



**Office of the Washington State Auditor
Pat McCarthy**

August 26, 2024

Via Electronic Mail

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

RE: Response to GAO Exposure Draft – *Standards for Internal Control in the Federal Government* (Green Book)

The Office of the Washington State Auditor appreciates the opportunity to provide input to the GAO on this important exposure draft. In our constitutional role as the auditor of public accounts for the State of Washington, our Office performs over 1,300 financial audits, single audits, performance audits, and attestation engagements for state agencies and local governments of all types in Washington.

We support the Green Book and applaud the efforts of GAO to continue to improve guidance on internal control in the government environment. Our comments on the Discussion Questions for Responses and other matters are as follows:

Change in definition of control activities

We object to the change in the definition of control activities from designing controls “to achieve objectives and respond to risks” to designing controls “to mitigate risks to achieving objectives to acceptable levels” for principles 10 and 11 and in Appendix I. This change implies that the control activities component is only a corollary to risk assessment, rather than retaining it as a separate, but interrelated component. While we understand the intent is to more closely align with COSO’s definition, we think the current definition in the Green Book is more practical and superior for the following reasons:

- In practice, controls are commonly designed and operated to achieve a specific positive (objective) rather than mitigate a negative (risk). While this could potentially be conceptualized as risk mitigation, it is much more easily understandable as an activity designed to ensure reasonable assurance that an objective is reached.
- In practice, the risk assessment component is rarely precise enough to be relied upon as the sole driver of control activities, especially in cases where the nature of the activity is new or unpredictable. In our opinion, this is not a deficiency in risk assessment but rather

an inherent limitation, which is why risk assessment is only one component of an interrelated system of internal control.

- In practice, control activities are often designed and performed by different organizational units and executed at different times than the risk assessment component. This makes it challenging to presume that control activities are solely a response to risk assessment and tolerances. While it could be imagined that the risk mitigation envisioned in the control activities definition is inclusive of proactive and speculative consideration of “what could go wrong” by personnel at all levels, we would point out that this is not how the risk assessment component is described in the model.
- Given that the Green Book is referenced by Yellow Book performance audit standards and Uniform Guidance for Single Audits, 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 current performance may be within the entity’s current risk tolerances, a performance audit may identify recommendations for far greater efficiency or effectiveness. When compared with management’s risk assessment and risk tolerance it is “good enough” but when compared to the entity’s objective there would be an audit finding.

We noticed that while some sections still maintain language on use of control activities to achieve objectives, in other sections this is deemphasized. We do not see a clear reason to change this language to depart from the overarching definition of internal control, given that this is the most common point of reference for auditors.

1) Documentation requirements in 7.15 and 9.08

We agree with the requirement to document the results of risk assessment.

However, we do not agree with requiring documentation of the process for responding to significant changes. In practice, we find that a documented process for *identification* and *analysis* of changes is necessary to ensure this occurs. However, we find that the nature of change means that the process for *responding* to changes can be highly variable, rendering a documented process ineffective or even counterproductive for certain types of changes or risks. For example, whereas responses to some types of predictable changes should be established as control activities (such as program change controls over software), many other types of changes and responses will require cross-functional teams, executive intervention, external advocacy or a combination of efforts that are unique to the circumstance rather than following a pre-established, documented process.

We agree with the new requirement to document specific consideration of fraud, improper payments and information security at the entity level. However, performance audits are often conducted at lower levels of the organizational structure and focused on a narrow objective where such considerations would not be relevant. For example, for an organizational unit or objective does not involve making payments, then improper payments would not be relevant. Although an audit should document these considerations even if it is obvious, we would not expect an entity’s system of controls to document consideration of these risks at every organizational level or for every objective when they are clearly irrelevant.

2) Relevance of attributes in OV2.08-09 and OV3.10

It would be preferable if application guidance could be clearly distinguished from requirements. Since they are mixed, the list of documentation requirements in Appendix I is particularly helpful.

3) Collaboration and responsibilities in OV1.07, OV2.17, 1.03-04, and 16.10

We agree with this application guidance. However, the term “oversight body” is used throughout the Green Book, whereas the Yellow Book uses the term “those charged with governance.” It is unclear whether these terms are intended to be the same. For this reason, it would be helpful if either the same term was used or if the definitions of these terms (such as in paragraph OV2.17) could explicitly clarify whether they are the same, and if not, how they are different.

4) External parties in OV4.01-06, 10.04 and 15.03-04

We agree with this application guidance.

5a) Periodic and ongoing risk assessments in 7.02, 7.07, 8.03, and 9.02 through 9.03);

We agree with this application guidance.

5b) Internal and external risk factors in 7.04-05, 8.05, 8.07, 8.12, and 8.15-16

We agree with this application guidance.

5c) Risk identification methods in 7.06 and 8.04

We agree with this application guidance.

5d) Evaluating residual risk in 7.03 and 7.13

We agree with this application guidance.

6a) Added requirement to assess improper payments in 8.01-05, 8.11-13

Adding a specific requirement to assess risk of improper payments may make sense for federal agencies. However, non-federal entities may not consider improper payments as a separate and distinct category. In any case, this appears to introduce a significant overlap with existing categories of fraud, waste and abuse. It would be helpful if a Venn diagram or other visual could be included to help distinguish between fraud, waste, abuse and improper payments. This is important because each category is attached to different requirements and application guidance in the Green Book and Yellow Book.

With regard to paragraph 8.11, we find that waste and deficiencies in internal control design are also potential causes for improper payments. We also noted that the term “mismanagement” was used only in paragraph 8.11 and were unsure how it would be distinguished from lack of

oversight, errors or deficiencies in the design of internal controls, or whether this was intended to describe a form of misconduct other than abuse or waste.

6b) Added requirement to assess information security risks in 8.14-20

We agree with this added requirement.

7) Assessing fraud risk in 8.06-07

We agree with this application guidance.

8) Identifying and responding to significant changes in 9.06 and 9.08-12

As explained in our response to question 1, we do not agree with adding a requirement to document the process for responding to significant changes. Instead, we think it would be more appropriate to require a documented process to *identify* and *analyze* changes - that is, the periodic process described in paragraphs 7.02-06.

9) Discrete processes to managing certain entity risks in 3.03, 7.12 and 8.20

This application guidance was not entirely clear and could be improved by using a consistent term and set of examples. We would have assumed these sections are referring to entity-level control activities, which are well-described in paragraphs 10.12-14 and are defined in the glossary as including controls related to risk assessment, control environment, service organizations, management override and performance or analytical reviews. However, paragraphs 3.03, 7.12 and 8.20 do not cite or use the term entity-level control activities. Moreover, only paragraph 8.20 refers to general controls, which is not currently included as an example of entity-level control activities although it is described in a similar way.

10) Categories of control activities in 10.04

Listing types of control activities is always helpful. However, it was not clear how this list relates to the list in Appendix II. If retained, it would be helpful if paragraph 10.4 could be divided into multiple numbered sections, as it is excessively long and therefore difficult to reference or cite.

We did not have concerns with examples of control activities, other than the section on management of human capital, which seemed duplicative of the control environment component.

11) Prioritizing preventative controls in 10.09-11

We agree with this application guidance.

12) Changes related to information technology in 11.01 and 11.02-17

The description of logical access controls in paragraph 11.11 groups user access controls for applications with those for networks. However, we would normally consider user access controls at the application level to be application controls rather than general controls.

We found the following sentence in paragraph 11.14 to be unclear: “Vulnerability management is the process of identifying system vulnerabilities where change may be necessary for remediation.” This definition is circular since it uses the term within the definition. It also lacks a response to identified vulnerabilities, which we see as necessary in order to be considered a control activity. This could be re-worded as: “Vulnerability management is the process of identifying security or system weaknesses and establishing a process for remediation.”

In paragraph 11.16, we would suggest “implementing” as a duty that should be segregated from designing. We would normally consider someone who can both change a program and implement the change to be a risk.

13) Focus of information and communication in 13.01-02, 14.01, 14.03 and 15.01

We agree with this application guidance.

14a) Evaluating whether components are present and functioning in 16.02 and 17.07

We agree with this application guidance, which is consistent with paragraph OV2.06.

14b) Scope and frequency of monitoring activities in 16.06

We found the first sentence of this section to be awkwardly phrased, but otherwise agree with this application guidance.

14c) Example methods and tools for monitoring activities in 16.04-06

We agree with this application guidance.

15a) New appendix II

Listing types of control activities is always helpful, and we did not have any concerns with the specific examples provided in the appendix.

However, it was not clear how this list in the appendix was related to the list in paragraph 10.4. Also, we noticed the examples of preventative and detective controls listed in the graphic did not match the list in the narrative. Finally, it was also not clear why the section on external data sources was included, or why this was limited to only two examples. These two examples have highly specific information and hyperlinks that may become obsolete prior to publishing the next Green Book.

15b) New appendix III

Appendix III includes valuable information. However, we would suggest this list of resources, as well as the examples of external data sources, might be better delivered as a GAO website that can be linked from the Green Book landing page. This approach allows for more frequent updates and ensures that the Green Book itself will not become quickly outdated as resources change. It would also allow for hyperlinks to the resources, rather than just descriptions, which would make the list of resources even more useful.

Other Comments

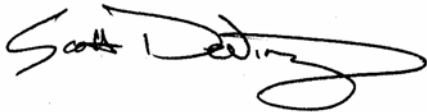
We did not find the new paragraph OV1.04 to be coherent. We further noted that this corresponds to a new glossary term “controls” that is significantly different than the definition of “internal control,” which is confusing.

Finally, we object to the idea that risk tolerance does not apply to compliance objectives, as stated in 6.09. In practice, we see risk tolerance applied to compliance throughout federal, state and local government; to imagine otherwise is unrealistic. With regard to likelihood, controls may be designed to provide reasonable assurance rather than absolute assurance of compliance, consistent with paragraph OV1.05. With regard to magnitude, control activities or monitoring may be designed to only prevent, detect or correct potential noncompliance if it exceeds a certain threshold amount, under which noncompliance would be considered trivial, inconsequential or otherwise not cost-beneficial to address. With regard to nature, certain types of noncompliance may be considered technical or insignificant rather than substantive enough to warrant follow-up or enforcement. For example, the concept of risk tolerance is reflected in Single Audit requirements with regard to likelihood, magnitude and nature of noncompliance.

Thank you for the opportunity to provide our comments. Any inquiries may be directed to me at

[REDACTED]

Sincerely,

A handwritten signature in black ink, appearing to read "Scott DeViney". The signature is fluid and cursive, with a large loop at the end.

Scott DeViney, CPA
Assistant Director for Quality Assurance