

#41

Document Title:		Comments to the GAO's Standards for Internal Control in the Federal Government (Green Book)		
Agency		Department of the Interior (Summary of comments from Bureaus and Offices)		
Point of Contact (Name)		Eric Eisenstein [REDACTED]		
#	Page	Section	Comment	Recommendation
1	All	General Observation	Throughout the exposure draft, the first item in each section starting after the attributes is identical and redundant in the second item (as though the writer intends to summarize the first item then uses the exact verbiage from the first item, then expands minimally in the second item.) This appears redundant throughout. (E.g., Principle 6 - Define Objectives and Risk Tolerances. First sentence in 6.03 is the exact first sentence in 6.04. Same with Principle 7; first sentence in 7.07 is the exact first sentence in 7.08, etc.)	Recommend removing redundancies.
2	iii	Enclosure I: Summary of Major Changes	Addition of 17 principles adds at least one level of direction/requirements for management. There is a possibility that adding another level of requirements compromises the flexibility of entities to design their internal control programs. This is especially difficult in the current environment of budget and funding challenges.	Recommend adding language to ensure entities maintain flexibility to design internal control programs using resources efficiently and effectively.
3	10	Objectives of an Entity O2.15	Circular A-123 considers external audits and reviews part of the internal control process, and guidance has been that it is not necessary for organizations to review internally the same program/processes that had been reviewed externally, and in fact, doing so could be an unnecessary use of resources	Recommend adding language that an internal review may not be necessary if an external review has taken place.
4	20	Control Environment, Principle 1	"Set Tone at the Top" - Do not believe the oversight body should be addressed in this section, only management.	Recommend removing reference to oversight body from 1.03, 1.04 and 1.05.
5	22	Compliance Objectives O2.22	Revise the sentence, 'In the government sector, objectives related to compliance with applicable laws and regulations can be more significant than in the private sector.' This sentence suggests that private sector organizations do not value legal or regulatory compliance and do not structure their organizations to achieve compliance. While laws do not prescribe a private organization's mission, legal compliance would certainly be one of the private organization's objectives/concerns.	Recommend the sentence to read, 'In the government sector, missions, strategic plans, and objectives are derived from the organic acts or other laws and regulations that established the purpose and authorities of those organizations.....'
6	23	Control Environment, Principle 2	Principle 2, Establish Oversight Structure, should be at the start of this section so the reader understands who the oversight body is. Otherwise, the reader speculates who is being referred to as "the oversight body"--External Auditors, OIG, Senior Management Council, or the Senior Assessment Team.	Recommend Establish Oversight Structure be moved to the start of the Control Environment section (that begins on p. 19)
7	23	2.05 and 2.06		Reformat headings to be included as part of the specific paragraphs as follows: 2.05 Responsibilities of an Oversight Body – When the oversight structure of an entity... 2.06 Qualifications for the Oversight Body – In selecting numbers for the oversight body...

#41

#	Page	Section	Comment	Recommendation
8	25			Rephrase title, Provide Oversight for the System of Internal Control, <u>to</u> Provide Oversight for the Internal Control System
9	33	5.09, 5.10 and 5.11	This is an excellent management principle. However, in current environment of sequestration and other budget challenges, more language should be included to support management in allocating resources (personnel) to prioritize internal control needs.	Recommend including language which encourages management to allocate resources to prioritize internal control needs.
10	37			Add "s" to the word "Risk" in the heading, Principle 7 – Identify, Analyze, and Respond to Risk at bottom of page 37 to be consistent with the statement in paragraph 7.01.
11	39	7.10	If the Green Book is going to add additional layers of specific requirements, it should also provide specific guidance for developing risk analysis methodologies and tools.	Recommend providing guidance for developing risk analysis methodologies and tools.
12	9, 19, 34, 45, 60 and 68			<b>Delete</b> the word "activities" from the 5 <sup>th</sup> component "Monitoring activities" of the cube (pages 9, 19, 34, 45, 60 and 68) to be consistent with the category "Monitoring" of the 5 components of internal control on page 6.
13	69			Reverse the order of the words, document and evaluate under paragraph 16.02c., to evaluate and document, to be consistent with statement found on page 71, under paragraph 16.12 and 16.13.
14	75-78	Glossary	Provide most relevant paragraphs to terms found in Overview Section.	<b>Change From:</b> Application material – Additional information that provides further explanation of the principle and attribute requirements of internal control (Overview: Components, Principles and Attributes). <b>To:</b> Application material – Additional information that provides further explanation of the principle and attribute requirements of internal control (Overview: Components, Principles and Attributes, paragraph O2.07). Similarly add relevant paragraphs to other terms in Glossary without paragraphs.

Responses to some GAO Questions

Questions		Responses
Question 1	Is the hierarchy of components, principles, and attributes clearly explained?	<p><b>No.</b> The hierarchy is unclear. For example the 5 principles on pages 20-33 – under Attributes, paragraphs a, b, and c are clearly subordinate to the attribute. But the numbering scheme under each attribute is not clear. 1.03 through 1.07 implies a successor to 1.02 rather than being subordinate to the first attribute. Recommend a different nomenclature such as A, B, C, D, E or i, ii, iii, iv, The nomenclature series should be repeated after each attribute. 3.03 page is a repeat of the attribute language rather than expanding on the attribute like the other attributes.</p> <p>The hierarchy of components, principles, and attributes are not clearly explained which made the exposure draft hard to read and follow.</p>
Question 2	Are there any internal control concepts unique to the government environment that should be in the Green Book that are not currently included?	The exposure draft does not mention proprietary & budgetary accounting interactions, including the budgetary SGL accounts.
Question 3	Does the framework provide the necessary information to allow program managers to evaluate the internal controls for their programs?	<b>No.</b> The definition of an effective internal control system in the GAO guidance is not clear and concise.
Question 4	Does the Green Book provide adequate criteria for auditors?	<p>In the updated Internal Control – Integrated Framework issued by COSO in 2013, new definitions and terminology were established, which will become the new standard for the accounting and auditing industry to follow. At a minimum, the Green Book should be consistent with COSO in the definition of internal control and the identification of the 17 principles and related points of focus. This will provide criteria that the auditors are familiar with when testing internal control and ease the transition.</p> <p>A. The "Requirements for Effective Internal Control" in the GAO exposure draft should be made consistent with the updated COSO Internal Control - Integrated Framework.</p> <ul style="list-style-type: none"> <li>• COSO requires all principles and components to be present and functioning in order for the internal control system to be considered effective and states that the associated component cannot be considered present and functioning if a relevant principle is not present and functioning. GAO does not include this information in the exposure draft. Instead, the term effectively "designed, implemented, and operating" are used.</li> <li>• COSO explicitly states that "An effective system of internal control provides reasonable assurance of achievement of an entity's objectives...An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective relating to one, two, or all three categories". GAO does not mention reducing risk to an acceptable level in the exposure draft.</li> </ul> <p>B. The "Attributes" in the GAO exposure draft should be made consistent with the "Points of Focus" in the updated COSO Internal Control - Integrated Framework.</p> <ul style="list-style-type: none"> <li>• Existence of the "attributes" is required by GAO when COSO does not require the "points of focus" to be present and functioning.</li> <li>• COSO acknowledges that the "points of focus" are examples, not requirements, and are not all inclusive.</li> <li>• Key "points of focus" are not included in the GAO standards.</li> </ul>

Questions		Responses
Question 8	Are the documentation requirements included in the Green Book clear, understandable, and adequate?	Examples of the types and extent of documentation to be maintained would be helpful.
		<p><b>Yes.</b> 1. Specific to Principle 11 - Design Activities for the Information System, this section did not include a significant threat. Paragraph 11.17 provides that internal threats come from former and disgruntled employees. Current research indicates that the major internal threat to information systems comes from current employees that may not be disgruntled. An example of this type of threat is an employee inadvertently transmitting privacy information in a non-secure environment. This could have been because the employee did not understand the requirement for securing privacy information or because the employee thought the transmission environment was secure and authorized for the type of information. There are many other examples of well-meaning employees working in an insecure manner and not knowing the threat they are creating. The cure for this is a well developed and functioning information security education program.</p> <p>2. Somewhere between Principles 5 and 6, the Green Book should discuss: The need to assess the status of the risk management system in the organization, and the need to inventory an organization's assets (the things that it values/those that are critical to the mission). It goes right into objectives, but does not describe a process through which management conducts an asset inventory and then determines the relative value of each asset. The organization cannot determine what the risk tolerance or acceptance level is for a thing if it does not know how important that thing or concept is to the mission in comparison to other things.</p> <p>3. Somewhere following the Monitoring section in the Green Book, GAO should discuss the need to maintain and improve the risk management process (to determine whether the current methodology still meets the needs of the organization).</p> <p>4. As a general recommendation, suggestion that the Green Book incorporate some concepts from the ISO (international standard) 31000 Enterprise Risk Management.</p>
Question 9	Is there a need for additional internal control implementation guidance? If so, what form should it take?	<p><b>Yes.</b> There is a need for additional guidance. However, adequate guidance for implementation of internal control systems is available from the AICPA and other organizations.</p>
Question 10	Is this Green Book written in such a way to allow state, local, and quasi-governmental entities, as well as not-for-profit organizations, to adapt it for their own use?	<p>Is it the intent of GAO and/or OMB to provide specifics as to the applicability to everyday operations? If not, how should the agencies use this new framework? What should agencies do differently in light of the new framework?</p> <p>In order for other entities to adapt the Green Book for their own use, it should be more consistent with the COSO Internal Control – Integrated Framework.</p>