Good Governance, Risk And Controls

By David Chew, Executive Director, Enterprises Risk Services Practice, Deloitte Singapore

More than a year has come to pass since the introduction of the SGX Listing Rule on the adequacy of internal controls and the 2012 Code of Corporate Governance. A straw poll suggests that most companies did not have difficulties in opining on the adequacy of internal controls over the prescribed risk categories and having a risk governance structure in place. Two common tools that organisations use to facilitate compliance with the risk management and internal control requirements are the enterprise risk management ("ERM") to identify and prioritise risks, and the Control Self-Assessment ("CSA") programme which comprises a bottoms-up controls documentation and assessment, followed by a top-down review and "sign-off".

The traditional ERM as many would call it, presents risks as separate events from a two dimensional points of view. This has been criticised to be overly simplistic given the complexity and the interrelationship of various events. The other criticism is that the process tend to focus on the downside risks, with insufficient consideration on how one could leverage or exploit the upside risks.

CSA approaches range from non-interactive processes, such as the completion of generic control questionnaires by management and staff, through to highly interactive facilitated workshops. CSA programs are widely used to provide continuous assessment of the state of the organisation's internal controls from the effectiveness and compliance perspectives. There are various methodologies to assess control points at the functional or process level and aggregating the CSA results at an enterprise level. There was, however, no common methodology to assess the overall adequacy of internal controls.

The peculiarity about the stock market is that everyone has the same information but interprets the information differently. Likewise, the concept of risk means different things to different people. Without an anchor, discussions around risk could swing from the mundane day-to-day occurrences to the abstract, leaving both the board and management none the wiser.

This paper discusses some techniques to improve the ERM and CSA processes.

"If a tree falls in a forest and no one is around to hear it, does it make a sound?"

The peculiarity about the stock market is that everyone has the same information but interprets the information differently. Likewise, the concept of risk means different things to different people. Without an anchor, discussions around risk could swing from the mundane day-to-day occurrences to the abstract, leaving both the board and management none the wiser.

Losses usually result from a complex confluence of events, which makes it difficult to predict or model. Most risk management processes adopt a taxonomy-based approach. This is a structured and methodological way to get the risk identification and assessment process started. However, rule-based risk management is not able to contemplate the full spectrum of the outcomes of the risk event (or a combination thereof), nor reduce the impact or likelihood of major disasters.

In order to fully understand the risk so as to treat it effectively, it is crucial to establish the context of the risk using scenario analysis. This involves uncovering and understanding the risks which are embedded within the 4P's – strategic plans, programs, projects and products. Scenario analysis based on consideration of major events and their possible outcomes is useful to assess the organisation's resiliency through a chain of events, and to evaluate the organisation's operations as an integral part of a wider eco system. A holistic picture of the organisation's risk profile could be built by careful selection, construction and analysis of scenarios unfolding over a period of time. In addition, with scenarios being articulated in the form of a storyline, there will be greater resonance with key stakeholders, as compared with discussions centred on distributions, tails and other mathematical constructs. Without proper context, one runs the risk of missing the woods for the trees.

"If you can't measure something, you can't manage it."

By attempting to measure risk using a single impact versus likelihood score, the ERM approach could not reflect the nature of uncertainty, which is better presented as a distribution of different outcomes. This approach is further constrained by our inability to visualise a scenario which we have never experienced, plus not many of us are that statistically inclined to be able to comprehend and distinguish situations with varying degrees of probability. Cognitive bias causes us to be overly confident or optimistic about positive events and underestimate the likelihood of negative ones. This very same bias also causes us to over-value evidence which is consistent with a favoured belief and discount those which are against.

Quantitative models are useful in helping to quantify risks, understand observed phenomena, explore the sources and impacts of the risk; and develop the corresponding mitigation plans. When properly used, models reduce bias and subjectivity from risk analysis. However, with the exception of a minority, not many CEOs understand how risk models work, let alone the board. In this context, one has to guard against the inclination of risk models being overly simplified to highlight limited aspects of complex combinations of exposures. Risk measurement is an applied science that makes the best use of data, the underlying assumptions, parameters and imperfections to derive a set of hard numbers. Risk management, on the other hand, is an art which requires experience and intuition to appraise these hard numbers in the context of the infinite permutations of people, process and systems related issues. Neither should be over emphasised at the expense of the other.

In order to fully understand the risk so as to treat it effectively, it is crucial to establish the context of the risk using scenario analysis. This involves uncovering and understanding the risks which are embedded within the 4P's – strategic plans, programs, projects and products.

By attempting to measure risk using a single impact versus likelihood score, the ERM approach could not reflect the nature of uncertainty, which is better presented as a distribution of different outcomes. This approach is further constrained by our inability to visualise a scenario which we have never experienced, plus not many of us are that statistically inclined to be able to comprehend and distinguish situations with varying degrees of probability.

Whither Control Deficiencies?

The original Internal Control – Integrated Framework by The Committee of Sponsoring Organisations of the Treadway Commission ("the COSO Framework") was first introduced in 1992. With the introduction of internal control certification legislation, such as the Sarbanes-Oxley Act of 2002, the COSO Framework has gained international acceptance as the standard for internal controls.

The 2013 update to the COSO Framework addresses stakeholder expectations related to accountability, governance, transparency and the prevention and detection of fraud, all of which should be issues which are close to the heart of the board of directors. The new COSO Framework articulates the management's responsibility for ensuring that each of the components and relevant principles of internal control which have be present and functioning in order to have an effective system of internal control. There is now guidance on the manner and whether major "deficiency" in a component or principle of control could be mitigated. For instance, an ineffective control environment could lead to the conclusion by the auditor that there was a "significant deficiency" or "material weakness". This approach is not new and has been in use to comply with control certification requirements. With the new COSO Framework, however, there is now an opportunity for wider adoption of the "control deficiencies" concept for assessment and mitigation purposes.

The updated framework contains more explicit guidance on the fundamental concepts that better reflect business realities that did not exist when the original framework was created. The transition period to the updated framework is up to December 2014. This would be a good timeframe for the board to set for the management to "upgrade" the CSA programs to be in line with the new framework.

A Brave New World

Major corporate decisions usually involve significant research, deliberation and due diligence. However, it is submitted that cognitive dissonance will cause the decision-makers to overlook any faults or defects relating to the decision. This is where the oversight function of the board will be best served by directors who ask the right questions. In today's volatile market, boards that ask, "What economic or environmental events could affect this initiative?" may uncover a variety of potential market and environmental risks. However, broadening the question to instead ask, "What could possibly go wrong with this initiative?" may identify a wider range of potential value-destroying risks beyond just those created by the market and environment[1].

The graveyard of former greats is littered with those whose swift fall were attributable to failing to appreciate the magnitude and velocity of the risks, compounded by an inflated sense of self-confidence. On the other end, business school case studies are also filled with those whose inactivity and risk adverseness brought about a slow and painful decline. A responsible and forward looking board would not wish for any of these outcomes to happen under their watch. ■

Quantitative models are useful in helping to quantify risks, understand observed phenomena, explore the sources and impacts of the risk; and develop the corresponding mitigation plans. When properly used, models reduce bias and subjectivity from risk analysis.

1 Directors' Alert 2013 published by the Deloitte Global Center for Corporate Governance.