

Issues with the COSO model revisions:

Limited discussions about uncertainty and risks are addressed in the section dealing with “**Provides Reasonable Assurance**” the framework states rightfully that “absolute assurance” acknowledges that limitations exist in all systems of internal control, and that uncertainties and risks may exist, which no one can confidently predict with precision. Absolute assurance is not possible.”

The framework goes further and states that “Reasonable assurance does not imply that an entity will always achieve its objectives.” The framework appears to offer an excuse for the failure of internal controls where collusion occurs and does not appear to address management’s role and responsibility in addressing uncertainty, risk, or the possibility of collusion. Anyone who has sat in on a SAS70 review with management and a public accounting firm where said accountants ask management if fraud occurred and management denies knowledge of fraud understands the lack of substance in these activities. These are significant exposures that COSO avoids to address head first and has led to repeated recurrence of failures and a lack of understanding regarding the role of senior management in executing their responsibility for executing higher level controls that set the tone for risks and uncertainty.

Further, COSO does not adequately address business objectives and the role that internal controls and risk management play in laying the foundational support to help achieve business objectives. There is an implied conflict of interest by the drafters of the COSO framework. The principles that are espoused by COSO do not go far enough to address internal controls nor do they adequately address risks and uncertainty. These gaps are serious oversights in the framework which lessen the credibility of the internal control guidance offered within by risk and compliance practitioners responsible for implementing these steps.

COSO lists three goals in the **Achievement of Objectives** section: Operating Objectives, Reporting Objectives, and Compliance Objectives; however, a fourth objective could be added that reflects the Going Concern goals of financial statement reports. Business Objectives – by including business objectives and the risks and uncertainty associated with achieving the execution of business objectives internal controls are then elevated to the C-suite and board level. It is in the execution of business objectives where excessive risks takes place or uncertain events must be dealt with using tools that internal controls may be inadequate to deal with. COSO should either acknowledge the limitations of effectively dealing with business objectives or develop guidelines that describe the role management must play in taking i) aggressive business objectives; ii) moderate business objectives; or iii) conservative business objectives. Adding categories to business objectives then makes it clear the implied risk taking stance management has chosen. There are a number of ways to create criteria to measure the level of aggressiveness in risk taking therefore there is no reason not to include the intentions of management in regards to it business objectives. During initial public offerings the offering circular will use similar statements of risky positions taken by management. These statements allow shareholders insight into business operations of a firm and why a firm has decided to take a certain stance to achieve its business objectives.

I do note that in the Objectives section a statement is made that “management specifies objectives that have been set so that risks to the achievement of those objectives can be identified and assessed” is a step in the right direction but falls short. The framework does not address the conflict of interests inherent in management’s role to ensure the firm is managed for the benefit of shareholders and not management’s own self interests.

Under the section **Objectives and Sub-Objectives**, the frameworks speaks to “management addresses the linkages or accepts increased risks”; however, the framework is silent on documentation for accepting increased risks, including reporting to the board, shareholders, or other reporting agencies. The disclosure of a more risky stance in business objectives should be considered a material event such as MF Global’s move to increase its exposure to a concentration of risky assets at a ratio of debt to equity that caused the failure of the firm. It’s important to note that PwC signed off on its internal controls attesting to the no material weaknesses in “controls” when in fact MF Global’s control environment had been materially weakened.

Under the five principles of **Control Environment** the COSO control environment does not include in its principles any mention of risks or uncertainty. Both the board and management are responsible for setting the right tone yet apparently the tone does not include a view of its risk stance to achieve its business objectives. I would posit that shareholders and the public would benefit in knowing whether management believes that an increase in risk is appropriate to achieve its stated business goals and objectives in order to evaluate whether ownership in these entities is justified given the risk tolerance of the “owners” of the firm. In fact, there appears to be very large gaps in recognizing the ownership of the firm and disclosures that inform ownership of the risk positions taken by the actors responsible for carrying out the strategy of the firm. It is only after the fact that risky strategic changes resulted in the failure of certain firms.

Under the section **Risk Assessment**, the COSO framework gives very light treatment to the area of risk assessment. While it is improper for COSO to provide prescriptive guidance on the types of risk assessments management decides to undertake there is no clear accountability established in the principle of risk assessment or the assignment of disclosure responsibility when changes in risk positions occur. The control framework is silent on establishing risk postures and the role of the board and management in authorizing and approving changes in the risk posture of the firm. Shareholders and outside public entities should be able to judge the relative changes in risk at a firm through some measure of the risk posture a firm decides to take. This position does not advocate that shareholders should be able to vote on the direction the firm may be taking but disclosure allows shareholders the opportunity to decide if the risk posture taken by management is consistent with the owners risk tolerance. Shareholders may decide to sell its position or advocate for less risk exposure either way the decision by management is brought to light and is no longer hidden in the dark until a Black Swan event exposes faulty decision making at the firm.

As a suggestion, under the section **Information and Communication**, none of the principles discusses the disclosure of changes in risk posture or to whom the Communications are made. I would strongly

suggest that consideration be given to more robust information and communications disclosures with respect to risk.

The COSO framework does not fully address the top-level controls environment. Just as Congress has established *separation of powers* it may now be advisable to firms to implement similar top level controls to avoid or eliminate concentrations of power in corporate suites. There are two levels of power in all publicly and some privately owned corporations. The board and management (as there are Executive and Legislative branches of government) represent the current two branches of power. The addition of a third branch of power should include an independent group responsible for advising, not deciding, the level of risk that a firm should take in major departures from stated business objectives. Management and board may override this third branch of power however the firm should be required to document its decision for doing so along with justifications to taking a more aggressive risk posture is warranted.

Conclusion

The overriding objection that I have with the COSO framework is that the framework is positioned to address audit risks primarily and does not sufficiently address Enterprise Risk Management while it gives the appearance of a remedy for addressing Enterprise Risks. I view Enterprise Risk much more broadly than the treatment of internal controls and the reduction of audit risk. Unfortunately, because of a lack of independence in the framers of the COSO framework and the dependence by management on public accounting firms to execute and implement an internal controls framework; the conflict of interest is pervasive in that each firm then hires the same said public accounting firms to attest to internal controls which the accounting industry has formulated to its own benefit.

In doing so, COSO is not able to address the root cause of weak internal controls and the inherent industry conflicts continue unabated. The need for a truly independent, risk based set of standards is needed. Unfortunately, I acknowledge that the risk management community has not organized itself into a credible body that is recognized by Federal agencies which could then oversee risk standards across all highly regulated industries. COSO is a compromised attempt at addressing risk management where it is wholly unqualified to address nor sufficiently independent to credibly advise management.