**General Comments**

- *Comment on the principles that are 'clarified' on report pg. 5 of the exposure draft.* Specifically, in principles 13-15, the words 'achieve the entity's objectives' were removed and replaced with 'support the functioning of the internal control system.' This seems like a significant narrowing of these principles. Reason? Clarification may be helpful as to why this change.

**Responses to GAO Questions**

**GAO Question: New Documentation Requirements**

1. Management would be required to document (1) the results of the risk assessment, including the identification, analysis, and response to risks that are completed on both a periodic and ongoing basis, including consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system (paragraph 7.15) and (2) a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur (paragraph 9.08).

Are these documentation requirements sufficiently clear and understandable?

***OIG Response***

- *The documentation requirements are generally clear; however, the term "consideration" requires additional clarity. Are agencies to document the conversations regarding risk even if deliberative? How extensive does GAO envision this documentation requirement? If extensive, would create an undue burden on agency risk management professionals?*

**GAO Question: Relevance of Attributes**

2. The proposed revision clarifies that management considers all attributes in properly applying the requirements and in assessing, including in summary documentation, whether the principles support the effective design, implementation, and operation of the internal control system (paragraphs OV2.08 through OV2.09 and OV3.10).

Is this application guidance relating to management's consideration of the relevance of attributes sufficiently clear and understandable?

***OIG Response***

- *The application guidance is not clear. The GAO question states that management consider attributes in properly applying the requirements, but that wording is not as direct in 2.08, 2.09, and 3.10. Suggest stating directly, as GAO does in the question, that "management consider the relevance of attributes" when responding to internal control requirements.*
- *Per OV2.08, attributes are guidance and are not mandatory. OV2.09 and OV3.10, however, inject a sense of "required". OV2.09 states that, "Management has a responsibility to understand the attributes and how they support fulfilling the requirements of the standards." OV3.10 adds, "Attributes are relevant to the proper application of the requirements and assessing whether the related principle is designed, implemented, and operating effectively."*

**GAO Question: Collaboration and Responsibility within the Internal Control System**

3. The proposed revision clarifies and adds application guidance emphasizing the importance of collaboration between all levels of management on the design, implementation, and operation of the internal control system. It also emphasizes collaboration with the oversight body, personnel, appropriate functions within the organizational structure, and external parties as applicable. It also emphasizes that the responsibility for the internal control system involves management at all levels and within all functions in the entity's organizational structure (paragraphs OV1.07, OV2.17, 1.03 through 1.04, and 16.10). Is the application guidance related to collaboration and responsibilities within the internal control system sufficiently clear and understandable?

*OIG Response*

- *16.10 is not clear regarding the term "collaborate" within the context of external parties and an agency responding to risks. GAO can clarify the use of this term to minimize the risk that there is expectation of collaboration between external independent oversight bodies such as Inspectors General, State Auditors, or GAO and an agency, which may impair independence.*
- *Note paragraph OV2.19 and footnote 9are conflicting. One says OIG is not a part of an entity's internal control system and footnote states an OIG is part of the entity's internal control system:*

**OV2.19** Oversight by external auditors and, if applicable, the office of inspector general (OIG), is not considered a part of an entity's internal control system.[9] While management may evaluate and incorporate recommendations from external auditors and the OIG, responsibility for an entity's internal control system resides with management.

[9]An OIG is an independent component within an entity. While an OIG is part of the entity's internal control system, management of the OIG is responsible for internal controls within the OIG itself.

- 

**GAO Question: External Parties**

4. The proposed revision replaced the extant discussion of service organizations with a discussion on external parties. The discussion includes service organizations and other external parties that interact with the entity, including those for which the entity has oversight responsibility (paragraphs OV4.01 through OV4.06). It also discusses control activities that management may perform to fulfill its oversight responsibilities and processes to communicate necessary information to appropriate external parties (paragraphs 10.04 and 15.03 through 15.04). Is the application guidance sufficiently clear and understandable?

OIG Response

- *The application guidance is generally clear; however, as some may consider OIGs an "external party," section 15.03 should include the words "when appropriate" so it does not imply that OIGs are helping agencies directly, hence potentially impairing OIG independence. Suggested addition highlighted below.*

- *Classifying true service organizations such as suppliers together with grantees all as "external parties" may be confusing. The reporting requirements for these two groups of external parties vary significantly – for example the entity may request a System and Organization (SOC) report from a supplier but the grantor-grantee reporting requirements at the federal government level are comprehensive and are managed by the OMB guidelines.*

**15.03.** Management communicates relevant and quality information externally through reporting lines so that appropriate external parties, when appropriate, can help the entity achieve its objectives and address related risks.

**GAO Question: Application Guidance in the Risk Assessment Component**

5. The proposed revision clarifies and adds application guidance throughout the risk assessment component for the following: (1) periodic and ongoing risk assessments (risk assessment overview, paragraphs 7.02, 7.07, 8.03, and 9.02 through 9.03); (2) internal and external risk factors, including examples (paragraphs 7.04 through 7.05, 8.05, 8.07, 8.12, and 8.15 through 8.16); (3) risk identification methods (paragraphs 7.06 and 8.04); and (4) evaluating residual risk (paragraphs 7.03 and 7.13).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

- *The application guidance is sufficiently clear and understandable. No comments.*
- *For risk documentation requirements, refer to OIG Response to GAO Question 1.*

**GAO Question: Adds Requirement to Assess Improper Payment and Information Security Risks**

6. The proposed revision adds a requirement to consider risks related to improper payments and information security when identifying, analyzing, and responding to risks. These risks are in addition to the extant requirement in principle 8 to consider the potential for fraud when identifying, analyzing, and responding to risks. The proposed revision also adds application guidance for assessing risks related to improper payments and information security (paragraphs 8.01 through 8.05 and 8.11 through 8.20).

Is the additional requirement and related application guidance sufficiently clear and understandable? Is the inclusion of the requirement and application guidance for assessing improper payments and information security risks within principle 8 appropriate?

*OIG Response*

- *The guidance in principle 8 is sufficiently clear and understandable*
- *Also suggest removing or expanding on 8.10. The three factors of the fraud triangle theory were meant to describe an individual's factors and are not comprehensive when considering fraud risk factors facing an organization. An individual's motivation would be hard for agencies to consider. Suggest deleting or expanding on this fraud risk factor section beyond the three elements of the fraud triangle theory.*

**GAO Question: Application Guidance Related to Assessing Fraud Risk**

7. The proposed revision clarifies and expands on application guidance for management's consideration of fraud risks, including guidance related to the types of fraud and external fraud risks (paragraphs 8.06 through 8.07).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

- *At a high level, the application guidance is sufficiently clear and understandable. GAO could point Green Book users to additional resources to understand the expansive and ever-changing types of fraud risks.*

**GAO Question: Identifying and Responding to Significant Changes**

8. The proposed revision clarifies and expands on application guidance for management's analysis of and response to significant changes and requires documentation of a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur (paragraphs 9.06 and 9.08 through 9.12).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

*The application guidance is sufficiently clear and understandable* **GAO Question: Discrete Processes to Manage Certain Entity Risks**

9. The proposed revision promotes developing separate and ongoing processes for managing certain risks as part of the entity's overall internal control system (paragraphs 3.03, 7.12, and 8.20).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

- *The application guidance is sufficiently clear and understandable*

**GAO Question: Categories of Control Activities**

10. The proposed revision clarifies and expands the categories of control activities illustrated in principle 10 (paragraph 10.04).

Are these categories of control activities sufficiently clear and understandable?

*OIG Response*

- *The categories of control activities are sufficiently clear and understandable.*

**GAO Question: Prioritizing Preventive Control Activities**

11. The proposed revision emphasizes the importance of designing an appropriate mix of preventive and detective control activities and prioritizing preventive control activities where appropriate (paragraphs 10.09 through 10.11).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

- *The application guidance is sufficiently clear and understandable.*

**GAO Question: Changes Related to Information Technology**

12. The proposed revision modifies the requirement in principle 11 to focus on general control activities (paragraph 11.01) and modifies and reorganizes the application guidance included in principle 11 (paragraphs 11.02 through 11.17). Information technology control activities and objectives that are not related to general control activities have been moved to principle 10.

Is the application guidance related to information technology in principles 10 and 11 sufficiently clear and understandable?

*OIG Response*

- *Yes. The application guidance is sufficiently clear and understandable.*

**GAO Question: Focus of Information and Communication**

13. Proposed changes to application guidance in the information and communication component clarify that relevant and quality information and communication, including information requirements, support the five components of internal control (paragraphs 13.01 through 13.02, 14.01, 14.03, and 15.01).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

- *Yes. The application guidance is sufficiently clear and understandable.*

**GAO Question: Monitoring Component**

14. The proposed revision clarifies that monitoring activities are used to evaluate whether each of the five components of internal control is present and functioning or if change is needed (paragraphs 16.02 and 17.07). It also (1) clarifies how management determines the scope and frequency of monitoring activities (paragraph 16.06), (2) explains the distinction between control activities and monitoring activities (see app. II), and (3) provides examples of methods and tools that management could use for monitoring activities (paragraphs 16.04 through 16.06).

Is the application guidance sufficiently clear and understandable?

*OIG Response*

- *Yes. The application guidance is sufficiently clear and understandable.*

**GAO Question: New Appendixes**

15. The proposed standard includes two new appendixes that provide (1) examples of preventive and detective control activities and (2) references to additional resources that management may leverage in designing, implementing, and operating effective internal control systems to address risk areas related to fraud, improper payments, information security, and the implementation of new or substantially changed programs, including emergency assistance programs.

Are these new appendixes sufficiently clear and understandable?

*OIG Response*

- *The new appendixes are sufficiently clear and understandable.*