

**From:** Mary [REDACTED]  
**Sent:** Tuesday, October 15, 2013 8:22 AM  
**To:** GreenBook  
**Cc:** [REDACTED]  
**Subject:** comments on exposure draft

I have reviewed the exposure draft on the proposed new standards on internal control for the Federal Government. As I am an instructor of this material and have worked extensively implementing both operational and financial controls since passage of the Sarbanes Oxley bill, I believe it is extremely important to be able to easily inform interested parties on the implementation of controls as well as be more realistic than theoretical with regard to the implementation of control systems within the Federal Government. My comments are below:

1. **While COSO inverted its cube, placing the Control Environment standard on the top, I would ask GAO to retain its former structure placing the Control Environment as the foundation of the program.** Here is why: COSO corporations are governed by a board of directors which are independent of and in control of management. Such is not the case in government. In most cases, management is politically appointed and is responsible for the success of the mission of the organization. Unless the legislative branch assumes oversight of organizational management in its role of “checks and balances,” management, in its current structure, will appoint the oversight body and have control over it. In government, the control environment sets the tone within all levels of the organization – it sets the tone for all other standards. Without a foundation of a strong control environment, risk assessments will not be adequate; without adequate risk assessments, adequate control activities will not be established, and so on. Without the strong foundation, the remaining standards will crumble.
2. 03.01 requires implementation of all attributes and principles; however, this **conflicts with the flexibility** provision expressed in para 02.06.
3. 03.09 should be required only if applicable – again, in conflict with 02.06.
4. 1.09: Management is ultimately responsible and appoints the oversight body. This para infers that the oversight body has authority above management’s authority, which is the case in the corporate world, but not in a politically run government environment.
5. 2.02a: The need to include mission-related key personnel on the oversight body should be mentioned in this attribute, even though it is included in supporting paragraphs. Key operational personnel support is critical to the success of an internal control program.
6. 2.03: same as above note
7. 3.07: Please clearly refer to the internal control objectives of efficiency and effectiveness of operations, reliable reporting, and compliance with laws and regulations. Those responsible for implementing internal control programs need good, clear, concise directions that they can refer to when assessing controls.
8. 4.11: Succession planning for permanent replacement is very difficult to do in the government setting; however, this is a very good recommendation for contingency operational planning. In cases of emergency, there should be succession plans (which would require cross-training as well as good communication and information techniques); but this should not be an attribute required for permanent succession planning. It is not realistic.
9. 5.05: The oversight cannot hold management accountable. It can recommend, but has no authority over management. The internal control program is a management-responsibility program.
10. 5.05: The term “adjust pressures on personnel” gives management authority to apply pressure, which may not result in a healthy climate or result. Suggest the term be reworded toward “providing direction” or “emphasis.”
11. 5.11: Replace “adjust” with “mitigate” or “reduce.”
12. 7.09: Again, problems with the oversight body authority – The oversight body may oversee but what recourse does it have when management is ultimately responsible. Within the Federal Government, the oversight body makes recommendations to management which either management either accepts or rejects.
13. 7.12: Not a good definition of “avoidance.” One may avoid the risk by moving operations to another location. Operations may not be causing the risk, but may be most vulnerable.

14. 8.10: Same situation as previously expressed: How can an oversight body, appointed by management, oversee management's ability to override controls. This is usually exposed during the use of GAO's management evaluation tool, if it is presented as a climate survey, and can then be presented to management as a climate observation.
15. 9.04: last sentence: confusing: Is change critical to an effective control system? Or, does the existence of change increase the possibility of new, unidentified risk?
16. 11.06: Please add "Restricted Access" to IT objectives. This objective is broad in scope and can be used at all levels of the IT environment, but when listed as an objective, it becomes more visible and its presence as an objective will effect more attention during the risk assessment and control activity design and implementation stages.
17. 12.02a: Please add personal responsibility, perhaps by position. As written, it is too vague to hold positions responsible.
18. 12.04: also vague: Does each unit establish and maintain IAW entity-level objectives or carry out direction from higher levels?
19. 12.04: Include in elements of written policy: Notification procedures for reporting an identified control gap or failure (deficiency).
20. Information and Communication Overview: Need to emphasize communication need up, down, and across the organization. (The old graphic depicted this well.)
21. 14.07: Unless responsibility structure is changes within government, the oversight body presents quality information to management. Management does not present to the oversight body.
22. Monitoring Overview: Delete "finally" – infers arduous program. Also, delete "quality of performance over time." The value of control activities and their success of achievement is what should be monitored.
23. Complete Corrective Actions: Include making resources available for remediation.
24. Glossary: Management: include with activities "process," and delete "all" before activities. Also, add "directing and staffing."
25. Glossary: Oversight body: change the definition to reflect reality in government environment; get away from ivory tower theoretics.  
This definition is similar to PHD business professor, who has spent his entire career teaching on campus and never working in a business environment, writing an Introduction to Business textbook. He has no sense of what is really happening out there.

I would be happy to discuss my comments with you.

Mary Braun

