Discussion Questions for Responses

1. New Documentation Requirements

DHS OCFO has reviewed the two new documentation requirements related to 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 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. Overall, the documentation requirements are sufficiently clear and understandable. However, DHS OCFO has provided the following comments to include proposed modifications and/or adjusted language to these documentation requirements:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
1	1. New Documentation Requirements	7.01	Recommend adding a fourth Attribute for Documenting the Results the Risk Assessment	Proposed Language Adjustments: 7.01 Management should identify, analyze, and respond to risks related to achieving the defined objectives. **Attributes** The following attributes contribute to the design, implementation, and operating effectiveness of this principle: • Identification of Risks • Analysis of Risks • Response to Risks • *Documenting the Results of the Risk Assessment*	Refer to comment #2 below.
2	1. New Documentation Requirements	7.15	Move language in 7.15 to a new proposed attribute associated with Documenting the Results of the Risk Assessment	Proposed Modification: Move language in 7.15 to a new proposed attribute associated with Documenting the Results of the Risk Assessment	The documentation requirements include the results of the risk assessment which has been defined to include identification, analysis, and response to risks. Since this documentation requirement spans all of those attributes, would not recommend embedding in the Response to Risks attribute as it is not confined to just that single attribute area.

2. Relevance of Attributes

DHS OCFO has reviewed the application guidance relating to management's consideration of the relevance of attributes and believes that is not sufficiently clear. As such, DHS OCFO has provided the following comment to include proposed

modifications and/or adjusted language to the application guidance and the relevance of attributes:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
3	2. Relevance of Attributes	OV3.10	The current application guidance regarding the attributes within the standards is not sufficiently clear.	Proposed Modification: Recommend that the standards more clearly define the impact to the component and principle if a relevant attribute is not effective. As currently stated, it appears management has the discretion to determine the impact, which will likely lead to inconsistency in application. At a minimum, recommend that guidance be provided to aid in standardizing management's process to determine impact.	The standards should provide greater clarity on the impact to the related principle and component if an attribute is not effective. The current language states that "If a principle is not designed, implemented, or operating effectively, then the respective component cannot be effective. Attributes are relevant to the proper application of the requirements and assessing whether the principle is designed, implemented, and operating effectively" (OV3.10). While the impact to a component when a principle is not effective is very clear, the impacts in not adhering to the attributes in determining the principle's effectiveness should be clarified.

3. Collaboration and Responsibility within the Internal Control System

   DHS OCFO has reviewed the application guidance related to collaboration and responsibilities within the internal control system and believes that it is sufficiently clear and understandable.

4. External Parties

   DHS OCFO has reviewed the application guidance related to external parties and believes that it is sufficiently clear and understandable. However, DHS OCFO believes that the language should be expanded to address subservice organizations and complementary subservice organization controls. DHS OCFO has provided the following comments to include proposed modifications and/or adjusted language to the application guidance related to external parties:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
4	4. External Parties	OV4.03	Language highlights business processes that may be performed by the Service Organization. However, would recommend that language be strengthened to ensure coverage related to Service Organizations that are providing Information Technology.	Proposed Language Adjustments: OV4.03 Management may engage external parties to perform certain business processes for the entity, such as accounting and payroll processing, security services, or health care claims processing. This may include any external party, such as a contractor, that provides services to achieve the entity's control objectives. *In addition, Management may engage external parties to provide information technology, such as to the infrastructure, platforms, and software used to automate business processes.* In the Green Book, these external parties are referred to as service organizations. Management, however, retains responsibility for the performance of controls over processes assigned to *and information technology provided by* service organizations and identifying, analyzing, and responding to associated risks. Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned business process *and information technology* and how the service organization's internal control system impacts the entity's internal control system.	The reader may not associate services and "business processes" that is currently in the language to a system being provided by an external party or service organization.

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
5	4. External Parties	OV4.03 - OV4.06 10.04 - Oversight of service organizations	Language for Service Organizations is silent related to sub-service organizations. Per SSAE 18, Subservice organization is defined as a service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting.	Proposed Modification: Recommend adjusting language in OV4.03 - OV4.06, 10.04 related to Oversight of service organizations, and XX to include Subservice Organizations as well as complementary subservice organization controls.	Ensure alignment with SSAE 18
6	4. External Parties	Glossary	Add definition for subservice organization	Proposed Language Adjustments: *subservice organization: A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control system.*	User entities internal control system is reliant on the service organization which is reliant on the subservice organization(s) and the complementary subservice organization controls. Cannot ensure assurance of the internal control system without this coverage.
7	4. External Parties	Glossary	Add definition for complementary subservice organization controls	Proposed Language Adjustments: *complementary subservice organization controls: Controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.*	User entities internal control system is reliant on the service organization which is reliant on the subservice organization(s) and the complementary subservice organization controls. Cannot ensure assurance of the internal control system without this coverage.

5. Application Guidance in the Risk Assessment Component

   DHS OCFO has reviewed the application guidance in the risk assessment component and believes that it is sufficiently clear and understandable.

6. Adds Requirement to Assess Improper Payment and Information Security Risks

   DHS OCFO has reviewed the additional requirement and application guidance related to assessing improper payment and information security risks and believes that it is sufficiently clear and understandable. However, DHS OCFO does not believe that the inclusion of the requirement and application guidance for assessing improper payments and potentially the information security risks within principle 8 is appropriate. DHS OCFO has provided the following comments to include proposed modifications and/or adjusted language to the requirement and application guidance related to improper payments and information technology risks:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
8	6. Adds Requirement to Assess Improper Payment and Information Security Risks	Principle 8	Consider moving the new improper payment and information security risk information to a separate appendix. **Higher priority proposed modification than #9 below**	<u>Proposed Modification:</u> Recommend the additional requirements be taken out of the standards and moved to an appendix. Also recommend clarifying language be added that agencies should consider these risk areas when determined to be significant to the entity performing the risk assessment.	A risk assessment involves an organization identifying its most significant risks to achieving its objectives and determining appropriate risk responses to mitigate these risks to an acceptable level. Depending upon the organization, improper payment risks and information technology risks may not be considered amongst the most significant risks. The concept of enterprise risk management (ERM) includes prioritizing the most significant risks across the entity for consideration and action. The requirement to always focus on certain risk areas, regardless of the assessed risk level to the organization performing the risk assessment, seems to run counter to the concept of ERM.
9	6. Adds Requirement to Assess Improper Payment and Information Security Risks	Principle 8	Consider moving the new information security risk information to a separate appendix. **Lower priority proposed modification than #8 above**	<u>Proposed Modification:</u> Recommend the additional requirements be taken out of the standards and moved to an appendix. Also recommend clarifying language be added that agencies should consider these risk areas when determined to be significant to the entity performing the risk assessment.	

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
10	6. Adds Requirement to Assess Improper Payment and Information Security Risks	8.11	Should the types of improper payments be expanded to also include payments that are insufficiently documented and/or technically improper payments in alignment with OMB Circular A-123 Appendix C language?	<u>Proposed Language Adjustments:</u> Types of improper payments include the following: • Overpayments - These payments are those in excess of the amount due to be paid to recipients. They include payments to an ineligible recipient, any payment for an ineligible good or service, and any duplicate payment. They could be either intentional—such as fraudulent payments—or unintentional. • Underpayments - These payments are those in which recipients did not receive some or all the funds to which they were entitled. *• Technically Improper Payments - These payments are those made to an otherwise qualified recipient for the right amount but the payment failed to meet all regulatory or statutory requirements.* *• Insufficiently Documented Payments - These payments are those where the entity is unable to obtain the documentation needed to determine whether the payment was made to the right recipient or for the right amount.*	Ensure alignment with the newly drafted OMB Circular A-123 Appendix C

7. Application Guidance Related to Assessing Fraud Risk

   DHS OCFO has reviewed the application guidance related assessing fraud risks and believes that it is sufficiently clear and understandable.

8. Identifying and Responding to Significant Changes

   DHS OCFO has reviewed the application guidance related to identifying and responding to significant changes and believes that it is sufficiently clear and understandable. However, DHS OCFO would strongly urge that the standards balance the need for effective risk management and internal control with the need for federal agencies to respond to rapidly changing conditions, such as emergency assistance programs in response to a disaster or catastrophic event. DHS OCFO has provided the following comment to include proposed modifications and/or adjusted language to the

requirement and application guidance related to identifying and responding to significant changes:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
11	8. Identifying and Responding to Significant Changes	9.05	Revise the timeline for performing risk assessments in response to changing conditions.	<u>Proposed Modification:</u> Recommend the standards revise language in 9.05 to instead be for entities to perform risk assessments and revisions to the internal control system as soon as possible, rather than before the entity responds to change. When time is of the essence, documenting a risk assessment and internal control revisions should not take precedent over disaster response, especially when a federal response is needed urgently to save human lives or prevent further disaster impacts. <u>Proposed Language Adjustments:</u> 9.05: As part of the risk assessment process, management analyzes and responds to change and related risks on a timely basis to maintain an effective internal control system. Changes in conditions affecting the entity and its environment often require changes to the entity's internal control system, as existing controls may not be effective for meeting objectives or addressing risks under changed conditions. Management analyzes the impact of identified changes on the internal control system and responds by revising the system on a timely basis, when necessary to maintain its effectiveness. This risk assessment, and revision to the internal control system when necessary, is completed by the entity ~~before the entity responds to~~ *as soon as possible to respond to* changing conditions; for example, by implementing a new program or making significant changes to existing programs or activities."	The standards need to balance the need for effective risk management and internal control with the need for federal agencies to respond to rapidly changing conditions, such as emergency assistance programs in response to a disaster or catastrophic event.

9. Discrete Processes to Manage Certain Entity Risks

DHS OCFO has reviewed the application guidance related to discrete processes to manage certain entity risks and believes that the language can be enhanced to ensure that it is sufficiently clear and understandable. DHS OCFO has provided the following comment to include proposed modifications and/or adjusted language to the requirement and application guidance related to discrete processes to manage certain entity risks:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
12	9. Discrete Processes to Manage Certain Entity Risks	7.12 & 8.20	Provide additional clarification on the separate and ongoing risk assessments for managing certain risks.	Proposed Modification: Recommend the standards include additional clarification and clarity in 7.12 and 8.20 regarding the separate and ongoing processes, with separate oversight responsibilities, for managing certain risks (including potentially fraud, improper payments, and information security).	The exposure draft already includes (1) periodic risk assessments and (2) ongoing risk assessments, and it is not entirely clear how the separate and ongoing risk management efforts outlined in 7.12 and 8.20 fit within that overall structure.

10. Categories of Control Activities

DHS OCFO has reviewed the categories of control activities and believes that the language is sufficiently clear and understandable. However, DHS OCFO believes that the language included may be duplicative as it related to improper payment related control activities and is not sufficiently expansive to include service and subservice organization controls. DHS OCFO has provided the following comments to include proposed modifications and/or adjusted language to the categories of control activities:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
13	10. Categories of Control Activities	10.04 Figure 6	Improper-payment-related control activities appears to be duplicative with many of the already listed control activities.	<u>Proposed Modification:</u> In alignment with comment #8 above, reconsider whether Improper-payment-related control activities needs to be listed or is already sufficiently covered. For example, the following already listed common categories of control activities relates heavily to the risk of improper payments: • Reviews by management at the functional or activity level • Proper execution of transactions • Accurate and timely recording of transactions • Appropriate documentation of transactions and controls • Oversight of grant programs • Segregation of duties	Remove duplication and ensure that the standards work for all organizations, programs, and risk types.
14	10. Categories of Control Activities	10.04 - Oversight of service organizations	Adding additional controls information related to oversight of service organizations.	<u>Proposed Modification:</u> Recommend that the discussion of oversight of service organizations in 10.04 include a discussion of both complementary user entity controls as well as other controls, to include service organization and subservice organization controls, similar to language that is already included in OV4.04: *Other controls may include those related to monitoring the effectiveness of the design, implementation, and operation of the service organization's controls in achieving the entity control objectives.*	Alignment and consistency with language used in OV4.04 regarding both complimentary user entity controls and other controls.

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
15	10. Categories of Control Activities	10.04 - Oversight of service organizations	Adjust language related to processes for communicating to establish a two-way communication channel. Also recommend adding a reference footnote on the communication language to point to Principle 15.	Proposed Language Adjustments: Oversight of service organizations Management establishes control activities to oversee service organizations that perform business processes on behalf of the entity. The entity may also establish complementary user entity controls that service organization management identified as being necessary for the entity to achieve its objectives. Management establishes processes for *obtaining communication from and* communicating necessary information to service *and subservice* organizations, such as relevant risks, internal control practices to consider, and other circumstances that may impact achieving the entity's objectives.	Alignment and consistency with Principle 15 language

11. Prioritizing Preventive Control Activities

    DHS OCFO has reviewed the application guidance related to prioritizing preventative control activities and believes that the language is sufficiently clear and understandable.

12. Changes Related to Information Technology

    DHS OCFO has reviewed the application guidance related to information technology in principles 10 and 11 and believes that the language is sufficiently clear and understandable.

13. Focus of Information and Communication

    DHS OCFO has reviewed the application guidance related to the focus of information and communication and believes that the language is sufficiently clear and understandable. DHS OCFO has provided the following comment to include proposed modifications and/or adjusted language to the application guidance related to the monitoring component:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
16	13. Focus of Information and Communication	13.04	Adjust language to be consistent with the Categories of Objectives listed in OV2.21	Proposed Language Adjustments: 13.04 Management obtains or generates relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Relevant data have a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. Management obtains relevant data through a variety of forms, including manual input or compilation, or using information technology. Sources of data can be operational, ~~financial~~ *reporting*, or compliance related. Management obtains data on a timely basis so that they can be used for effective monitoring.	Consistency with the Categories of Objectives listed in OV2.21

14. Monitoring Component

DHS OCFO has reviewed the application guidance related to the monitoring component and believes that the language is sufficiently clear and understandable. However, DHS OCFO believes that the language can be streamlined to correlate to principle 16. DHS OCFO has provided the following comment to include proposed modifications and/or adjusted language to the application guidance related to the monitoring component:

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
17	14. Monitoring Component	12.05	Update language to identify ongoing monitoring and separate evaluations in 16.04 as a periodic review of control activities.	Proposed Modification: Recommend adding a reference footnote to point to Principle 16, Internal Control System Monitoring to highlight that the ongoing monitoring and separate evaluations highlighted in 16.04 can serve as a way to satisfy the periodic review of control activities.	Streamlining execution and relating like activities

15. New Appendixes

DHS OCFO has reviewed the new appendices and believes that the language within the appendices is sufficiently clear and understandable.

DHS Comment #	Associated Discussion Question	Paragraph / Document Location	Comment	Proposed Language or Modification	Rationale for Proposed Language or Modification
18	N/A	Appendix III: Additional Resources	Will this appendix be published separately so that it can be updated as needed to keep references current and accurate but not requiring a republication of the entire Green Book?	N/A	N/A