



Advance. Grow. Accelerate.

August 23, 2024

Government Accountability Office  
441 G Street NW  
Washington, DC 20548

RE: Comments on *Standards for Internal Control in the Federal Government* (Green Book), 2024  
Exposure Draft

The Financial Management Standards Board (FMSB) of the AGA appreciates the opportunity to provide comments on the Government Accountability Office's proposed standards. Our responses to the questions asked by the Government Accountability Office, along with other comments on the revisions, are included below:

**Question 1: New Documentation Requirements**

We are supportive of the new documentation requirements. However, we found it confusing that documentation requirements are located within attributes. For example, paragraph 7.15 is located within the "response to risk" attribute, but appears to also apply to other attributes. In any case, it would be preferable if application guidance could be clearly separated from requirements. For these reasons, we suggest moving documentation requirements to the section describing the principle, or to a separate section.

**Question 2: Relevance of Attributes**

We found this new application guidance to be unclear. Specifically, paragraph OV2.08 provides a description of the purpose of attributes and states that they are not requirements. However, it is unclear whether paragraph OV2.09 is intended to create a presumption that management use attributes as criteria to assess whether internal controls are designed, implemented and operating in conformity with principles. It is further unclear whether the reference to attributes in paragraph OV3.10 is intended to convey a requirement to consider attributes when making a summary determination about principles. In other words, are attributes relevant as a sort of presumptively mandatory requirement to consider because they "support" the principles? Or are attributes only relevant to help understand the intent of the principles because they serve to organize application guidance and make it easier for readers to navigate and relate it to the principles? We suggest explaining the relevance of application guidance in a way that is similar to the Yellow Book.

**Question 3: Collaboration and Responsibility within the Internal Control System**

We found this application guidance to be sufficiently clear and understandable.

However, we notice the term “oversight body” is used throughout the Green Book, whereas the Yellow Book uses the term “those charged with governance.” While we assume these terms are synonymous, it would be helpful if either the same term was used in both sets of standards, or if the definitions of these terms could explicitly clarify that they are the same (or if not, how they are different).

#### **Question 4: External Parties**

We found this application guidance to be sufficiently clear and understandable.

#### **Question 5: Application Guidance in the Risk Assessment Component**

We are supportive of this application guidance, but found certain aspects to be unclear. Some members were unclear as to the difference between “specific times” and “regular intervals” since use of the word “and” rather than “or” in paragraph 7.02 implies that periodic risk assessments are performed at both specific times and regular intervals. Also, some members were unsure how strongly “such as annually” was being suggested by the application guidance in paragraph 7.02. This uncertainty is due to several factors, including (1) perceived ambiguity regarding the degree to which attributes are to be used to determine compliance with the framework as discussed in our response to question 2, (2) differences between paragraph 7.02 and paragraph 16.04, and (3) having only one example given with little further guidance about how to establish frequency. Some members suggested curing this uncertainty by clearly establishing or recommending a minimum frequency for periodic risk assessments. Alternatively, application guidance could be expanded to provide more examples or discussion of factors to consider in determining the scope and frequency of periodic risk assessments. For example, if an annual frequency is suggested due to OMB A-123 guidance, it may be helpful to describe this in a footnote in order to clearly convey the source or intent of this suggestion to nonfederal entities.

#### **Question 6: Added Requirement to Assess Improper Payment and Information Security Risks**

We agree that these added requirements are appropriate. We also found the application guidance to be sufficiently clear and understandable.

#### **Question 7: Assessing Fraud Risk**

We found this application guidance to be sufficiently clear and understandable.

#### **Question 8: Identifying and Responding to Significant Changes**

Principle 9 requires management to identify, analyze and respond to significant changes, consistent with the general Principle 7. We were therefore unclear why the documentation requirement and related application guidance only address identification and response, but not analysis. See also our response to question 1.

#### **Question 9: Discrete Processes to Manage Certain Entity Risks**

We are supportive of this application guidance to describe how certain controls may be commonly or best implemented as discrete processes at different levels of the organization.

However, we found it unclear how this new application guidance relates to extant guidance on entity-level control activities (as defined in paragraphs 10.12 through 10.14 and the glossary). Application guidance could be improved by either using a consistent term and set of examples (if new guidance is intended to describe the same concept as entity-level controls), or by better distinguishing these as different concepts.

#### **Question 10: Categories of Control Activities**

We found the categories of “proper execution of transactions” and “accurate and timely recording of transactions” to be somewhat confusing, since these titles appear to be describing a control objective more than a control activity. Proper execution might be better titled as “authorizations and approvals,” similar to COSO. In contrast, the explanation of accurate and timely recording did not appear to describe a separate category of control activities.

In addition, some members were not clear how this list relates to the list in Appendix II and suggested a single list of example controls, preferably located in the appendix.

#### **Question 11: Prioritizing Preventative Control Activities**

We found this application guidance to be sufficiently clear and understandable.

#### **Question 12: Changes Related to Information Technology**

We found this application guidance to be sufficiently clear and understandable.

However, we are aware of a variety of cybersecurity control frameworks used by state and local governments. For example, NIST standards are described in Appendix III. We also note that cybersecurity controls, risks and terminology have been continuously evolving, necessitating frequent updates of these frameworks. It may be helpful to acknowledge that different cybersecurity control frameworks exist and may use different terminology or categories of controls than those used in the Green Book.

#### **Question 13: Focus of Information and Communication Component**

We found the change in how these principles are described to be sufficiently clear and understandable.

#### **Question 14: Monitoring Component**

We found the change in how these principles are described, and related application guidance, to be sufficiently clear and understandable.

#### **Question 15: New Appendixes**

Regarding Appendix II, we noticed that the graphic on page 112 displays examples of preventative and detective controls that do not match the subsequent narrative. Specifically, the list of preventative controls in the graphical display does not include logical access control activities and physical access control

activities, but does include password management, network security, and authentication controls. Similarly, the list of detective controls in the graphical display does not include information security logging, but does include controls over automated processes and malicious software detection.

We also believe the description of the “automated approvals” preventative control could use additional clarity to either relate or distinguish it from preventative data analytics. This clarity could be provided by describing the rules or coding (that is, how the automation provides control); for example, as comparison of transactions against a set of established requirements such as authorization limits, edit checks, data matches, or risk scoring factors. Alternatively, automated approvals could be described as a potential application of preventative data analytics.

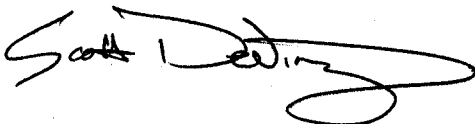
Finally, although we appreciate the inclusion of Appendix III information about additional resources, we are concerned it might become outdated in future years. Unless the GAO is planning to update the Green Book on a more frequent basis, we suggest moving the list and description of resources to a referenced website that could be updated by GAO as needed.

#### **Other Comments**

We found the new guidance in paragraph OV1.04 and the new glossary term “controls” to be somewhat confusing. We also found the definition of internal control system in paragraph OV1.05 and the glossary as a “continuous built-in component of processes” to be (1) somewhat confusing, (2) potentially contrary to the definition of internal control (as “a process” rather than a “built-in component of processes”), (3) potentially contrary to guidance in paragraph OV1.06 (that internal control is not a separate system), and (4) potentially contrary to the definition of “component.” We would suggest that not all of this content may be necessary or meaningful. We further suggest that the glossary term for “controls,” if needed, might be clearer if it were the same definition as used by COSO.

Finally, our group had mixed views on the change in the definition of control activities. We understand the desire to more closely converge with COSO definitions, and some members preferred the new language. Other members were concerned that it was less straight-forward and could be problematic, especially in the context of Yellow Book performance audits.

Sincerely,

A handwritten signature in black ink, appearing to read 'Scott DeViney', with a large, sweeping flourish at the end.

Scott DeViney, CPA  
Chair, Financial Management Standards Board



Advance. Grow. Accelerate.

AGA  
Financial Management Standards Board

The FMSB comprises the following 21 members with accounting and auditing backgrounds in federal, state, and local government, as well as academia and public accounting. The FMSB reviews and responds to proposed standards and regulations of interest to AGA members. The purpose of the FMSB is to advocate for the improvement of accounting and financial reporting standards at all levels of government and thus advance government accountability. The views of the FMSB do not necessarily represent those of AGA. Local AGA chapters and individual members are also encouraged to comment separately.

Scott DeViney, Chair  
Craig Murray, Vice Chair  
Crystal Allen  
Orinda Basha  
Eric Berman  
Gerry Boaz  
David Cook  
Jim Dawson  
Christopher Goeman  
Simcha Kuritzky

Qi Li  
Dean Michael Mead  
Lealan Miller  
Mickey Moreno  
Audrea Nelson  
Kerrey Olden  
Mark Reger  
Stacie Tellers  
John Troyer  
Brittney Williams  
Ann Ebberts, CEO, AGA