From: Polen, Chris - OCFO
To: Green Book Comments
Cc: [redacted]
Subject: DOL Feedback on GAO"s Updated Draft "Green Book"
Date: Monday, August 26, 2024 11:50:37 AM
Attachments: GreenBook Update - Review Template - DOL RESPONSES.xlsx

GAO – DOL sent the draft Green Book updates to senior program officials across the Department to prepare comments on behalf of their program/agency. This included grants, benefits, contracts/administrative, investigative, enforcement, etc. Attached, please find comments to each of the review questions from five responding DOL component agencies – see tab "3 Review Questions", columns C-G. In addition, one component noted the following which doesn't apply to any of the specific review questions:

> Agency "*noted that the graphics on the first pages are dizzying, and the additional graphics don't seem to be 508 compliant. The graphics are alt tagged but not with a description of the actual picture. Each picture references a source, not a description.*"

Please let me know if you have any questions.

Chris Polen
Director, Financial Policy
Division of Financial Policy & Compliance, Office of the Chief Financial Officer
Department of Labor

Office of the Chief Financial Officer
United States Department of Labor

[redacted]

[redacted]

INSTRUCTIONS: After reviewing the Tab 2 SUMMARY OF CHANGES, reviewers should respond to each of the questions below. Please use the included Green Book update found on p. 21-126 of the included GAO EXPOSURE DRAFT doc.

CATEGORY	REVIEW QUESTION	DOL AGENCY RESPONSES - Agency 1	DOL AGENCY RESPONSES - Component Agency 2	DOL AGENCY RESPONSES - Component Agency 3	DOL AGENCY RESPONSES - Component Agency 4	DOL AGENCY RESPONSES - Component Agency 5
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?	See response for #3.	Yes	Yes, the documentation requirements are clear and understandable. The inclusion of periodic and ongoing risk assessments ensures comprehensive monitoring, and the process for adapting to significant changes enhances flexibility and responsiveness in the internal control system.	These new documentation requirements are clearly articulated, particularly in terms of emphasizing periodic and ongoing risk assessments. This approach not only aligns with previous guidelines but also introduces a more structured method for documenting these assessments, which is essential for maintaining transparency and accountability throughout the review process. The mandate to document a process for responding to significant changes and associated risks (as outlined in Paragraph 9.08) could be highlighted further. This is crucial as it ensures that internal controls can quickly adapt to changing conditions.	The requirements are sufficiently clear and understandable.
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?	See response for #3.	Yes	Yes, the guidance on considering the relevance of attributes is clear. It provides a structured approach for management to assess and document the effectiveness of internal controls, ensuring that all necessary attributes are considered.	The requirement for managers to consider all attributes when applying the requirements facilitates a thorough evaluation of the internal control system. This comprehensive approach aids in identifying potential weaknesses that might be missed if only selected attributes were considered. The focus on summary documentation enables management to effectively communicate their assessments and the overall effectiveness of the internal control system.	Yes, this application guidance related to management's consideration of attribute relevance is sufficiently clear and understandable.
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?	While the implemented changes are recognizable and understandable to those who deal with risk management, planning and practice, it's probably beyond the scope and understanding of most managers in terms of implementing the changes as it relates to their own internal control responsibilities. These expanded responsibilities should themselves be managed through additional training or controls implemented at a Departmental level (such as through a Leading @ Labor course) to allow managers to understand their own expanded risk management responsbilities under the new Green Book guidance.	Yes	Yes, the application guidance on collaboration and responsibilities is clear. It highlights the need for a cohesive approach involving all levels of management and relevant external parties, ensuring a comprehensive and integrated internal control system.	The emphasis on collaboration across all levels of management and with external parties promotes an integrated, cohesive, and transparent approach to internal controls. This collaborative strategy enhances a culture of shared responsibility, positively impacting the overall internal control system. The updated guidance effectively outlines the roles and expectations for management at all levels, aiding in the facilitation of thorough reviews. Consequently, this ensures that all parts of the organization are aligned and collaboratively working towards the same internal control objectives, fostering a more robust and effective system.	Yes, this application guidance related to collaboration and responsibilities within the internal controls system is sufficiently clear and understandable.
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?	See response for #3.	Yes. In addition, it would be ideal if 15.03 defines how external parties help the management. Any examples?	Yes, the guidance on external parties is clear. It provides a detailed explanation of how to manage interactions with service organizations and other external parties, ensuring that oversight responsibilities are effectively fulfilled.	By broadening the discussion to encompass all external parties, not just service organizations, the guidance provides a transparent view of the complex network of interactions that modern entities navigate. This approach allows entities to leverage external relationships to enhance their internal control systems effectively. The guidance on communication processes and control activities involving external parties is detailed and practical. It promotes increased interaction between stakeholders and offers management well-defined steps to follow. Throughout the Green Book GAO allows for management judgement. Paragraph OV4.05 does not mention judgement or materiality to detemine the extent of oversight of service organizations. We believe materiality should be a factor to consider in oversight of external parties under paragraph OV4.05.	"OV4.04 If controls the service organization performs are necessary for the entity to achieve its control objectives related to the assigned business process, the entity's internal controls may include complementary user entity controls and other controls, as appropriate, related to the use of the service organization." - VERBIAGE IN RED IS CONFUSING.

CATEGORY	REVIEW QUESTION	DOL AGENCY RESPONSES - Agency 1	DOL AGENCY RESPONSES - Component Agency 2	DOL AGENCY RESPONSES - Component Agency 3	DOL AGENCY RESPONSES - Component Agency 4	DOL AGENCY RESPONSES - Component Agency 5
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?	See response for #3.	Yes	Yes, the application guidance in the risk assessment component is clear and comprehensive. It provides detailed steps for conducting risk assessments, identifying risks, and evaluating residual risks, which enhances the overall risk management process.	The application guidance in the risk assessment component provides detailed instructions on conducting both periodic and ongoing risk assessments, which are crucial for maintaining a dynamic and responsive internal control system. The inclusion of specific examples of internal and external risk factors is particularly beneficial, as it aids management in identifying and addressing a broad spectrum of potential risks. Furthermore, the guidance on risk identification methods and the evaluation of residual risks is comprehensive, offering practical tools and techniques for effective risk management. This ensures that organizations are not only aware of the risks they face but are also equipped to measure and mitigate these risks appropriately.	"Typically, controls are not needed when an entity chooses to either accept or avoid a risk. - VERBIAGE IN RED IS CONFUSING. **I would think even at the most acceptable level of risk tolerance, there should be controls in place that satisfy one or more components.** 8.14 Management considers the types of risks that could impact the entity's information and information technology to provide a basis for identifying and analyzing risks related to information security." - Is this accurate to say that controls are not need just because the entity chooses to avoid or accept risk?
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?	See response for #3.	Yes. 8.05 could also include public such as taxpayers and citizens who benefit from government services in addition to other external parties. 8.15 can be expanded to include such unintentional factors as lack of understanding and lack training among employees that ultimately contribute to higher internal risks.	Yes, the additional requirement and related application guidance are clear and appropriate. Including improper payments and information security risks within principle 8 ensures a comprehensive approach to identifying and managing these critical risk areas.	By explicitly including improper payments and information security risks, the revision targets critical vulnerabilities that can significantly impact an entity's operations and reputation. The detailed application guidance offers reasonable and actionable steps for assessing these risks, thereby enhancing the robustness of the internal control system. Including these requirements within Principle 8 is strategically sound as it consolidates guidance on fraud, improper payments, and information security into a single, comprehensive framework for risk management.	The additional requirement and related application guidance is sufficiently clear and understandable. The inclusion of the requirement and application guidance for assessing improper payments and information security risks within principle 8 is appropriate.
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?	See response for #3.	Yes	Yes, the guidance on assessing fraud risk is clear and comprehensive. It provides detailed information on identifying different types of fraud, including external fraud risks, which is essential for robust risk management.	By expanding on the types of fraud and including external fraud risks, the revision provides a more holistic framework for identifying and mitigating fraud risks. This detailed guidance is crucial as it helps management understand the various dimensions of fraud and its potential impacts on an entity. The expanded guidance aligns with best practices in fraud risk management, significantly enhancing the entity's capabilities to detect and respond to fraud effectively. This approach not only addresses the traditional areas of fraud but also considers the evolving nature of fraudulent activities, especially in a digital and globalized business environment.	The application guidance is sufficiently clear and understandable.
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?	See response for #3.	Yes	Yes, the guidance on identifying and responding to significant changes is clear. The requirement for documenting processes ensures that the internal control system remains adaptable and responsive to evolving conditions and risks.	The requirement to document a process for responding to significant changes is a crucial enhancement that increases management's ability to adapt the internal control system to new conditions. This proactive approach is essential for maintaining the effectiveness of internal controls in a rapidly changing business environment. The expanded guidance offers clear, actionable steps for analyzing and responding to changes, enabling management to address new risks swiftly and effectively. By providing a structured framework for response, the guidance ensures that entities are not only reactive but also preemptive in their approach to risk management. This capability to quickly adapt and respond is particularly valuable in today's dynamic market conditions, where changes can occur abruptly and have significant impacts.	The application guidance is sufficiently clear and understandable.
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?	See response for #3.	Yes. The Organization Structure may also include a separate section to periodically assess the existing structure to see whether it needs any updates in response to various changes affecting the organization.	Yes, the guidance on developing discrete processes for managing certain entity risks is clear and understandable. This approach allows for specialized focus on high-risk areas, ensuring that they are managed effectively within the overall internal control system.	The application guidance for developing separate and ongoing processes for managing certain risks is indeed clear and effectively addresses the need for specialized attention to critical areas such as fraud, improper payments, and information security. Recognizing that these risks require continuous and focused management is crucial for maintaining robust internal controls. By promoting discrete processes for these specific risk areas, the revision ensures that each is managed with an appropriate level of focus and resources. This structured approach not only enhances the effectiveness of internal controls but also aligns with best practices in risk management. It allows organizations to tailor their risk management strategies to the unique challenges posed by these high-risk areas, ensuring that mitigation efforts are both efficient and effective.	The application guidance is sufficiently clear and understandable.

CATEGORY	REVIEW QUESTION	DOL AGENCY RESPONSES - Agency 1	DOL AGENCY RESPONSES - Component Agency 2	DOL AGENCY RESPONSES - Component Agency 3	DOL AGENCY RESPONSES - Component Agency 4	DOL AGENCY RESPONSES - Component Agency 5
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?	See response for #3.	Yes	Yes, the expanded categories of control activities are clear. The detailed examples and explanations provided help to better understand and implement appropriate control activities for various risk scenarios.	The expansion and clarification of the categories of control activities in the revision indeed provide a more comprehensive framework for designing and implementing control activities. This enhancement is crucial as it helps management ensure that all relevant types of controls are considered and appropriately applied across various operational and functional areas. By detailing the categories of control activities, the revision aids management in understanding the breadth and depth of controls that can be utilized. This thorough approach ensures that control activities are not only identified but are also aligned with the specific risks and requirements of the organization. The inclusion of detailed examples of control activities further assists management by offering practical, real-world applications that can be tailored to meet specific organizational needs.	Transactions are authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources are initiated or entered into. Management clearly communicates authorizations to personnel by assigning the capabilities to their credentials in the technology system, or by signature or other methods of express approval. Management may require approval from multiple levels or units (multi-level authorization) to authorize unique or recurring transactions that present a greater risk to the entity. - **Suggestion to include verbiage on recurring recertification of system and credential access. Also to include requirements to document unique situations where system overrides are approved to post necessary transactions. Those that have temporary superuser access for instance should only remain on the access tables for temporary time-periods.**
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?	See response for #3.	Yes. In addition, 10.10 or 10.11 may mention that no control activity is proven to be 100% effective to address unintended events or results.	Yes, the guidance on prioritizing preventive control activities is clear and well-structured. Emphasizing preventive controls ensures that risks are mitigated effectively before they can materialize, which is both cost-efficient and strategic.	Emphasizing the importance of preventive controls is crucial as it enables organizations to address risks proactively, preventing them from escalating into significant issues. This proactive stance is fundamental to effective risk management and aligns with best practices in internal control systems. The guidance on balancing preventive and detective controls offers a practical framework that helps organizations design an effective mix of controls, ensuring that risks are not only prevented but also detected and corrected in a timely manner. This balanced approach is essential for a robust internal control system, as it allows for both the anticipation of risks and the ability to respond when risks materialize.	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. Is the application guidance related to information technology in principles 10 and 11 sufficiently clear and understandable?	See response for #3.	Yes	Yes, the revised guidance on information technology is clear and appropriately detailed. The separation of IT-related control activities between principles 10 and 11 helps to clarify their specific roles and responsibilities within the internal control framework.	By emphasizing the importance of preventive controls, the guidance enables organizations to take a proactive approach to risk management, which is crucial for preventing issues before they escalate. This approach not only mitigates risks but also aligns with the best practices in internal control systems. The inclusion of a balanced perspective on both preventive and detective controls provides organizations with a practical framework to design a comprehensive mix of controls that are tailored to their specific operational needs and risk profiles. This balanced mix is vital for a robust internal control system, as it ensures that risks are managed comprehensively—preventing potential issues and detecting and addressing those that occur.	The application guidance is sufficiently clear and understandable.
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?	See response for #3.	Yes	Yes, the guidance on the information and communication component is clear and ensures that all relevant information supports the five components of internal control. This clarity enhances the overall effectiveness of information dissemination and communication within the entity.	By clarifying the role of relevant and quality information and effective communication, the guidance reinforces how these elements support all five components of internal control—control environment, risk assessment, control activities, information and communication, and monitoring activities. This approach is essential for maintaining the effectiveness and coherence of the internal control system. Information and communication are the backbone of any internal control system, facilitating the proper functioning and alignment of all other components. The detailed guidance on information requirements and communication processes is particularly valuable as it provides practical steps for ensuring that information is accurate, timely, and accessible. This ensures that all levels of the organization have the necessary information to perform their roles effectively and that there is a clear understanding of the internal control processes across the organization.	The application guidance is sufficiently clear and understandable.

CATEGORY	REVIEW QUESTION	DOL AGENCY RESPONSES - Agency 1	DOL AGENCY RESPONSES - Component Agency 2	DOL AGENCY RESPONSES - Component Agency 3	DOL AGENCY RESPONSES - Component Agency 4	DOL AGENCY RESPONSES - Component Agency 5
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?	See response for #3.	Yes. Separate Evaluations in 16.06 can be expanded to include special tests to see whether the established procedure generates desired results.	Yes, the guidance on the monitoring component is clear and comprehensive. It provides detailed instructions on evaluating internal controls, determining the scope and frequency of monitoring, and distinguishing between control and monitoring activities.	The revised application guidance on the monitoring component of internal control clarifies the role of monitoring activities in evaluating the effectiveness of the internal control system. The guidance ensures that all components of internal controls are continuously addressed, assessed, and improved as necessary. This approach is vital for maintaining the integrity and effectiveness of the internal control system. Monitoring is a dynamic component that provides feedback on the performance of all other internal control components, facilitating timely adjustments and continuous improvement. The detailed guidance on determining the scope and frequency of monitoring activities is particularly valuable as it helps management design an effective monitoring process that is tailored to their specific organizational needs and risk profiles. Additionally, the distinction made between control activities and monitoring activities in the guidance, along with practical examples of methods and tools for monitoring, provides insightful and actionable information. This helps organizations implement an effective monitoring system that not only detects and corrects inefficiencies but also aligns with strategic objectives and compliance requirements.	The application guidance is sufficiently clear and understandable.
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?	See response for #3.	Yes. Detective Control Activities in Appendix II can include findings from periodic financial audits performed by OIG or independent auditors. Furthermore, Sources of External Data in the same appendix can be expanded to include Treasury's Invoice Processing Platform (IPP) that is used by federal agencies to pay their invoices with private service providers.	Yes, the new appendixes are clear and very helpful. The examples of preventive and detective control activities provide practical insights, and the additional resources offer valuable guidance for addressing various risk areas effectively.	The inclusion of new appendixes in the guidelines indeed marks a significant enhancement in terms of clarity, usability, and practical application for management. By providing examples of preventive and detective control activities, the appendixes offer concrete, actionable guidance that can assist in the design and implementation of effective controls tailored to specific organizational needs and risk profiles. These examples serve as valuable tools for understanding how theoretical control principles can be applied in real-world scenarios, thereby facilitating more effective and efficient control environments. Moreover, the references to additional resources within these appendixes are crucial. They provide management with easy access to a broader range of information and best practices that can be leveraged to address specific risk areas and challenges. This not only enhances the organization's ability to implement robust controls but also supports ongoing education and improvement in internal control practices.	**The "Do Not Pay" and "Death Master File" titles should be capitalized in the visual.**