Comments on 2013 Exposure Draft – Standards for Internal Control in the Federal Government

Three of the suggested reviewer questions in the draft ask if particular aspects of the standards are "clear, understandable, and adequate." The comments that follow address this concern by focusing on the definitions of terms in the Glossary. Because those definitions refer the reader to the body of the draft, I hope that any thoughts below that you find useful will help in both locations of the draft.

To convince federal program managers that they should strengthen internal controls, auditors must use clear, understandable, and convincing arguments. The Green Book along with OMB Circular A-123 – "Management's Responsibility for Internal Control" and department or agency-level internal control guidance are among the sources (or tools) that federal auditors use. To win over the program managers who are often the recipients of audit report recommendations, auditors need to get the message across that effective internal controls are an integral part of managing programs and achieving results. As the Yellow Book also points out in paragraph 6.15c, they serve as a defense in safeguarding assets and in preventing and detecting errors; fraud; noncompliance; or abuse. Without a meeting of the minds, some managers may think of internal controls as a foreign language that must be translated during an annual FMFIA "paperwork exercise." The underlying premise for my comments is that the Green Book should be as clear and compelling a publication as possible even though it is all about a seemingly dry subject.

Consider the term "control activities." The word "activities" implies actions of some sort. But the definition explains this as "policies, procedures, techniques, and mechanisms." How about "control structure" instead? The control structure is composed of the "policies, procedures, and mechanisms" that are part of the program design. Then a separate term and definition might be in order for "control activities." Those might include human behavior and computer-generated actions (resulting from human-produced code). For example, COSO's Executive Summary uses the word "actions" when it defines control activities as "…the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out."

Clarifying other terms in the Glossary would make it easier to get key points across. Using plain English as much as possible can help all involved. The Plain Writing Act of 2010 requires the federal government to write all new publications, forms, and publicly distributed documents in a "clear, concise, well-organized" manner that follows the best practices of plain language writing.[1] The term `plain writing' means writing that the intended audience can readily understand and use because that writing is clear, concise,

[1] See http://centerforplainlanguage.org/resources/plain-writing-laws/plain-writing-act-of-2010/

well-organized, and follows other best practices of plain writing. Although the Green Book is not covered by the Act's requirements as I understand it, the more it adheres to best practices, the better tool it will be for auditors and managers.

- Application material – used also in paragraph O2.07. This phrase sounds technical and is unclear. If it simply means additional helpful information for applying the concepts, then stating it directly would make the point clearer.
- Baseline. In this instance, the word is clear but the definition clouds the meaning. Why not just define this as the starting point for judging changes in internal control over time? The current definition would be easier to grasp if it was shorter and used fewer prepositions.
- Complementary user entity controls. This definition is rather long and is difficult to follow.
- Contingency plans. This definition refers to sudden personnel changes impacting the organization. Consider mentioning other significant changes such as physical disasters and government shut-downs.
- Deficiency. Suggest changing the order of the points in the definition. When a control does not work to achieve control objectives (or address the related risks), it is due to a deficiency in the control's design or implementation. The phrase "in the normal course of performing their assigned functions" could be implied. Cutting it out would make the definition less cumbersome.
- Defective control. This definition is confusing because it is too long. Please consider breaking the ideas into separate, simpler sentences.
- Entity-level control. This is another rather long sentence. Please divide it into two or more sentence to be clear—it's an important concept.
- Fraud. This is a good example of a simple and clear definition.
- General control activities. The definition refers to information system controls. It would be clearer if you put that up front as part of the term you're defining. What about something like Information System: General Control Activities?
- Inherent risk. This definition proposes only two possibilities: (1) inherent (uncontrolled) risk which exists in the absence of management doing anything; and (2) controlled risk after management responds to the inherent risk. Though I "get" it, it sounds too simple. First, I see no reason why the response shouldn't also be expected from all levels of the entity--from line employees, staff office employees, all the way up to executives and the oversight board. The responsibility for ensuring that internal controls are adequate should be a shared concern, not just a management concern. Second, it might be useful to recognize that inherent risk may come from multiple sources. For example, inherent risk may be (1) external and come with the "territory" of the function (e.g., homeland security may have inherent risk even after management's response); (2) built into the entity's environment (e.g., information technology may become so complex that it retains inherent risk after management's

response); or (3) dynamic, changing business risk for which management cannot fully plan, as in some NASA missions.

- Internal control. In addition to plans, methods, policies and procedures, would operational processes be considered a separate component? The Yellow Book includes them in its overall definition in paragraph 2.11c:

  > "Internal control comprises the plans, policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal control includes the processes and procedures for planning, organizing, directing, and controlling program operations, and management's system for measuring, reporting, and monitoring program performance."

- Internal control system. This may be the most important definition. I suggest using "implemented" as a clearer, more common verb than "effected." COSO does use the second verb, but when I read it in the Green Book for the first time, I though the authors meant "affected." Also, the overall definition would be more tangible if it was shorter. Perhaps using more than one sentence would help.
- Key role. This definition is unclear. How about something closer to: Key roles for ensuring the entity has an effective internal control system are held by senior managers. These key roles are built into the organizational structure and specific positions as part of the internal control structure.
- Organizational structure. This definition should not include "organizational processes." The organizational structure should be what you can draw in an organizational chart. Processes are part of the internal control structure.
- Oversight body. This is responsible for overseeing the entity's operations, not just the internal control system. How about "Those responsible for overseeing the entity, including design, implementation, and operation of an internal control system."?
- Performance measures. I suggest adding a footnote in the Glossary or paragraph 6.09 referring the reader to GPRA and explaining that some of the internal control performance measures may serve as performance measures for GPRA also. And, consider also noting that GPRA requires by law a structure for strategic plans, annual plans, and related performance measures.
- Policies. This definition differs from commonly used definitions of policies with which auditors and program managers would be familiar. Is the draft definition implying that policies can be more useful and help managers get their programs to work better by including the components listed? If so, then saying that directly would be helpful.

[Submitted to greenbook@gao.gov by Bram Hass 1-14-14]