U.S. Department of the Interior
2024 Green Book Exposure Draft - Comment Matrix

https://www.gao.gov/products/gao-24-106889

Commenter	Input					
Bureau/Office	**Section**	**Section Title**	**Page Number**	**Current Text in the *GAO Green Book 2024 Exposure Draft* Associated with the Feedback**	**Identify the Issue with the Draft**	**Recommended Fix/Updated Wording**
BOEM	Letter		Infographic (before the letter)	The cube The standards in the Green Book are organized by the five components of internal control shown in the cube below. The five components apply to staff at all organizational levels and to all categories of objectives	The infographic relies on the old COSO internal control cube and does not incorporate ERM, including COSO's own updated ERM model.	Adopt COSO or similar diagram that includes ERM and internal control (cube should include Strategic Risks, for example). See: https://www.accaglobal.com/gb/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-leader/technical-articles/coso-enterprise-risk-management-framework.html
BOEM	Letter		1 (7 of PDF)	To help ensure that the standards continue to meet the needs of the federal community and the public it serves, the Comptroller General of the United States established the Advisory Council on Standards for Internal Control in the Federal Government (Green Book Advisory Council) to review GAO's proposed revision of the standards and consider any other necessary changes. The Green Book Advisory Council includes those knowledgeable in internal control drawn from federal, state, and local government; the private sector; and academia. This exposure draft includes the Green Book Advisory Council's input regarding the proposed changes. We are currently requesting public comments on the proposed changes in the exposure draft.	1. The Letter does not acknowledge other major Federal policy and legislative changes since 2014 (e.g. revision to OMB Circular A-123 to include ERM, PMIAA, Evidence Act, DATA Act, etc.) 2. The GAO seems to have relied upon a somewhat limited set of expertise across the Federal sector when drafting this revised Green Book. Upon reviewing the Appendix IV Acknowledgements (pages 127-128) it is clear that neither the OMB nor the CFO Council were consulted. This means there is no alignment with the Federal ERM Playbook.	This document is not ready for widespread release because of the failure to integrate ERM and related disciplines. If this must go forward, then the letter and overview should be amended to state the limitations of this document and/commitment to future efforts to integrate so that governmental entities will have a more complete toolkit for implementation.
BOEM	Enclosure I	Major Changes in the Proposed Green Book 2024 Revision	5 (11 of PDF)	Principle 10. Management should design control activities t*o mitigate risks* to achieving the *entity's* objectives *to acceptable levels* ~~and respond to risks.~~ Principle 11. Management should design the ~~entity's information system and related~~ *general* control activities *over information technology to mitigate risks* to achieving *the entity's* objectives t*o acceptable levels* ~~and respond to risks~~.	These textual changes are otherwise reasonable, however, the addition of the phrase "to acceptable levels" implies the use of the concept of "risk tolerance." While risk tolerance is discussed throughout the document, there is no mention of the term "risk appetite" (the aggregate of risk that management/leadership is willing to take on). There is also no Appendix to provide support on methods for determining "acceptable levels" of risk. Needs integration with OMB Circular A-123, Federal ERM Playbook and related sources.	

Commenter	Input					
Bureau/Office	Section	Section Title	Page Number	Current Text in the *GAO Green Book 2024 Exposure Draft* Associated with the Feedback	Identify the Issue with the Draft	Recommended Fix/Updated Wording
BOEM	Overview	External Parties	37 (43 of PDF)	Other Parties Interacting with the Entity OV4.06 Management interacts with other external parties to obtain or share information relevant to the entity's internal control system. This may include information from legal or regulatory requirements or data-sharing agreements with other government entities.13 Management also interacts with external parties for which the entity has oversight responsibility, including those that receive federal awards, such as grants, from the entity. Establishing two-way communication with external parties promotes information sharing that may improve the internal control systems of both parties and facilitate effective stewardship of public resources.	Adding external parties (that are not Servicing Organizations) is a welcome addition as it recognizes the organizational, structural and political complexities faced by the entity/government agency.	Recommend adding an Appendix that can be footnoted in this section on External Parties (examples, considerations (trade-offs, risks and benefits of exchanging information and risk transfer)
PFM	Enclosure II: Questions for Commenters	Discussion Questions for Responses	13-14	Discussion Questions for Responses - 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?	OMB is planning it issue updated Payment Integrity Informaiton Act (PIIA) guidance, OMB Circular A-123 Appendix C in 2024. We want to ensure the requirements within the Green Book align with the new guidance to ensure the requirements are not conflicting or causing duplicative efforts.	Coordinate with OMB and other applicable parties to ensure the requirements within the Green Book align with the PIIA guidance.

Commenter	Input					
Bureau/Office	Section	Section Title	Page Number	Current Text in the *GAO Green Book 2024 Exposure Draft* Associated with the Feedback	Identify the Issue with the Draft	Recommended Fix/Updated Wording
PFM	Enclosure II: Questions for Commenters	Discussion Questions for Responses	13-14	Discussion Questions for Responses - 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?	Within Principle 8 - Assess Fraud, Improper Payment, and Information Security Risk it stated "Management identifies risks related to fraud, improper payments, and information security through the same risk identification process performed for all analyzed risks.", "Management analyzes and responds to identified fraud, improper payment, and information security risks so that they are effectively mitigated. These risks are analyzed through the same risk analysis process performed for all identified risks.", and "Management responds to fraud, improper payment, and information security risks through the same risk response process performed for all analyzed risks." It is unclear what is meant by "same" in the statement above (e.g. is this using the same tools/templates, assessing at the same frequency?). There are other federal laws and regulations for risks assessments of these areas such as PIIA and OMB Circular A-123 Appendix C. Also, the proposed Green Book Guidance promotes developing discrete processes to manage certain entity risks which may result in differences with how the risk assessments are conducted. If multiple risk assessments need to be performed over the same areas it will cause duplicative efforts.	Clarify what is meant by "same" when saying that risk related to fraud, improper payments, and information security need to be assessed through the same risk identification process performed for all analyzed risks (e.g. can different tools/templates be used?) and the objective of using the same risk identification process for all risks. Additionally, elaborate what flexability is possible in the risk assessment efforts to qualify as the "same".
BSEE	Control Activities	Design of Appropriate Types of Control Activities	81-83	paragraphs 10.06 - 10-08 10.06 Management designs information technology control activities to support the operation and security of the entity's information technology and automated business processes. Information technology control activities consist of general,68 application, and user controls. 10.07 Application control activities are automated control activities that are incorporated directly into application software to achieve the completeness, accuracy, and validity of transactions and data. Application controls include control activities over the input, processing, and output of data. User control activities, sometimes referred to as information technology-dependent controls, are partially automated control activities that are performed by individuals using the entity's information technology or by relying on the information processed through technology.69 For example, management may authorize a transaction as part of an automated workflow or may respond to incidents flagged in system log reports. 10.08 Figure 7 lists common categories of information technology control activities related to general, application, and user controls and illustrates how information processing and information security objectives align with the three types of control activities.70 The common categories of information technology control activities listed in figure 7 are meant only to illustrate the range and variety of control activities that may be useful to management. This list is not all inclusive and may not include all information technology control activities that an entity may need.	The draft splits the attributes associated with Information Technology by relating Principle 10 to application controls and principle 11 to general controls. The reasoning for the split is not clear. When testing assessing compliance with these principles for general and application controls, it is an unnecessary and cumbersome split in trying to appropriately address all attributes.	Recommend moving application controls to Principle 11 and change Principle 11's title to "Design Control Activities over Information Technology." Another attribute can be added titled "Design of Appropriate Types of Application Controls."

Commenter	Input					
Bureau/Office	Section	Section Title	Page Number	Current Text in the *GAO Green Book 2024 Exposure Draft* Associated with the Feedback	Identify the Issue with the Draft	Recommended Fix/Updated Wording
BSEE	Overview	Definition of Internal Control	22	OV1.04 Embedded in the internal control process are documented policies and procedures that establish controls.5 Policies reflect management or oversight body statements of what should be done to effect internal control. Procedures consist of actions that implement policies. Management establishes controls within each component of internal control to effect relevant principles. Controls are interrelated and may support multiple principles and entity objectives. Controls that management establishes as part of the control activities component to specifically mitigate risks to achieving the entity's objectives to acceptable levels are considered control activities. Control activities support all the components of internal control but are particularly aligned with the risk assessment component.	This paragraph is meant to identify the definition of control and control activities based on the "Key Changes in Terminology" section on page 11. It does not provide a definition of either and instead, seems to describes characteristics. The first sentence is confusing since this paragraph is attempting to differentiate controls and control activities.	Recommend deleting the sentence "Embedded in the internal control processes are documented policies and procedures that establish controls" and use definitions as provided in the glossary to state: " Controls are policies and procedures management establishes to effect relevant principles withing each component of internal control. Embedded within those policies and procedures are control activities that mitigate risks to achieving the entity's objectives"
BSEE	Overview	Definition of Internal Control	22	Footnote. 5Policies and procedures that establish controls are a subset of the entity's overall policies and procedures.	I don't understand what this is trying to explain. Is it that policies and procedures fall under other policies and procedures? Is so, that does not make sense. A federal entity may have one governing policy or procedure that all have to follow and would not require layers of policies and procedures for the same requirement.	Clarify or remove this footnote.