The **Department of Health & Human Services'** consolidated comments on the *Standards for Internal Control in the Federal Government* 2024 exposure draft.

New Documentation Requirements

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).

	RESPONSE
1. Are these documentation requirements sufficiently clear and understandable?	9.08 - The documentation that management needs to make is in response to significant changes and related risks for quick adaptation for the internal control system. Are there examples of responses to changes like COVID-19 or natural disasters, or do these changes pertain solely to organizational restructuring? Please include brief details of both internal and external changes and risks that impact the internal control system.

Relevance of Attributes

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).

	RESPONSE
2. Is this application guidance relating to management's consideration of the relevance of attributes sufficiently clear and understandable?	Yes, the application guidance relating to management's consideration of the relevance of attributes is clear and understandable.

Collaboration and Responsibility within the Internal Control System

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).

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

External Parties

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).

RESPONSE

4. Is the application guidance sufficiently clear and understandable?

Yes, the application guidance is sufficiently clear and understandable.

Application Guidance in the Risk Assessment Component

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).

	RESPONSE
5. Is the application guidance sufficiently clear and understandable?	
	7.04 - We recommend including national security as an external risk factor. Additionally, could you clarify whether the information in 8.15 and 8.16 pertains to 8.12?

Adds Requirement to Assess Improper Payment and Information Security Risks

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).

	RESPONSE
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?	**For consistency, we recommend that the Green Book guidance align more closely with OMB Circular A-123, Appendix C concerning improper payments (8.11-8.20): 1) Definition and Terminology:** The definition of improper payments and related terminology should be consistent across federal guidance (e.g., Amount Properly Paid, Amount Improperly Paid, Unknown, Monetary Loss, and Non-Monetary Loss). For instance, while 8.11 defines an improper payment as 'any payments that should not have been made or that were made in an incorrect amount,' it does not explicitly include payments that were not made but should have been. The definition should reflect all types of improper payments, including underpayments. **2) Unknown Payments:** We recommend that the Green Book guidance specifically address Unknown payments. **3) Language on Internal Control Deficiencies:** OMB Circular A-123, Appendix C refers to 'significant deficiencies in the audit report or other relevant management findings of the agency that might hinder accurate payment certification.' In contrast, the Green Book language in 8.12 states 'identified internal control deficiencies that might hinder accurate payment processing.' We suggest combining these approaches, as the language in A-123, Appendix C is broader and encompasses the certification of payments, not just their processing.

Application Guidance Related to Assessing Fraud Risk

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).

RESPONSE

7. Is the application guidance sufficiently clear and understandable?

8.07 - We suggest also addressing internal party risks in the "Types of Fraud and Fraud Risk Factors" section.

Identifying and Responding to Significant Changes

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).

	RESPONSE
8. Is the application guidance sufficiently clear and understandable?	Yes, the application guidance is sufficiently clear and understandable.

Discrete Processes to Manage Certain Entity Risks

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).

	RESPONSE
9. Is the application guidance sufficiently clear and understandable?	
	Yes, the application guidance is sufficiently clear and understandable.

Categories of Control Activities

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

	RESPONSE
10. Are these categories of control activities sufficiently clear and understandable?	Yes, the categories of control activities are sufficiently clear and understandable.

Prioritizing Preventive Control Activities

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).

	RESPONSE
11. Is the application guidance sufficiently clear and understandable?	Yes, the application guidance is sufficiently clear and understandable.

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.

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

Focus of Information and Communication

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).

	RESPONSE
13. Is the application guidance sufficiently clear and understandable?	Yes, the application guidance is sufficiently clear and understandable.

Monitoring Component

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).

	RESPONSE
14. Is the application guidance sufficiently clear and understandable?	Yes, the application guidance is sufficiently clear and understandable.

New Appendixes

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.

	RESPONSE
Are these new appendixes sufficiently clear and understandable?	Yes, the new appendixes are sufficiently clear and understandable.