



August 26, 2024

Mr. James R. Dalkin  
Director, Financial Management and Assurance  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Dalkin:

**Subject: Standards for Internal Control in the Federal Government: 2024 Exposure Draft**

The American Institute of CPAs (AICPA) is the world's largest member association representing the CPA profession, with more than 400,000 members in the United States and worldwide, and a history of serving the public interest since 1887. AICPA members represent many areas of practice, including business and industry, public practice, government, education, and consulting. AICPA sets ethical standards for its members and U.S. auditing standards for private companies, not-for-profit organizations, and federal, state, and local governments. It develops and grades the Uniform CPA Examination, offers specialized credentials, builds the pipeline of future talent and drives continuing education to advance the vitality, relevance and quality of the profession.

On behalf of the AICPA and its Governmental Audit Quality Center, we appreciate the opportunity to comment on the U.S. Government Accountability Office (GAO) 2024 Exposure Draft (ED), *Standards for Internal Control in the Federal Government* (Green Book). Overall, the AICPA supports GAO's efforts to update the Green Book to: (1) emphasize additional risk areas; (2) continue harmonization with the Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control - Integrated Framework* (COSO); and (3) make other modifications to clarify the intent of certain requirements. However, we do have comments and recommendations for GAO to consider as it finalizes the Green Book. Our comments reflect feedback received from AICPA members with federal government audit experience.

The following section of this letter includes our responses to the questions for commenters where we have feedback. The second section of the letter includes our other comments and recommendations, and the final section provides our editorial suggestions.

**Responses to Certain Questions for Commenters Posed in the ED**

*Question 1. 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). Are these documentation requirements sufficiently clear and understandable?

*AICPA Response.* The documentation requirements are generally clear and understandable. However, we have the following comments and recommended changes:

- Paragraph 7.02 states: “Management identifies risks throughout the entity on a periodic and ongoing basis to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses. Periodic risk assessments are performed at specific times and at regular intervals, such as annually.” This guidance aligns with COSO, which requires an ongoing iterative process. However, GAO uses the plural “specific times” and the plural “regular intervals” but provides an example of “annually.” We recommend GAO revise the guidance to clarify its intent as to the frequency of “periodic.”
- The inclusion of the documentation requirements of paragraph 7.15 within the “*Response to Risks*” attribute suggests the documentation requirements are specific to that attribute rather than the entirety of Principle 7. We recommend that GAO include the documentation requirement within each attribute of Principle 7 (that is, *Identification of Risks*, *Analysis of Risks*, and *Response to Risks*).

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

*AICPA Response.* The guidance relating to the relevance of attributes is generally clear and understandable. However, we have the following comment and recommended changes:

- While paragraph OV2.08 states “These attributes are intended to help organize the application guidance management considers when designing, implementing, and operating the associated principles,” the same paragraph also states: “Other than the minimum documentation requirements, such guidance does not in itself impose a requirement.” Therefore, we believe it is unclear whether there is a *requirement* [emphasis added] for management to consider all attributes, which could lead to diversity in practice. We recommend GAO clarify the guidance accordingly, such as through the use of “should.” We also recommend that GAO clarify whether management should document its consideration of all attributes, similar to the following language used in paragraph OV2.06 related to the relevance of principles: “If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented and operated effectively.”

*Question 8. 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). Is the application guidance sufficiently clear and understandable?

*AICPA Response.* The guidance in paragraphs 9.10 and 9.11 relating to identifying risks related to change and responding to assessed risks related to a change is generally clear and understandable. However, GAO does not provide guidance as to how an entity *analyzes* the identified risks related to a change prior to responding to risk. Therefore, we recommend that GAO include guidance, similar to paragraphs 9.10 and 9.11, as to how an entity *analyzes* the identified risks related to a change.

*Question 13. 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). Is the application guidance sufficiently clear and understandable?

*AICPA Response.* The guidance relating to information and communication is generally clear and understandable. However, we have the following comment and recommendation:

- We recommend GAO add the following language, from the Information Quality section of COSO Principle 13, to Green Book Principle 13 to provide considerations about quality information coming from service organizations:
  - Information that is obtained from outsourced service providers that manage business processes on behalf of the entity, and other external parties on whom the entity depends, is subject to the same internal control expectations.
  - Information requirements are developed by the organization and communicated to outside service providers and other similar external parties. Controls support the organization's ability to rely on such information, including internal control over outsourced service providers such as vendor due diligence, exercise of right-to-audit clauses, and obtaining an independent assessment over the service provider's controls.

*Question 14. 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). Is the application guidance sufficiently clear and understandable?

*AICPA Response.* The guidance relating to the monitoring component is generally clear and understandable. However, we have the following comment and recommendation:

- Paragraph OV2.19 states: "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* [emphasis added.] While management may evaluate and incorporate recommendations from external auditors and the OIG, responsibility for an entity's internal control system resides with management." Footnote 9 within paragraph OV2.19 states: "An OIG is an independent component within an entity. *While an OIG is part of the entity's internal control system* [emphasis added], management of the OIG is responsible for internal controls within the OIG itself." The paragraph and footnote are contradictory in terms of the role of the OIG and whether it is or is not part of the entity's internal control system. This should be clarified by GAO.

*Question 15. 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. Are these new appendixes sufficiently clear and understandable?

*AICPA Response.* We support the inclusion of the new appendixes and believe they are generally clear and understandable. However, we offer the following comments and recommendations to enhance the appendixes:

- It is important for governmental entities to properly, and consistently, design and implement the Green Book framework, as intended. We agree that the examples of preventative and detective control activities included in Appendix II, *Examples of Preventive and Detective Control Activities*, will assist users of the Green Book who are responsible for designing, implementing and operating a system of internal control. While we recognize that it is not possible to illustrate all aspects of the components and relevant principles necessary for an effective system of internal control, we recommend that GAO consider including additional examples or develop a more holistic compendium of examples. Providing additional examples of components, relevant principles, controls, risks and other concepts included in the framework will further illustrate to governmental entities how principles may be present and functioning in an effective internal control environment.
- We also recommend GAO include examples addressing the completeness, accuracy and validity of information used in the performance of such controls. This would support the guidance in paragraph 10.16 and emphasize the importance of management developing its own procedures and controls over completeness and accuracy of data/reports produced from the information systems and their evolution as technology changes (for example, from completeness and accuracy over a point-in-time user listing used for a user access review evolving to completeness and accuracy over a tool or module for rolling user access reviews). Such examples should provide guidance for users to illustrate the evidence management should retain to demonstrate that they are using valid, complete and accurate information/data/reports for their controls (for example, report parameters, periodic reviews of query logic). Such an expanded appendix of examples would be consistent with similar compendiums provided within the COSO framework.
- The graphic on the first page of Appendix II includes the following examples of detective controls: 1) post-payment reviews, 2) reconciliations, 3) detective data analytics, 4) respond to reported risks and incidents, 5) controls over automated processes, and 6) malicious software detection. We recommend replacing “controls over automated processes,” which is a broad category of detective controls, with an example of a detective control over automated processes such as “information system logging” which is described further in Appendix II, in the subsection, *Examples of Preventive and Detective Control Activities*.” We also recommend providing a narrative description of “malicious software detection” within this subsection.
- Appendix III contains 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, and information security. As there are many requirements that governmental entities face regarding information systems management, financial management and execution of their respective missions, GAO should work closely with other federal agencies that also issue federal financial guidance or requirements to continue harmonization across such guidance and requirements and with COSO.
- GAO should consider whether Appendix III should reference non-governmental guidance, such as, COSO or the compendium of approaches and examples or other guidance that may also be relevant for governmental entities to design, implement and conduct an effective system of internal control.

## Other Comments and Recommendations

*Clarify Definition of Oversight Body.* Throughout the ED, the standards refer to “oversight body” and the responsibilities of such. Paragraph OV2.17 provides a definition of the “oversight body.” We recommend the GAO update the definition to include examples of who would be considered the “oversight body” to provide consistency in application across federal agencies.

*Precision and Timeliness Enhancements.* Throughout Principles 10, 11, and 12 there is reference to the “precision” and “timeliness” of a control. As the definitions of precision and timeliness are proven challenges for federal entities, we recommend GAO include an example in the Green Book, similar to the examples in COSO, to aid entities in understanding and properly addressing these topics.

*Revise References to External Audits.* Throughout the ED there is reference made to “external audits” in the context of various scenarios. To avoid entities solely relying on external audits, we recommend revising the reference to “external audits” to “internal and external audits.” This will help ensure entities understand their responsibilities for their requirements and results under OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

*Level of Needed Commitment to Integrity and Ethical Values.* Paragraph 1.01 describes Principle 1 and states “The oversight body and management should demonstrate a commitment to integrity and ethical values.” However, this seems inconsistent with the notion that the *entire organization* [emphasis added] needs to demonstrate a commitment to integrity and ethical values as described in:

- Paragraph 1.03 which states “...*personnel throughout the entity* [emphasis added] play an important role in setting the tone that permeates the organizational culture.”
- Paragraph 1.09 which states “...The oversight body evaluates management’s adherence to the standards of conduct *as well as the overall adherence by the entity* [emphasis added].”

*Oversight Structure Determination Responsibility.* Within Principle 2, we suggest GAO clarify its intent as to who has the responsibility for determining the oversight structure. Paragraph 2.02 states: “The entity determines an oversight structure...”, whereas paragraph 2.09 states: “The oversight body’s responsibilities for the entity’s internal control system include the following: ...establish oversight structure ...”

*Move Language Regarding Oversight Structure.* We recommend moving the following language from paragraph 2.08 within the *Oversight Structure* attribute to within the *Oversight for the Internal Control System* attribute: “Members of an oversight body scrutinize and question management’s activities, present alternative views, and act when faced with obvious or suspected wrongdoing.”

## Editorial Comments

We recommend the following revisions to the referenced paragraphs below to improve the readability of the Green Book.

*Paragraph OV2.08.* “The Green Book also contains application guidance organized into categories, or in the form of attributes. ~~These attributes are intended to help organize the application guidance management~~ Management considers these attributes when designing, implementing, and operating the associated principles.”

*Paragraph OV2.10.* “Management establishes control activities through policies that document ~~by documenting expectations in policies what is expected and in~~ through procedures that document specified actions.”

*Paragraph OV2.23.* “Operations objectives relate to achievement of operations that achieve an entity’s mission, strategic plan, goals, and objectives. including program, financial, and administrative goals. ~~An entity’s mission may be defined in a strategic plan. Such plans set the goals and objectives for an entity along with the effective and efficient operations necessary to fulfill these objectives.~~” We recommend these revisions to align with paragraph OV1.03.

*Paragraph OV2.26.* “In the government, ~~objectives related to compliance with applicable laws and regulations are significant~~ may have a significant impact on the achievement of objectives. Laws and regulations often prescribe a government entity’s objectives, structure, methods to achieve objectives, and reporting of performance relative to achieving objectives. Management considers objectives in the category of compliance comprehensively for the entity and determines what controls are necessary to design, implement, and operate for the entity to achieve these objectives effectively.”

*Paragraph OV4.01.* “External parties may include suppliers, contractors, service organizations, regulators, federal entities, state and local governments, grantees, and the public. Management interacts with external parties regarding matters impacting the functioning of the internal control system. Service organizations are external parties ~~can be service organizations~~ that manage business processes on behalf of the entity or other parties interacting with the entity. ~~External parties may include suppliers, contractors, service organizations, regulators, federal entities, state and local governments, grantees, and the public.”~~”

*Paragraph OV4.03.* “Management may contract with ~~engage~~ external parties to develop and perform certain business ~~processes~~ process controls that help achieve the entity’s control objectives for the entity, such as controls over 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 the Green Book, these external parties are referred to as service organizations. Service organization controls are part of the entity’s internal control system. Management, ~~however,~~ retains responsibility for the performance of controls over processes assigned to service organizations and identifying, analyzing, and responding to associated risks. Therefore, management should ~~needs to~~ understand the controls each service organization has designed, has implemented, and operates for the assigned business process ~~and how the service organization’s internal control system impacts the entity’s internal control system.”~~”

*Paragraph 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.~~ Complementary user entity controls are those controls that service organization management identifies as necessary for the user entity to implement in addition to controls the service organization performs to achieve its control objectives. 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’s control objectives.”

*Paragraph OV4.07.* “Information technology may be essential to achieving the entity’s objectives and better controlling its business processes. Entities and individuals are ~~becoming more~~ interconnected using information technology, while types of information technology and the ways it is used ~~are~~ evolve rapidly evolving.”

*Paragraph OV4.10.* “Management allocates appropriate resources, including personnel, to maintain and secure the entity’s information technology.”

*Paragraph OV4.16.* “Management decides how an entity evaluates the costs versus benefits of various approaches to implementing an effective internal control system. However, cost alone ~~is~~ may not be an acceptable reason to avoid implementing internal controls. Management is responsible for meeting internal control objectives. The costs versus benefits considerations support management’s ability to effectively design, implement, and operate an internal control system that balances allocating resources with the degree of risk, complexity, or other factors relevant to achieving the entity’s objectives.”

*Paragraph 1.09.* “Management uses established standards of conduct as the basis for evaluating adherence to integrity and ethical values across ~~the organization. Management evaluates the adherence to standards of conduct across~~ all levels of the entity.”

*Paragraph 1.10.* “Management determines the tolerance level for deviations. Management may determine that the entity will have zero tolerance for deviations from certain expected standards of conduct, while deviations from others may be tolerated. ~~addressed with warnings to personnel~~. Management establishes a process for evaluations of individual and team adherence to standards of conduct that escalates and remediates deviations ~~Management addresses deviations from expected standards of conduct~~ timely and consistently. Depending on the severity of a deviation determined through the evaluation process, management, with oversight from the entity’s oversight body, takes appropriate actions, such as warnings to personnel, and may also need to consider applicable laws and regulations in its determination of appropriate actions to take. The standards of conduct to which management holds personnel, however, remain consistent.”

*Paragraph 2.02.* “The entity determines an oversight structure to fulfill responsibilities set forth by applicable laws and regulations, relevant government guidance, and feedback from key stakeholders. The entity will select, or if mandated by law will have selected for it by an applicable body, an oversight body. When the oversight body is composed of entity management, activities referenced in the Green Book as performed by “management” exclude these members of management when in their roles as the oversight body.”

*Paragraph 3.12.* “~~Some~~ An appropriate level of documentation, however, is necessary so that the components of internal control can be designed, implemented, and operating effectively.”

*Paragraph 5.50.* “Management holds service organizations accountable for their assigned internal control responsibilities. Management may contract with service organizations to perform roles in the organizational structure. However, management remains accountable for overseeing the service organization and is ultimately accountable for the service organization’s internal control responsibilities.”

*Paragraph 7.13.* “After designing risk responses, management then considers residual risk. ~~The risk response need not necessarily result in the least amount of residual risk. But where~~ Where a risk response would result in residual risk exceeding defined risk tolerances, management revisits and revises the response. Operating within the defined risk tolerance provides greater assurance that the entity will achieve its objectives.”

*Paragraph 7.15.* “This includes, but is not limited to, documentation of the consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system.”

*Paragraph 10.04.* In both the narrative text and Figure 6 we suggest the following revision:

- ~~Proper execution~~ Authorization and approval of transactions
- ~~Control activities over~~ Accurate accurate and timely recording of transactions

*Paragraph 10.09.* “Control activities can be either preventive or detective. ~~The main difference between preventive and detective control activities is timing, that is, when the control activity occurs within an entity’s operations.~~” We believe this sentence is not necessary as the description of preventive and detective controls that follows in paragraph 10.09 is sufficient.

*Paragraph 12.02.* “Management establishes control activities through policies that document ~~by documenting expectations in policies what is expected and in~~ through procedures that document specified actions.”

*Paragraph 12.03.* “Management documents in policies and procedures for each unit its responsibility for a business process’s objectives and control activity design, implementation, and operating effectiveness. Doing so mitigates related risks to acceptable levels. Each unit, with guidance from management, determines the policies and procedures necessary to operate the process based on the objectives and related risks for the business process. Each unit also documents policies and procedures in the appropriate level of detail to allow management to effectively monitor the control activity. The documentation may appear in various forms, such as management directives, administrative policies, or operating manuals.”

*Paragraph 12.05.* “A new law or regulation may change an entity’s objectives or how an entity is to achieve an objective. Further, in the federal environment, this may occur through government-wide policy or guidance issued by other federal agencies with regulatory or oversight responsibilities ~~the Office of Management and Budget or the Department of the Treasury.~~” As written, this sentence suggests that the OMB and the Department of Treasury are the only entities that issue government-wide policies or guidance. We suggest revising this sentence to clarify that agencies with regulatory or oversight responsibilities may issue such policies or guidance.

*Paragraph 13.02.* “Management designs information systems to achieve ~~a process that uses the entity’s objectives and related risks to identify the information requirements needed to achieve~~ the entity’s objectives, address ~~the related~~ risks, and support the five components of internal control. Information requirements consider the needs of both internal and external users. Management defines the identified information requirements at the relevant level and requisite specificity for appropriate personnel.”



*Paragraph 13.06.* “Management develops information systems to obtain, generate, and process ~~large volumes of~~ relevant data into quality information to meet the identified information requirements and support the internal control system.”

*Paragraph 14.08.* “Management ~~periodically~~ evaluates the entity’s methods of communication on a periodic and ongoing basis so that the organization has the appropriate tools to communicate quality information.”

*Paragraph 16.05.* “Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, trend analysis, data analytics, activities to identify improper payments or potential fraud, testing, and other routine actions.”

*Paragraphs 16.06 and 16.07.* We suggest reordering the narrative as follows to separate the concepts of 1) separate evaluations, and 2) scope and frequency of evaluations.

16.06 Management uses separate evaluations to monitor the design and operating effectiveness of the overall internal control system at a specific time or of a specific function or process. Management also uses the results of separate evaluations performed in connection with external audits, investigations, and other evaluations that may involve the review of control design and direct testing of internal control to help identify issues in the internal control system. These audits and other evaluations may be mandated by law and are performed by internal auditors, external auditors, inspectors general, and other external reviewers.

[New paragraph] Separate evaluations include observations, inquiries, reviews, improper payment estimates, and other examinations, as appropriate. These evaluate whether controls to effect principles across the entity are designed, implemented, and operating effectively. Separate evaluations may also take the form of self-assessments, which include cross-operating unit or cross-functional evaluations. Separate evaluations provide greater objectivity when performed by reviewers who do not have responsibility for the activities being evaluated.

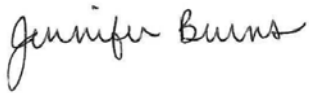
[New paragraph] The scope and frequency of separate evaluations depend primarily on the assessment of risks, risk responses, evolving technology, identification of new risks or deficiencies, results of ongoing monitoring, and rate of change within the entity and its environment. Management may ~~also~~ increase the frequency of separate evaluations when management rapidly implements a new program or substantially changes an existing one, such as emergency assistance programs.

*Paragraph 17.02.* “Personnel report internal control issues through established reporting lines to the appropriate internal and external parties on a timely basis to enable the entity to promptly evaluate and respond to those issues.”

Mr. James R. Dalkin  
August 26, 2024  
Page 10

We appreciate the opportunity to provide our feedback on the proposed changes to the Green Book for consideration by GAO. If you would like to discuss our feedback or have any questions, please feel free to contact us.

Sincerely,



Jennifer M. Burns  
AICPA Chief Auditor



Mary M. Foelster  
Senior Director  
AICPA Governmental Auditing and Accounting