GAO-13-830SP Standards for Internal Control in the Federal Government 2013 Exposure Draft

Please note page references are to pdf versions of the respective documents.

1. Is the hierarchy of (5) components, (17) principles, and (48) attributes clearly explained? Yes, but may appear confusing if read by area, rather than as a whole (as suggested).
    a. **Repetition and Structure**: The respective principles and attributes' descriptions were repetitious. The breakout by Component was an innovative method to tie in to the COSO model, but the breakout could benefit greatly from having a similar structure in an updated from [2001] GAO Internal Management and Evaluation Tool (GAO-01-1008G), or even on an appendix table (simplified example attached).
    b. **Language**: The instruction on how to use the Green Book states that the requirements for the Green Book were marked through the use of "must" and "should." (GAO GB Draft; p12/90) However, the text only defines the word "should" as a means to denote a principle or attribute statement. This could create an issue with different users' (local, quasi-governmental, as well as not-for-profits) interpretations of the identified standards. Although the principles and underlying attributes represent the **requirements necessary to achieve the standards** of internal control, (GAO GB Draft; O2.05, p15/90) the use of "should" may lead a reader to interpret a principal or attribute statement as truly optional.

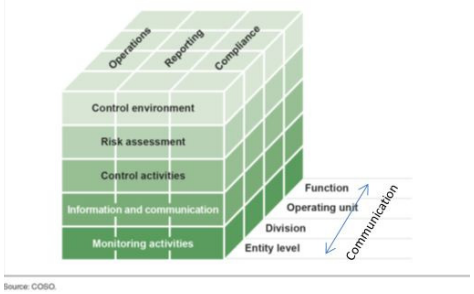
        For example, in other circumstances, GAO has specific definitions for "must" and "should"
        i. Must: Auditors must comply with an unconditional requirement in all cases where such a requirement is relevant (GAGAS uses the word "must") (GAO Yellow Book 2011 (GAO YB 2011); 2.15(a), p26/241)
        ii. Should: Auditors must comply with a presumptively mandatory requirement in all cases where such a requirement is relevant, except in rare circumstances where the auditors determine it necessary to depart from such a requirement. (GAGAS uses the word "should") In such cases, the auditors must document their justification for the departure and identify how any alternative procedures performed in the circumstances were sufficient to achieve the intent of that requirement. In rare circumstances, auditors and audit organizations may determine it necessary to depart from a relevant presumptively mandatory requirement. In such rare circumstances, auditors should perform alternative procedures to achieve the intent of that requirement. (GAO YB 2011; 2.15(b)-2.17, p27/241)

2. Are there any internal control concepts unique to the government environment that should be in the Green Book that are not currently included? Generally no, but please consider adding references as follow:

    References: Although specific requirements for assessing and reporting on controls in the federal government are noted as being on Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, emphasis could be made to OMB Circular A-123's Appendix A and its instructions. **If** GAO updates its (2001) Internal Management and Evaluation Tool, it would be a helpful reference for users in understanding these standards and how they may use and evaluate them.

3. Does the framework provide the necessary information to allow program managers to evaluate the internal controls for their programs? Generally yes, suggestions noted below:
    a. **Framework:** Although the framework identifies the standards and their respective principles and attributes, evaluations of internal controls are presented as comparison to management established baseline criteria to monitor the internal control system in supporting the entity in achieving its objectives. (GAO GB Draft; 16.04-16.05, p78/90)
    b. **Other:**
        i. Organizational Structure:

1. Entity organization structure is presented in COSO cube, but not discussed in area—footnote on previous page noted "discussion of organizational structure, but didn't provide context. (GAO GB Draft; O2.12-O2-13, p18/90) This illustration could benefit from a two-sided arrow to denote communication across different levels—and be presented as such, for example:



2. Reference for O2.10 on footnote is unclear as to how/where it's related to Organization Structure. (on GAO GB Draft; footnote 3, p17/90)

ii. Sub-objectives: Sub-objectives are discussed in O2.20 and O2.25. (GAO GB Draft; pp11,12/90) These could be combined in O2.20 for clarification and consistency.

4. Does the Green Book provide adequate criteria for auditors? Generally no, please note the following:
   a. **Documentation:** Although the Standards state the importance of effective documentation, (GAO GB Draft; O3.13, p37/90) the Green Book has limited situations where documentation is required (**minimum documentation criteria noted below for question 8**).
   b. **Criteria:** Although an entity "must" have an effective internal control system to comply with the standards, and an effective internal control system requires that each of the five components, with related principles and attributes are effectively designed; implemented; and operating. And the five components are operating together in an integrated manner. (GAO GB Draft; O2.01 and O3.01, pp14,22/90, respectively) Using that as criteria, if all the components, principles and attributes, as applicable aren't operating as prescribed, then the entity may not have an effective internal control system. This goes back to language (question 1) and documentation requirements (question 8).
   c. **Sufficiency of documentation requirements:** The Green Book stated that the extent of documentation supporting the design, implementation, and operating effectiveness of the five components of internal control is a matter of judgment for management. Management considers the cost-benefit of documentation requirements for the entity as well as the size, nature, and complexity of the entity and its objectives. **However, documentation may be necessary to ensure that the components of internal control are designed, implemented, and operating effectively.** (GAO GB Draft; 3.14, p38/90) This may become an issue with an auditor seeking reasonable, sufficient, and reliable support for a material management decision or assertion if this is the information that management decided was "optional," since it may not follow minimum documentation requirements (**question 8**)

5. Are the requirements for management to design, implement, and operate an internal control system clear, understandable, and adequate? Generally no. Wording isn't strong enough. Tie in to matching objectives and evaluation criteria would be helpful.

6. Is the evaluation of deficiencies discussion clear, understandable, and adequate?
   Yes, however it could benefit to a reference to an updated GAO's Internal Management and Evaluation Tool and the OMB Circular A-123, Appendix A Implementation Guide.

7. Are the roles, divisions, and overlaps of responsibility for the oversight body, management, and personnel clear, understandable, and adequate? Yes.

8. Are the documentation requirements included in the Green Book clear, understandable, and adequate?
<u>Documentation requirements understandable, but not necessarily adequate</u>:
    i. If management decides a principle or attribute is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle or attribute, the associated component could be designed, implemented, and operated effectively. (GAO GB Draft; O2.06, pp15-16/90)
    ii. O4.08 The Green Book **has specified documentation requirements** in five attributes in the framework, with discussion of these requirements in the accompanying application material. These are:
        1. Principle 3: Paragraph 3.12: Management should develop and maintain documentation of its internal control system.
        2. Principle 12: Paragraph 12.03: Management should document in policies the internal control responsibilities of the organization.
        3. Principle 16: Paragraph 16.12: Management should evaluate and document the results of ongoing monitoring and separate evaluations to identify internal control issues.
        4. Principle 17: Paragraph 17.07: Management should evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.
        5. Principle 17: Paragraph 17.09: Management should complete and document corrective actions to remediate internal control deficiencies on a timely basis [Oversight body noted as tracking status to ensure completion in a timely basis] (GAO GB Draft; O4.08, pp26-27/90)

9. Is there a need for additional internal control implementation guidance? If so, what form should it take? Tie in principles and attributes to an updated document similar to GAO's Internal Management and Evaluation Tool. Any tie must be loose, since the Green Book identifies these internal control standards and does not prescribe the process for how management designs, implements, and operates its internal control system. (GAO GB Draft; O2.08, p16/90)

10. Is this Green Book written in such a way to allow state, local, and quasi-governmental entities, as well as not-for-profit organizations, to adapt it for their own use? The Language and minimum documentation requirements noted in questions 1 and 4, respectively may present challenges to organizations trying to adapt these Standards in an effective manner.

Additional Comments:

1. O2.02; p14/90: change from "building them in" to "incorporated"
2. O2.06; p15/90: there either be a requirement for (using "should") or a standard for the suggested "documentation that includes the rationale of how, in the absence of that principle or attribute, the associated component could be designed, implemented, and operated effectively" where management decided the principle or attribute wasn't relevant.
3. O2.18; p19/90: change from:
"Management groups objectives into one or more of the three categories of objectives:" to "Management should group objectives into one or more of the three categories of objectives:"

GAO Green Book: Five Components of Internal Control and their 17 Related Principles for Design, Implementation, and Operating Effectiveness		
Internal Control Component	**Related Principles**	**Related Attributes**
Control Environment	The oversight body and management should demonstrate a commitment to integrity and ethical values.	Set the Tone at the Top - The oversight body and management should demonstrate the importance of integrity and ethical values through their directives, attitudes, and behavior. (Standards of Conduct)
Control Environment	The oversight body and management should demonstrate a commitment to integrity and ethical values.	Establish Standards of Conduct - Management should define expectations concerning integrity and ethical values in the entity's standards of conduct. (Processes for evaluations and addressing deviations)
Control Environment	The oversight body and management should demonstrate a commitment to integrity and ethical values.	Evaluate Adherence to Standards of Conduct - Management should establish processes to evaluate performance against the organization's expected standards of conduct and address any deviations in a timely manner.
Control Environment	The oversight body should oversee the entity's internal control system.	Establish Oversight Structure - The entity should determine an appropriate oversight structure based on applicable laws and regulations, relevant government guidance, and feedback from key stakeholders.
Control Environment	The oversight body should oversee the entity's internal control system.	Provide Oversight for the Internal Control System - The oversight body should oversee management's design, implementation, and operation of the internal control system.
Control Environment	The oversight body should oversee the entity's internal control system.	Provide Input for Remediation of Deficiencies - The oversight body should provide input to management's plans for remediation of deficiencies in the internal control system as appropriate.
Control Environment	Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.	Establish Organizational Structure - Management should establish an organizational structure.
Control Environment	Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.	Assign Responsibility and Delegate Authority - Management should assign responsibility and delegate authority to key roles throughout the organization.
Control Environment	Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.	Document Internal Control System - **Management should develop and maintain documentation of its internal control system.** Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties such as external auditors. Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity. The extent of documentation supporting the design, implementation, and operating effectiveness of the five components of internal control is a matter of judgment for management. Management considers the cost-benefit of documentation requirements for the entity as well as the size, nature, and complexity of the entity and its objectives. Some level of documentation, however, is necessary to ensure that the components of internal control are designed, implemented, and operating effectively.
Control Environment	Management should demonstrate a commitment to attract, develop, and retain competent individuals.	Establish Expectations of Competence - Management should establish expectations of competence throughout the organization.
Control Environment	Management should demonstrate a commitment to attract, develop, and retain competent individuals.	Attract, Develop, and Retain Individuals - Management should attract, develop, and retain competent personnel.
Control Environment	Management should demonstrate a commitment to attract, develop, and retain competent individuals.	Plan and Prepare for Succession - Management should define succession and contingency plans for key roles in the organization.
Control Environment	Management should evaluate performance and hold individuals accountable for their internal control responsibilities	Enforce Accountability - Management should enforce accountability for performance of internal control responsibilities.
Control Environment	Management should evaluate performance and hold individuals accountable for their internal control responsibilities	Consider Excessive Pressures - Management should evaluate and adjust pressures on personnel related to achieving objectives as they assign responsibilities and evaluate performance. If management establishes incentives, management recognizes that actions can yield unintended consequences and evaluates incentives to ensure that they align with the entity's standards of conduct.
Risk Assessment	Management should define objectives and risk tolerances.	Define Objectives - Management should define objectives in specific and measurable terms to enable the design of internal control for related risks.
Risk Assessment	Management should define objectives and risk tolerances.	Define Risk Tolerances - Management should define the risk tolerances for the defined objectives.
Risk Assessment	Management should identify, analyze, and respond to risks related to achieving the defined objectives.	Identify Risks - Management should identify risks throughout the entity.
Risk Assessment	Management should identify, analyze, and respond to risks related to achieving the defined objectives.	Analyze Risks - Management should analyze the identified risks to estimate their significance.
Risk Assessment	Management should identify, analyze, and respond to risks related to achieving the defined objectives.	Respond to Risks - Management should design responses to the analyzed risks.
Risk Assessment	Management should consider the potential for fraud when identifying, analyzing, and responding to risks.	Consider Types of Fraud - Management should consider the types of fraud (and potential waste and abuse) that can occur within the organization.
Risk Assessment	Management should consider the potential for fraud when identifying, analyzing, and responding to risks.	Consider Fraud Risk Factors - Management should consider fraud risk factors.
Risk Assessment	Management should consider the potential for fraud when identifying, analyzing, and responding to risks.	Respond to Fraud Risks - Management should analyze and respond to identified fraud risks.
Risk Assessment	Management should identify, analyze, and respond to significant changes in the internal control system.	Identify Change - Management should identify changes that could significantly impact the entity's internal control system.
Risk Assessment	Management should identify, analyze, and respond to significant changes in the internal control system.	Analyze and Respond to Change - Management should analyze and respond to identified changes that impact the entity's internal control system.
Control Activities	Management should design control activities to achieve objectives and risk responses.	Respond to Objectives and Risks - Management should design control activities that respond to the entity's objectives and risks.
Control Activities	Management should design control activities to achieve objectives and risk responses.	Design the Types of Control Activities - Management should design appropriate types of control activities needed for the entity's internal control system.
Control Activities	Management should design control activities to achieve objectives and risk responses.	Design Control Activities at Various Levels - Management should design control activities at appropriate levels in the organizational structure.
Control Activities	Management should design control activities to achieve objectives and risk responses.	Consider Segregation of Duties - Management should consider segregation of duties in designing the assignment of control activity responsibilities.
Control Activities	Management should design control activities for the entity's information system.	Design the Entity's Information System - Management should design the entity's information system to respond to the entity's objectives and risks.
Control Activities	Management should design control activities for the entity's information system.	Design Appropriate Types of Control Activities - Management should design appropriate types of control activities in the entity's information system.
Control Activities	Management should design control activities for the entity's information system.	Design the Information Technology Infrastructure - Management should design control activities over the information technology infrastructure.
Control Activities	Management should design control activities for the entity's information system.	Design Security Management - Management should design control activities for security management over the entity's information system.
Control Activities	Management should design control activities for the entity's information system.	Design Information Technology Acquisition, Development, and Maintenance - Management should design control activities over the acquisition, development, and maintenance of information technology.
Control Activities	Management should implement control activities.	Document Responsibilities through Policies - **Management should document in policies the internal control responsibilities of the organization.**
Control Activities	Management should implement control activities.	Perform Periodic Review - Management should periodically review the implementation of control activities to determine their continued relevance, redesign them when necessary, and communicate them as appropriate.
Information and Communication	Management should use quality information.	Identify Information Requirements - Management should design a process to identify information requirements.
Information and Communication	Management should use quality information.	Obtain Relevant Data from Reliable Sources - Management should obtain relevant data from reliable internal and external sources on a timely basis based on the identified information requirements.
Information and Communication	Management should use quality information.	Process Data into Quality Information - Management should process the obtained data into quality information.
Information and Communication	Management should internally communicate the necessary quality information.	Communicate throughout the Entity - Management should communicate quality information throughout the entity utilizing established reporting lines.
Information and Communication	Management should internally communicate the necessary quality information.	Select Appropriate Method of Communication - Management should select appropriate methods to communicate internally.
Information and Communication	Management should externally communicate the necessary quality information.	Select Appropriate Method of Communication - Management should select appropriate methods to communicate externally.
Information and Communication	Management should externally communicate the necessary quality information.	Communicate with External Parties - Management should communicate with, and obtain quality information from, external parties utilizing established reporting lines.
Monitoring	Management should establish monitoring activities to monitor the internal control system and evaluate the results.	Establish a Baseline - Management should establish a baseline for monitoring the internal control system.
Monitoring	Management should establish monitoring activities to monitor the internal control system and evaluate the results.	Monitor Internal Control System - Management should monitor the internal control system through ongoing monitoring and separate evaluations.
Monitoring	Management should establish monitoring activities to monitor the internal control system and evaluate the results.	Evaluate Results - **Management should document and evaluate the results of ongoing monitoring and separate evaluations to identify internal control issues.**
Monitoring	Management should ensure identified internal control deficiencies are remediated on a timely basis.	Report Issues - Personnel should report internal control issues to appropriate internal and external parties on a timely basis.
Monitoring	Management should ensure identified internal control deficiencies are remediated on a timely basis.	Evaluate Issues - Management should evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.
Monitoring	Management should ensure identified internal control deficiencies are remediated on a timely basis.	Complete Corrective Actions - **Management should complete and document corrective actions to remediate internal control deficiencies on a timely basis.**

#8 Granado

Green denotes minimum required attributes