August 19, 2024

ISACA
1700 East Golf Road, Suite 400
Schaumburg, IL, 60173
POC: Ron Lear, Vice President
Email: [redacted]

RE: ISACA Responses to the GAO Green Book Exposure Draft – **GAO-24-106889** Published: Jun 27, 2024. Publicly Released: Jun 27, 2024.

Thank you for the opportunity to submit comments to the GAO Greenbook Standards for Internal Control in the Federal Government. The following contains our comments, and if you have any questions, you can reach to Ron Lear at the email address noted above.

Q1: New Documentation Requirements

ISACA Response: Yes, the documentation requirements are sufficiently clear and understandable. It could be noted/clarified further that such documentation can be embedded in a risk tool or system, and the various requirements addressed in multiple ways/places/data, including more than one internal control system. These last two items offer the agency flexibility in choice and agility in implementation.

Q2: Relevance of Attributes

ISACA Response: While the application guidance is clear and understandable as is, the language used is relatively passive in voice and tone, when we think it should be more direct. A direct governance action/involvement ***Senior*** management perspective and expectation would strengthen the GB vs. just "management" or "management's consideration" We have found that it is often middle management where breakdowns can occur, and this can be directly linked to Senior management not being actively involved or having direct engagement and oversight. Structured language and deliberate linkage within and across any organization increases likelihood of effective adoption and monitoring.

Q3: Collaboration and Responsibility within the Internal Control System

ISACA Response: This is not as clear as it could be. The concern is that when it included phrases like "all levels of management" without specific roles and responsibilities, it can be construed as "someone else will address this". For example, when discussing "*design, implementation, and operation of the internal control system,"* Senior management would typically not be involved in lower level/daily implementation and operation, nor arguably even in

design except at the highest level. They would set expectations and high-level goals for this, with clear measurements that they want to see to verify progress. Recommend a change to be more explicit about which levels of management are engaged in each specific activity with a summary of how and why they are engaged.

Q4: External Parties

ISACA Response: We concur this change is clearer by removing the extant discussion specific to service organizations. However, some external parties may not have any interactions with the entity engaging them – such as the case where the entity may be purchasing Off-the-Shelf (OTS) solutions that require only a purchase order to acquire. Recommend that the attention on suppliers be one based on risk – which suppliers and/or their components pose the greatest risk to the entity's systems, infrastructure, etc. or those suppliers who provide components or solutions to a significant portion of the entity's solution and controls. This is consistent with increasing emphasis on seeking and assessing any organizations supply chain risk management.

Q5: Application Guidance in the Risk Assessment Component

ISACA Response: Guidance on risk assessment is clear, however, we were surprised that the GB contains no reference to opportunities along with risks similar to ISO 31000 and other similar standards. Opportunities have somewhat different handling aspect, but some are similar to risk, such as:

For example, options for leveraging opportunities should include:

- Creating
- Exploiting
- Transferring
- Monitoring
- Enhancing
- Accepting

Q6: Adds Requirement to Assess Improper Payment and Information Security Risks

ISACA Response: Clear and understandable and no additional comments.

Q7: Application Guidance Related to Assessing Fraud Risk

ISACA Response: Clear and understandable and no additional comments.

Q8: Identifying and Responding to Significant Changes

ISACA Response: With the operative word in Principle 9 being "significant" we believe this can be made clearer by directing that the adopting organization define criteria for what the term "significant" means – where it's financial, operational, reputational, etc. It is not realistic to expect an organization to respond to all changes, just those that have the significant impact on the business, so the business should identify this criteria in either the risk or change management plan. This could also be linked to efforts by SEC to establish and identify 'materiality' (impact, scope, scale) and 96-hr reporting timeline. Otherwise, this section is clear.

Q9: Discrete Processes to Manage Certain Entity Risks

ISACA Response: Clear and understandable and no additional comments.

Q10: Categories of Control Activities

ISACA Response: Clear and understandable and no additional comments.

Q11: Prioritizing Preventive Control Activities

ISACA Response: Clear and understandable and no additional comments. Figure 7 is particularly helpful. Our only additional comment would be where regulatory controls would fit into this mix, as they don't seem to be mentioned.

Q12: Changes Related to Information Technology

ISACA Response: Clear and understandable and no additional comments.

Q13: Focus of Information and Communication

ISACA Response: We would recommend not limiting use in Principle 13 to just Quality Information. Data, metadata, measurement data and information. Additionally the term "quality information" is misleading in some industries – it could be easily misconstrued as "information about quality" vs. data quality. The more common term would be "data quality" or "quality of information". We would also include in the definition the 3 pillars of data quality – completeness, coverage, and accuracy – the GB has "complete and accurate" covered, but not completeness. Also, clearly recognizing agency/industry-specific language that covers similar requirements pertaining to data may be helpful, e.g., in DoD parlance … "authoritative" data and "data provenance."

Q14: Monitoring Component

ISACA Response: As this term came up in the US ISO Technical Advisory Group 176 discussions last week in Washington, DC, you may want to clarify between the terms "continually" vs. "continuously" as some industries distinguish a difference, with continually being intermittent, whereas continuously means "nonstop". Note that in some languages (latin based for example, such as Italian and Spanish) there isn't a difference in these two words, but in other contexts, including some business contexts, there is a difference. Additionally, we would recommend changing the Principle 16.01 wording to as follows: *16.01 Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results, and take action as needed.* Otherwise, evaluation by itself is not enough.

Q15: New Appendixes

ISACA Response: Clear and understandable and no additional comments, other than the above responses should be addressed, if changed, for consistency in the Appendices.