RMA | Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

GAO Green Book Exposure Draft Comments

Table 1: RMA Associates Feedback

Section(s)	Discussion Question #	Printed Page(s)	Comment
Clarified Principle and Documentation Requirements	N/A	5	Please clarify why was the phrase "respond to risks" removed from Principle 10 Risks and internal controls are interrelated. Consider revising the name or the introductory sentence of Principle 10 to explicitly include the concept of risk mitigation. For example, the principle could be titled "Design and Implement Control Activities to Mitigate Risks" or the description could start with, "Management should design and implement control activities specifically aimed at mitigating risks to achieving the entity's objectives.
OV 1.07, OV2.17, 1.03-1.04 and 16.10	Responsibility and Internal Control System	22 29 42 105	Consider providing a clearer delineation of responsibilities among various levels of management could prevent overlaps or gaps in accountability. Consider a responsibility matrix or a clear delineation of roles within the guidance to ensure that responsibilities are well-defined and understood across the organization.
OV 2.08 OV 2.09	Application Guidance (attributes)	25 26	To avoid misinterpretation, consider including specific examples or case studies on how management can assess the relevance of attributes in different scenarios.
OV2.23-.27	N/A	31-32	Please consider adding examples of operation, reporting, and compliance objectives to the Green Book to assist the reader.
OV2.29	N/A	32-33	Please consider adding examples of sub-objectives to the Green Book to assist the reader.
OV3.08	N/A	34-35	Please consider adding a visual showing definitions of the magnitude, likelihood, and nature of the deficiency or a bulleted list. Lists can be hard to read in paragraph form.
OV4.01 - .06	4 – External Parties	36, 37	Please consider adding two visuals or bullets showing examples of external parties and examples of what things can be identified by open communication with external parties. Lists can be hard to read in paragraph form. The guidance could be enhanced by addressing the risks associated with increasing reliance on external service providers, particularly in the context of cybersecurity and data protection. Consider including specific recommendations for mitigating risks associated with external parties, particularly in areas such as data sharing and cybersecurity. This could involve setting minimum security standards that external service providers must adhere to.
OV4.09	N/A	38	Please consider changing the sentence "Information technology enables organizations to connect with internal and external end-users, process high volumes of transactions, transform data into information to support sound decision-making and share that information in real-time" into a bulleted list. Lists can be hard to read in paragraph form.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Section(s)	Discussion Question #	Printed Page(s)	Comment
7.15 and 9.08	Risk Assessment documentation And Significant Changes	61 71	The requirement to document risk assessments for improper payments and significant changes in internal controls, including responses to risks, on both a periodic and ongoing basis, maybe an overwhelming volume of documentation without necessarily improving internal control effectiveness. Consider providing additional guidance or a scaled approach based on the size of the organization to documentation requirements.
11.01	12 – Changes Related to Information Technology	87	General control activities are included but application controls to ensure the overall integrity and effectiveness of the internal control system. Consider change to: • **Design of Appropriate Types of General and Application Control Activities** Please consider providing a more detailed explanation of the reasons behind moving information technology control activities not related to general controls to principle 10. Additionally, clarify how these changes should be implemented in practice to ensure consistency and effectiveness in the application of the revised principles.
11.02	12 – Changes Related to Information Technology	87	The 2014 version includes a discussion of what an information system is and its purpose, while the new version doesn't. This provided essential context and clarity for readers, especially those who may not have a technical background. However, this discussion appears to be absent in the new version.
12.02	N/A	93	Please elaborate on any details "Management establishes control activities by documenting in policies what is expected" (of whom or for what?) "and in procedures specified actions" (for what?). **"What is expected"**: Clarify who is expected to perform these activities and in what context (e.g., roles and responsibilities). **"Specified actions"**: Explain what actions are to be taken, in what situations, and by whom.
12.03	N/A	93	Please clarify why was "related risks" removed from the first sentence. While the guidance later states that documenting each unit's responsibility for process objectives and control activities will mitigate related risks, explicitly mentioning "related risks" upfront could better emphasize the importance of identifying and addressing these risks. Consider reintegrating "related risks" into the first sentence to ensure that the reader is immediately aware of the importance of considering risks when documenting responsibilities. Clearly identifying risks from the outset can help management and each unit better understand potential pitfalls and enhance the overall effectiveness of risk mitigation strategies.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Section(s)	Discussion Question #	Printed Page(s)	Comment
13.05-.07	N/A	97	The second sentence, "An information system comprises the people, processes, data, and information technology that management uses to obtain, generate, communicate, or dispose of information to support the entity's business processes," provides a foundational definition that is crucial for understanding the rest of the section. Consider moving this sentence to the beginning of the section to establish the context upfront. This reordering would help readers better understand the role of the information system before diving into how data is processed into quality information.
14.02	13 – Focus on Information and Communication	98	The second sentence in Paragraph 14.02, "Communication is the continual, iterative process of providing, sharing, and obtaining necessary information," provides a foundational definition of communication that is essential for understanding the section. Consider moving this sentence to the beginning of Paragraph 14.01 on Page 97. Introducing the definition of communication at the outset will help readers grasp the concept before delving into how management communicates information throughout the entity.
14.08	N/A	99	The guidance suggests that management should select appropriate methods of communication but does not provide specific examples. Including examples of appropriate communication methods could be beneficial for helping entities understand how to effectively apply this guidance in various contexts. Consider adding examples of appropriate methods of communication back to the Green Book. Examples could include methods such as formal reports, intranet postings, email newsletters, team meetings, or dashboards, which would provide management with practical options to consider when ensuring quality information is communicated throughout the entity.
17.06	N/A	107	Please consider changing the text listing for the proper documentation of corrective plans to a bulleted/numbered list instead. This would delineate each element that should be included in the documentation, such as: • Root-cause analysis, • Planned actions, • Interim milestones, • Completion dates, • Measurable indicators of compliance and resolution, • The entity official responsible for monitoring the status of the corrective actions.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Section(s)	Discussion Question #	Printed Page(s)	Comment
			This format would make the guidance more user-friendly and ensure that all aspects of the corrective action documentation are easily identifiable.
Appendix II	15 – New Appendices	112	Please consider matching the examples of preventative and detective controls in the graphic to the examples that are explained on pages 114 to 119.
Appendix III	15 – New Appendices	121	Please consider adding the Federal Manager's Financial Integrity Act (FMFIA) to the section on Fraud Resources, highlighting its framework for establishing and maintaining internal controls, especially in relation to OMB Circular A-123
Appendix III	15 – New Appendices	124-125	Please consider moving NIST SP 800-53, Revision 5 to a bullet point separate from NIST SP 800-39.