National Association of State
Auditors, Comptrollers
and Treasurers

NASACT

Headquarters Office
449 Lewis Hargett Circle, Suite 290
Lexington, KY 40503-3590
P (859) 276-1147, F (859) 278-0507
www.nasact.org

Washington Office
The Hall of the States
444 N. Capitol Street, NW, Suite 548
Washington, DC 20001
P (202) 989-6801, F (202) 989-6804

August 19, 2024

U.S. Government Accountability Office
441 G St. N.W.
Washington, DC 20548

To Whom it May Concern:

On behalf of the National Association of State Auditors, Comptrollers and Treasurers (NASACT), representing the nation's top state financial leaders, we are pleased to provide the following comments on proposed revisions to the *Standards for Internal Control in the Federal Government* (Green Book).

We applaud GAO for prioritizing revisions to the Green Book related to preventive controls. Throughout the pandemic, our members were at the forefront of administering the federal government's financial response to the pandemic. This included implementing controls in accordance with evolving guidance and identifying fraud, waste, and abuse along with significant control deficiencies in emergency assistance programs. We also appreciate GAO's recognition of the growing cybersecurity threats not only in frequency but in sophistication as well.

Following this letter, you will find a complete summary of our comments, with responses to specific questions contained within the proposed revisions to the Green Book. We appreciate the time and effort put into revising this important document. We look forward to a continued dialogue on the proposed revisions and believe that the best way to achieve the stated objectives is to consider the views of all affected parties.

Should you have any questions or wish to discuss our comments further, please contact our Deputy Executive Director Josh Winfrey [redacted]. I may also be reached directly at [redacted].

Sincerely,

Greg S. Griffin
State Auditor of Georgia
NASACT President, 2023-2024

Comments from NASACT: *Standards for Internal Control in the Federal Government, 2024 Revision*

Requests for Comment

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?*

   Overall, we believe the documentation requirements are sufficiently clear and understandable. However, we believe the language in paragraph 07.02 that dictates the frequency of periodic risk assessments should include a minimum amount of time between each formal risk identification process. Currently, the language states, "such as annually" which reads more like an option than a requirement. Setting an expectation of every two years would still provide flexibility for entities to more frequently identify risks as needed but also ensure that a significant amount of time does not lapse between assessments.

   To ensure the documentation burden is proportionate to the risks, the Green Book should make it clear that the proposed requirements around identification and documentation of risks should only apply to applicable risks. For example, the Yellow Book requires auditors to assess the risks of fraud and information systems controls in every performance audit but acknowledges these aspects may not be significant. The same consideration should be present in the Green Book.

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?*

   We agree that the application guidance relating to management's consideration of the relevance of attributes is sufficiently clear and understandable.

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

   Overall, we feel the guidance related to collaboration and responsibilities within the internal control system is sufficiently clear and understandable. However, clarification of the term "oversight body" is needed. The Yellow Book uses the term "those charged with governance" and we are familiar with this term in the context of audits. The Green Book should declare whether these terms are synonymous or clearly define and explain the differences between the two within the document.

4. ***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).*

Is the application guidance sufficiently clear and understandable?

Overall, we agree the application guidance is sufficiently clear and understandable but ask for certain additional clarifications and considerations.

In many cases in the state government environment, 'external parties' could include another agency within the same government which performs services such as payroll, accounting, etc. We request the definition of external parties, which is used throughout the draft, be expanded to emphasize the importance of relevant risks and internal controls in these situations.

In OV4.05, we recommend adding guidance around when management should consider obtaining a System and Organization Controls (or SOC) report as part of its oversight for the business processes assigned to the service organization.

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

   We agree the application guidance is sufficiently clear and understandable.

6. ***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). 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?*

   We agree that the additional requirement and related application guidance is sufficiently clear and understandable. Specific to the requirement for assessing risks of improper payments, we ask that an illustration, possibly even a Venn diagram, be included to provide additional guidance and examples of improper payments, fraud, waste, and abuse as the requirements and application guidance for each of these situations are different across professional standards.

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

   We agree the application guidance is sufficiently clear and understandable.

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?*

   We agree the application guidance is sufficiently clear and understandable.

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

We agree the application guidance is sufficiently clear and understandable.

10. ***Categories of Control Activities:*** *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?*

    We agree the categories of control activities are sufficiently clear and understandable.

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

    We agree the application guidance is sufficiently clear and understandable.

12. ***Changes Related to Information Technology:*** *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?*

    Overall, we agree the application guidance related to information technology in principles 10 and 11 is sufficiently clear and understandable. In 11.16, GAO should consider segregating the implementation of the controls from the design of the controls. The implementation is expounded on in Principle 12, but the distinction could be made in 11.16 as well.

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?*

    We agree the application guidance is sufficiently clear and understandable.

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?*

    Overall, we agree the application guidance is sufficiently clear and understandable. We point back to our response to question 1, **New Documentation Requirements,** and request a minimum amount of time be prescribed by GAO between each formal risk identification process.

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?*

    We appreciate greatly and applaud GAO on the additions of appendixes to help users understand

the guidance. We have several recommendations related to the appendixes.

Appendix II

- We recommend adding non-IT related examples of preventive and detective controls such as segregations of duties.
- GAO also should add additional context to the 'Automated Approvals' Control to make clear these are for transactions under a certain dollar amount or that are lower risk for some other reason to avoid conflicting with the 'Proper Execution of Transactions' guidance.
- For the 'Reconciliation', we believe bank reconciliations are a significant enough control that it should be named in this section as an example.
- The 'Sources of External Data' seems out of place and would perhaps be better suited to Appendix III 'Additional Resources'.
- There are two external-to-GAO hyperlinks included in the footnotes on page 119 which could be obsolete at some point in the future.

Appendix III

- While this appendix is helpful, it may be more efficient to link to a website hosted by GAO that can be updated as needed rather than including these resources in the Green Book proper.

COMMENTS IN ADDITION TO THE LISTED REQUESTS FOR COMMENT

Principles 10 and 11 in Control Activities

We are concerned with the deemphasis of the role of control activities in achieving an organization's objectives. Specifically, principles 10 and 11 within the Control Activities component of internal control are worded in such a way as to define control activities as risk mitigation tools rather than tying them to actual organizational objectives. Given that the Green Book is referenced by both the Yellow Book and the Uniform Guidance, we are concerned with the implication that control activities would be evaluated based on management's risk assessment *and risk tolerances* rather than directly against objectives. For example, while an auditee's current control activities may be sufficient to mitigate risks to meet the auditee's current risk tolerances, a performance auditor may identify recommendations for far greater efficiency or effectiveness. This could create a situation in which the auditee deems their control activities "good enough" in relation to their risk tolerance, but compared to a program's objectives, the audit report may still include an audit finding related to opportunities for increased program efficiency and effectiveness.

A possible revision to address this concern would be to reword principles 10 and 11. Principle 10 might be worded as, "Management should design control activities to **mitigate risks to acceptable levels** and to achieve the entity's objectives". Principle 11 might be reworded as, "Management should design general control activities over information technology to **mitigate risks to acceptable levels** and to achieve the entity's objectives.

Definition of Risk Tolerance and Management Objectives

In paragraph 06.04, it would be helpful to have an example of measurable objectives to flesh out this concept.

In paragraph 6.09, it is stated that the concept of risk tolerance does not apply to compliance objectives because an entity is either compliant or non-compliant. For auditors performing Single Audits or even for grantees administering federal programs, the concept of risk tolerance for compliance is pervasive and is often based on materiality, the likelihood of noncompliance, and the nature of possible instances of noncompliance. GAO should consider revising paragraph 6.09 to account for this reality in practice.

Other Comments

- Consider adding an illustration to tie attributes to Figure 3 on page 25 so that the relationship between components, principles, *and* attributes is visualized as well.