

**Response to Questions for Commenters**  
**GAO-24-106889 Federal Internal Control Standards**  
**Department of the Treasury**  
**Office of the Deputy Chief Financial Officer**  
**August 1, 2024**

---

**New Document Requirements**

1. Are these documentation requirements sufficiently clear and understandable?

Response: *Yes.*

**Relevance of Attributes**

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

Response: *Yes.*

**Collaboration and Responsibility within the Internal Control System**

3. Is the application guidance related to collaboration and responsibilities within the internal control system sufficiently clear and understandable?

Response: *Yes. While the important role of “personnel” is stated, it would be helpful to emphasize the importance of all employees, regardless of level, in an internal control system.*

**External Parties**

4. Is the application guidance sufficiently clear and understandable?

Response: *Yes*

**Application Guidance in the Risk Assessment Component**

5. Is the application guidance sufficiently clear and understandable?

Response: *Yes.*

**Adds Requirement to Assess Improper Payment and Information Security Risks**

6. 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?

Response: *Generally, yes, the additional requirement and related application guidance is sufficiently clear and understandable. However, it is a little confusing to have information security risks addressed in principle 8 and again in principle 11. Suggest covering this comprehensively in one principle. Also, suggest moving improper payments risk to principle 7 related to assessing risks related to achieving defined objectives. Improper payments can occur*

*due to a variety of factors, only one of which is fraud, therefore, assessing risk related to improper payments would be better included under principle 7.*

#### **Application Guidance Related to Assessing Fraud Risk**

7. Is the application guidance sufficiently clear and understandable?

Response: *Yes. (However, see comments under question number 6 regarding improper payments and information security risks.)*

#### **Identifying and Responding to Significant Changes**

8. Is the application guidance sufficiently clear and understandable?

Response: *Yes.*

#### **Discrete Processes to Manage Certain Entity Risks**

9. Is the application guidance sufficiently clear and understandable?

Response: *Yes.*

#### **Categories of Control Activities**

10. Are these categories of control activities sufficiently clear and understandable?

Response: *Yes. Providing a contextual example on how a risk to a specific objective might be addressed with a control activity would be helpful for less experienced practitioners.*

#### **Prioritizing Preventive Control Activities**

11. Is the application guidance sufficiently clear and understandable?

Response: *Yes*

#### **Changes Related to Information Technology**

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

Response: *Yes.*

#### **Focus of Information and Communication**

13. Is the application guidance sufficiently clear and understandable?

Response: *Yes.*

#### **Monitoring Component**

14. Is the application guidance sufficiently clear and understandable?

Response: *While there are examples of monitoring methods and tools, expanding the discussion of the examples would be helpful so that less experienced practitioners could gain a better understanding of what an internal control system monitoring plan might look like.*

## New Appendixes

15. Are these new appendixes sufficiently clear and understandable?

Response: *Providing a scenario in Appendix II to show how a control objective addresses a specific risk, and how an appropriately designed control activity satisfies the objective would help less experienced practitioners make the connections between risk and internal control activity.*

---

## Specific Comments

### GAO-24-106889 Federal Internal Control Standards

#### Department of the Treasury

#### Office of the Deputy Chief Financial Officer

August 1, 2024

1. OV2.04 regarding the Five Components of Internal Control: In the fifth bullet on “Monitoring”, we suggest including that “reviews” includes internal management reviews.
2. OV2.19 regarding Roles in an Internal Control System: Says “Oversight by ...OIG is not considered part of an entity’s internal control system.” This statement references footnote 9, which seems to contradict this statement by saying: “...While an OIG is part of the entity’s internal control systems...” This should be clarified.
3. OV2.28 regarding Safeguarding of Assets: Given the importance of data as an asset, clarifying that assets include data in this section would be helpful.
4. OV3.05 regarding Evaluating the Design and Implementation of Controls: Defining the methodology to determine the severity of a deficiency would be helpful.
5. OV3.06 regarding Evaluating the Operating Effectiveness of Controls: Add at the end of the first sentence, “...and whether they were applied as designed.” The sentence would then read as follows:

*In evaluating operating effectiveness, management determines if controls were applied at relevant times during the period under evaluation, the consistency with which they were applied, by whom or by what means they were applied, and whether they were applied as designed.*

6. OV4.07 regarding Information Technology: Suggest replacing “may be” in the first sentence with “is” given the criticality of information technology.
7. 7.01 regarding the Attributes: Suggest adding “Documentation of Risk Assessment Results” as an attribute.
8. 7.06 regarding Root Cause Analysis: While the update notes that performing analysis to identify the root cause of internal control deficiencies can assist management in identifying risks, it may be helpful provide examples of what to look for in root cause analysis and how to perform the analysis.
9. 8.01 regarding Attributes: Suggest adding “Documentation of Fraud Risk Assessment Results” as an attribute.

10. 9.01 regarding Attributes: Suggest adding “Documentation of Process for Responding to Change” as an attribute.
11. 10.04, Figure 6: Common Categories of Control Activities: Consider replacing “Oversight of grant programs” with “Oversight of federal financial assistance programs,” “Oversight of federal awards.” or something similar. This would encompass grants and all other types of federal awards that require oversight/control activities.
12. 17.05 regarding Evaluation of Internal Control Issues: Defining a methodology to determine the severity of issues would aid the user in determining the potential nature, timing, and extent of corrective actions.