HHS OIG 2013 Green Book Comments

1. Is the hierarchy of components, principles, and attributes clearly explained?

   The hierarchy is explained. However, the new internal control standards introduce many new concepts and terms, so a simplifying graphic would greatly assist users in making connections among them. To display them all (from categories to attributes) on a single page is not possible with a readable font, but a workable alternative is to show the three categories/overarching objectives of internal control (i.e., operations, reporting, compliance), followed by the five internal control components and the 17 associated principles. A note at the bottom of the graphic can refer users to the text of the Green Book to understand how the many internal control *attributes* function within this framework. See enclosed example, in PowerPoint.

   Note that this example not only shows the inter-relationships among the terms/concepts, but also re-emphasizes the fundamental purpose of internal control, which is to provide *reasonable assurance* that operations are effective and efficient, reports are reliable, and the entity complies with laws and regulations. The example also helps users to better understand how the many COSO internal control 'cubes' in the Green Book relate to the text.

   Although page 8 of the Green Book offers a text box showing the components and principles, it does not tie those concepts back to the categories of internal control and the concept of reasonable assurance. The text box is also very small, underplaying its importance.

2. Are there any internal control concepts unique to the government environment that should be in the Green Book that are not currently included?

   Yes. As written, paragraph 01.01 is vague about the purpose of internal controls, introduces two critical concepts without defining them (reasonable assurance and risk), and does not explain "overlapping" quite accurately. These are highly important concepts to understand from the outset.

   The three categories of control – effectiveness, reporting, compliance – are explained only as categories rather than as overarching objectives. This can lead readers to misunderstand that when designing or operating internal controls, those purposes *must* be served. The 1999 Green Book and OMB Circular A-123 made this very clear. For example, the 1999 Green Book defined internal control as "An integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

   - effectiveness and efficiency of operations
   - reliability of financial reporting, and
   - compliance with laws and regulations."

OMB Circular A-123 restated these objectives, and both documents (Green Book and A-123) made clear that the reliability of reports applied to non-financial information, not just to financial. Written this way, users clearly understood what internal controls were, how they applied to an organization, and the standard of effectiveness (reasonable assurance).

Reasonable assurance and risk: Though explained later in the Green Book, these terms should be explained when introduced because they are critical to understanding the internal control standards. (The glossary offers a brief explanation, but it is not referenced on p. 1.) Footnotes are probably best here because users can literally stay on the same page when reading the standards and not interrupt their grasp of the material.

"Overlapping" controls: An entity may design or operate a control in a way that satisfies more than one of the three objectives of internal control (effective & efficient operations, reliable reports, compliance with laws and regulations). The current text is unclear about this and incorrectly states that the objectives are overlapping categories. In fact they are distinctly different. What *can* be "overlapping" is a particular internal control. Through efficiency or ingenuity, it is possible to design and/or implement one control that achieves two or more of the overarching internal control objectives (i.e., categories). This 'dual approach' occurs in design or implementation, not in conceptualization.

Recommended Rewording:

Page 1, para. 01.01: "Internal controls exist to provide reasonable assurance[1] that: (1) operations are effective and efficient, (2) internal and external reports, whether financial or programmatic, are reliable, and (3) the entity complies with laws and regulations. These are the fundamental purposes of internal control. An entity must have objectives that satisfy these purposes, and those objectives will vary by the mission and goals of the agency. The objectives must be sufficiently clear to identify and assess risks[2] to their achievement."

---

[1] Reasonable assurance is a high degree of confidence. It is not absolute because there are events beyond management's control that could . . .? The concept recognizes that . . . ? [Some explanation along these lines would be clarifying. The AICPA standards are possibly helpful here. It would also be helpful to explain the link between the range of acceptable performance for an objective and the amount of control necessary to obtain reasonable assurance of achieving it. To use an abstract example, if 80% is the minimum necessary "score," then management needs controls that provide reasonable assurance of attaining *that* score and not some other (50% would be too low, and 100% would be burdensome and costly).]

[2] Risk is the possibility that an event will occur and adversely affect achievement of an objective. Risks inhere with the creation of an objective, as there are always events (existing and potential) that can thwart objective achievement. Management must identify those risks and mitigate them to a low level of occurrence or impact so that objectives are achieved. The relationships that objectives bear to reasonable assurance and to risk are critical for users to understand. For risks particularly, this is probably why COSO said objectives must be expressed with enough clarity to identify and assess risks. QUESTION: Can the Green Book say something like this? Even if footnoted on p. 1 and explained more fully in the text later, it would be extremely helpful. GAO has used detailed footnotes before, such as in explaining the COSO components of internal control in previous GAGAS editions.

Page 1, para. 01.02: "A particular internal control of an entity may satisfy one or more of the three purposes specified in paragraph 01.01."

Note: The above suggested re-wording maintains the clarity of the 1999 Green Book about the overarching objectives of internal control, identifies reasonable assurance as the performance standard, ties risks to objectives, reaffirms the (COSO) 'clarity standard' for those objectives, and states that a particular control may possibly satisfy more than one control objective. Ideally this will be done in the opening paragraph.

3. Does the framework provide the necessary information to allow program managers to evaluate the internal controls for their programs?

   Not entirely. An objective, practical method is needed to evaluate whether an internal control provides reasonable assurance. Financial statement auditing standards refer to the risk of material misstatement. But most government audits uses GAGAS performance standards, and performance brings a range of other factors to bear. Recommended factors to consider are materiality, significance of objective or program, whether reports are internal or external, reliance on information by decisionmakers, significant requirements in law/regulation, and presence of all five components of internal control. These examples can be elaborated upon, as needed (e.g., by adding 'sensitivity' to the significance factor). See example chart below:

Factor	Tolerance for error or omission	Degree of control necessary to achieve reasonable assurance
Materiality	Higher – small dollar accounts Lower – high dollar accounts	Lesser – small dollar accounts Greater – high dollar accounts
Reporting	Higher – internal reports (within the agency or operating division of an Executive Department) Lower – external reports (to Executive Department-level officials of the agency, Congress, OMB, the public)	Lesser-internal reports Greater-external reports
Significance of objectives (key or mission critical	Higher-less significant	Lesser—less significant

objectives of program; whether program is major or minor)	objectives Lower – more significant objectives	objectives Greater – more significant objectives
Reliance on information by agency decisionmakers	Lower – significant reliance by senior decisionmakers Higher – low level reliance by lower management	Greater – significant reliance Lesser – low level reliance by lower management
Significant compliance requirements in law/regulation	Lower – significant requirements Higher – less significant requirements	Greater – significant requirements Lesser – less significant requirements
Missing components of internal control	Higher – for a less significant operation or program Lower – for a more significant operation or program	Lesser – less significant operation or program Greater – more significant operation or program

Generally, for a given level of assurance, greater error/omission can be tolerated for: (1) non-material amounts or accounts, (2) internal reports, (3) less significant programs and objectives, (4) information not used by high level decisionmakers, and (5) less significant legal or regulatory requirements. Reasonable assurance is also more difficult to attain when one or more of the five internal control components is not in evidence.

In summary, the determination of reasonable assurance requires an honest appraisal of the objectives and controls, with the recognition of what would cause failure yet still enable acceptable performance.

4. Does the Green Book provide adequate criteria for auditors?

Not entirely. On page 6, paragraph 02.06 states that management determines when "a principle or attribute in not relevant for the entity to achieve its objectives and address related risks. . ." While this is true for the operation of a program, it leaves management with final say on the application of principles and attributes. That can lead to an impasse when management and auditors disagree about a finding or recommendation.

Also, the word "must" appears also to be missing from this paragraph in the sentence: "If management decides a principle or attribute is not relevant, management supports **[do you**

mean 'must support'?] that determination with documentation that includes the rationale of how, in the absence of that principle or attribute, the associated component could be designed, implemented, and operated effectively." Finally, what does "associated component" mean in that sentence, and why use the term "could," since it allows management to satisfy internal control standards by writing about what is possible rather than what is actual?

Recommended rewording: "If management decides a principle or attribute is not relevant, then management must document how, in the absence of applying that principle or attribute, the objectives of internal control – effective and efficient operations, reliable reports, and compliance with laws and regulations – are achieved."

5. Are the requirements for management to design, implement, and operate an internal control system clear, understandable, and adequate?

   Not entirely.

   On page 8, paragraph 02.10 states that "A direct relationship exists among an entity's objectives, the five components of internal control, and the organizational structure of an entity."

   It is not clear whether "entity's objectives" refers to the overarching objectives (effectiveness, reporting, compliance) or the sub-objectives that entities develop. Also, "organizational structure" is the wrong term for this standard. The direct relationship is with the organization's system of internal controls, since it is that system (rather than the organization's structure) that is subject to internal control standards.

   Recommended rewording: "A direct relationship exists between the overarching objectives (effective and efficient operations, reliable reporting, compliance), the five components of internal control, and the system of internal control used by the entity."

   Page 12, paragraph 02.25: The meaning of objectives and subobjectives is not clear. Does the term "objectives" refer to the three overarching objectives on effectiveness, reliability, and compliance? Does the term "subobjectives" refer to the lesser objectives set by management to achieve those overarching objectives?

   Page 14, paragraph 03.06: As written, the standard does not state what management must do: "If substantially different controls were used. . . management evaluates operating effectiveness separately for each unique control system."

   Recommended rewording: "If substantially different controls were used. . . management must evaluate operating effectiveness separately for each unique control system."

6. Are the roles, divisions, and overlaps of responsibility for the oversight body, management, and personnel clear, understandable, and adequate?

   Yes.

7. Are the documentation requirements included in the Green Book clear, understandable, and adequate?

   Not entirely. Citing specific examples of effective documentation would be helpful. For instance, a flowchart graphically and succinctly conveys the "who, what, when, where, and why" of internal controls specified in paragraph 3.13 on p. 28. A flowchart is highly effective in conveying information, but its greatest utility derives from the work of preparing one. A good flowchart requires walking around, asking questions, examining documents, and looking anew at familiar processes. In this way, management can more readily identify internal control deficiencies and formulate solutions.

   Recommended rewording, p. 28, para. 3.13: Add the following as the last sentence to the paragraph: "A highly effective form of documentation is a flowchart."

8. Is there a need for additional internal control implementation guidance? If so, what form should it take?

   Yes. An updated Internal Control Management and Evaluation Tool is needed. The last version was published in 2001. Consider being more prescriptive in management's use of the checklist, and specify or recommend that sources of information obtained by management be indicated or referenced.

9. 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?

   Yes.

* Additional Comments:

- <u>Policy vs. Procedure</u>: The 1992 COSO Framework defined these as distinctly different terms. In the glossary, policy was defined as "Management's dictate of what should be done to effect control. A policy serves as the basis for procedures for its implementation." Procedure was defined simply as "An action that implements a policy." In the text, COSO explained that policy is something written or oral, and procedure is action that executes policy. The 2011 COSO does not make these distinctions, nor does the Green Book. Though policy and procedure are both forms of control activities, the similarity ends there. There is a risk that agency management may think it has effective internal controls because it (or an external oversight entity) wrote

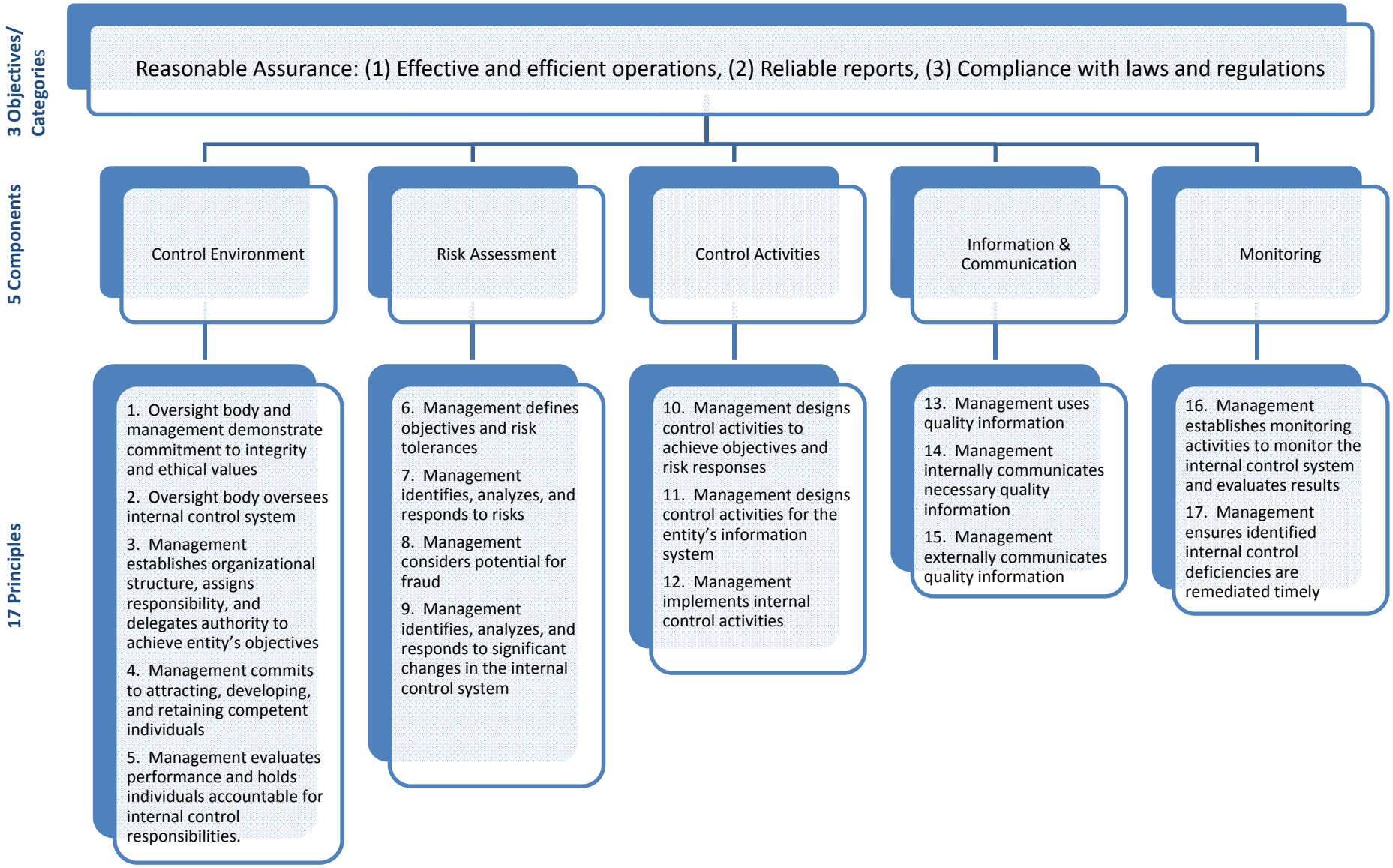
a policy, yet the actual operation of the agency program may lack the procedures necessary to achieve the purposes stated in the policy. Within the audit community, reports may sometimes cite "inadequate policies and procedures" without describing the actual breakdown in internal controls. Situations like these enable the root cause of a problem to remain unexamined. Making a distinction between 'policy' and 'procedure' can help to emphasize that effective internal control requires action, and not just policy or a directive.

- Consistent Terms for "agencies" and "management": Use of consistent terms for agencies and management would make the text clearer. For federal agencies, the Green Book uses "federal executive branch entities," "federal government entities," "entity," and "organization." For personnel, the Green Book uses "federal managers," "managers," and "management." If there is a reason to use different terms, it would be helpful to offer it via context or explanation.
- Add 'should' and 'must' to the glossary: Adding these terms would be helpful, especially if the practical effect is also shown. For example, if management decides a principle or attribute does not apply, then it must (or should) document how its internal control system achieves its objectives without them.
- Use of the terms "must" and "should": The Green Book cites 'must' only once: "An entity must have an effective internal control system to comply with the standards." Yet throughout this section the Green Book cites standards that management only *impliedly* must follow if it is to actually have an effective internal control system. The clearest standard is one that implies nothing. A less careful read of the Green Book could lead to the conclusion that unless 'must' (or 'should') is actually stated, the standard may be deemed descriptive or optional. In a number of paragraphs throughout the Green Book, 'must' or 'should' need to be added to make clear that the internal control standards are not descriptive. Some example paragraphs where 'must' ought to be inserted (there are others):
    - Forward, first paragraph:
        - Current: "As programs change and entities strive to improve operational processes and implement new technology, management continually evaluates its internal control system. . .
        - Recommended revision: "As programs change and entities strive. . . management must re-evaluate. . . **Note**: in addition to adding "must," use of "re-evaluate" states the requirement more clearly.
    - Paragraph 01.05:
        - Current: "Internal control is recognized as an integral part of the operational processes management uses to regulate and guide its operations rather than as a separate system within an entity."

- Recommended revision: "Internal control is an integral part of the operational processes management must use to regulate and guide its operations rather than as a separate system within an entity."

- Paragraph 02.17:
  - Current: "Management, as part of designing an internal control system, defines the objectives in specific and measureable terms to enable management to identify, analyze, and respond to risks related to achieving those objectives."
  - Recommended revision: "Management, as part of designing an internal control system, must define the objectives in specific, measureable terms to enable management to identify, analyze, and respond to risks related to achieving those objectives." **Note:** COSO was clear about the importance of this because there are inherent risks to the achievement of objectives, and they can be better identified when objectives are clear.
- Paragraph 02.18:
  - Current: "Management groups objectives into one or more of the three categories of objectives:"
  - Recommended: "Management must group all of its objectives into one or more of the three categories of objectives:" **Note**: All objectives should tie back to the agency's mission and the three overarching objectives. If not, then there is an elevated risk of fraud, waste, or abuse. Agencies are funded to achieve program objectives, and program objectives support the agency mission.

How the components and principles of internal control support reasonable assurance



See pp. 19-74 of the Green Book to understand how specific attributes support the principles, components, and objectives/categories shown above.