McGladrey

Internal Controls – COSO Revisited
Q&A Responses

- You keep saying COSO is the standard in the United States. Is there another standard applicable to international audits and controls?
  - Currently in the U.S., the only standard internal control framework is the COSO model. The COSO model is also used by companies/organizations around the world, but there are other models that have been published, such as:
    - CoCo - Canada
    - Cadbury – UK

- What would be the incentive for having not-for-profit organizations adapt COSO?
  - Management is responsible for establishing appropriate controls for their organization based on size, complexity and other factors. Controls are put into place to either prevent errors or fraud or to detect them timely within the normal course of business. Use of the COSO model should improve management's control structure, thereby, reducing the risk of control failure. However, control risk can never be zero but it can be minimized in a well designed system.

- Can you include internal audit function as an important function in this process?
  - Certainly. Internal audit fits under the "Monitor" element of the COSO model. However, cost/benefit considerations call for a certain critical mass (revenue size) before it makes sense for an organization to develop in internal audit function.

- Before you adopt the COSO model, does the organization have to go through enterprise risk management (ERM) at the entity level?
  - Not necessarily under the current or revised model. The COSO-ERM document is a very robust model and organizations at some point in their evolution should consider its concepts, but the integrated framework of COSO for "normal" controls is ready for implementation without such an exercise. Perhaps you are thinking of the "Risk Assessment" element of COSO. I would agree that a well thought out risk assessment is absolutely necessary when designing control activities (and other COSO elements) for an organization.

- How important is having documented / repeatable processes and procedures as it relates to internal controls.
  - Very important. Documented control activities get everyone on the same page and helps ensure consistent application of procedures. Organizations that rely on corporate memory in a key employee's head run a large risk of control risk once that employee is no longer in the organization.

- What resources are there to help a small organization to do the risk assessment and internal control review?
  - The new exposure draft of COSO provides guidance for smaller organizations. In addition, COSO published a document for "small public companies" in 2006. The guidance contained on that document is also valuable for smaller entities of any type (public, private, or non-profit). Both documents can be found on the COSO website (www.coso.org).

- Is there a checklist or questionnaire available with these 17 principles that we could use?
  - Please refer to the AICPA's white paper on the new COSO model

    http://www.aicpa.org/interestareas/frc/auditattest/downloadabledocuments/coso/coso-2012_whitepaper.pdf

McGladrey

Internal Controls – COSO Revisited
Q&A Responses

- It says one of the concerns is "checklist mentality." Why is this a concern? It seems that a checklist would be a good resource for NFPs to use to ensure they are covering all areas.
    - I love checklists and studies have shown that they are very valuable in all sorts of professions (pilots, doctors and even accountants), but the concern being raised is that the new 17 principles will be interpreted as all that an organization needs to do to be fully COSO compliant when in fact it could only be a tip of an iceberg.

- What is ERM?
    - "Enterprise Risk Management" Follow this link for more information on the COSO-ERM model:

      http://www.coso.org/-ERM.htm

- Is there any governing body overseeing NFPs that require specific financial roles be employed or contracted by an NFP? I have a potential client that is trying to rely on existing controls and not hire a Controller to review their accounting department. I don't recommend that direction but not sure there is a requirement anywhere that would prevent them from doing so.
    - I am not aware of any. The NFP sector has been very loud and clear that it can self regulate its affairs and does not need an outside body to dictate which policies it should and should not have. Some states (such as California) have nonprofit statutes that govern audit committee structure, audit requirements, etc. but there is none currently at the Federal level. One could argue that the new Form 990 is trying to change behavior by peer pressure, but it does not mandate that certain governance practices be used. In your specific situation, it sounds like they may have a control environment issue (tone at the top) and may not recognize the importance of control design and monitoring. While this may be disappointing and not a best practice, it may not be illegal. I am not a lawyer so I really cannot comment on any exposure senior management or the board may have if this case calls into question their fiduciary duty.

- Any recommendation on how to move away from "case by case" travel policies?
    - Yes – develop and document a formal travel policy for the organization. A consistent approach to travel and have it communicated (and enforced) is a sign of a good control environment and helps prevents "misinterpretations" that are discovered after the fact.