law 64(1)(*b*) of the Securities (General) By-Laws, 2015, Registrants (defined under Section 51(1) of the Securities Act, Chapter 83:02 of the Laws of the Republic of Trinidad and Tobago as Broker-Dealers, Investment Advisers and Underwriters) are required to "*establish, maintain and apply a system of controls and supervision sufficient to manage the risks associated with their business in conformity with prudent business practices"*. Such a system should be documented in the form of written policies and procedures. As part of its risk-based supervision, the TTSEC would evaluate the efficacy of these policies and procedures, as well as whether or not Registrants are adhering to them. Enterprise risk management is ever evolving. The TTSEC therefore encourages Registrants to review their risk management practices and update them accordingly.

END

For more information on the securities market and the role and functions of the TTSEC, please visit our corporate website at www.ttsec.org.tt. To become a smart investor, download our IPA via the Google Play and Apple Stores. You can also take the investor education online course on our investor education website, www.InvestUcateTT.com, and test your knowledge in our interactive investing game InvestorQuestTT at www.InvestorQuest-tt.com, and remember, to connect with us via Facebook; Twitter, Instagram, LinkedIn or You Tube.

Published Article – Business Express Newspaper
April 13th, 2022