Enclosure I: Overview of Major Changes in Proposed *Standards for Internal Control in the Federal Government* 2024 Revision

Since the *Standards for Internal Control in the Federal Government* (commonly known as the Green Book) was last revised in 2014, events such as pandemics and cyber-attacks have highlighted the challenges management faces when addressing risks related to fraud, improper payments, information security, and the implementation of new or substantially changed programs, including emergency assistance programs. This revision provides additional requirements, application guidance, and resources for addressing these risk areas when designing, implementing, and operating an effective internal control system. Other changes are made to continue harmonization with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control - Integrated Framework* and make other modifications to clarify the intent of the requirements. Updates emphasize prioritizing preventive control activities and highlight management's responsibility for internal control at all levels and within all functions in the entity's organizational structure, such as program and financial managers.

Major Changes in the Proposed Green Book 2024 Revision

The proposed Green Book 2024 revision (proposed revision) would replace the extant *Standards for Internal Control in the Federal Government* 2014 revision. Although the five components of internal control and 17 related principles remain, some principles were modified, and attributes were added or expanded upon. Two new documentation requirements have been added, and two extant documentation requirements have been modified. In addition, two new appendixes are proposed. One (appendix II) provides examples of preventive and detective control activities. The other (appendix III) provides resources that management may leverage in designing, implementing, and operating effective internal control systems to address risk areas related to fraud; improper payments; information security; and the implementation of new or substantially changed programs, including emergency assistance programs. A discussion of the major changes in the proposed revision follows.

Commented [OMB1]: OMB recommends reducing additional documentation requirements where possible. Acknowledging the intent is that management at all levels assess risk and fraud. As many agencies contract out these reviews, the cost to implement may exceed the value of additional documentation.

New Requirements

The proposed revision adds a requirement to consider risks related to improper payments and information security when identifying, analyzing, and responding to risks (paragraph 8.01). 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.

Two new documentation requirements have also been added to the proposed revision.

- Management documents the results of the risk assessment, including the identification, analysis, and response to risks, that are completed on both a periodic and ongoing basis. This may include~~s~~ documentation of the consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system (paragraph 7.15).
- Management documents a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur (paragraph 9.08).

Commented [OMB2]: Documentation of consideration of all risks on the topics listed for each program or activity would be extensive and overly burdensome.

Clarified Principle and Documentation Requirements

The following principles have been clarified; proposed new language is shown in italics and deletions in strikethrough font:

- Principle 10. Management should design control activities *to 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 *to acceptable levels* ~~and respond to risks~~.
- Principle 12. Management should implement control activities through policies *and procedures*.
- Principle 13. Management should *obtain or generate, and* use *relevant,* quality information to ~~achieve the entity's objectives~~ *support the functioning of the internal control system*.
- Principle 14. Management should internally communicate ~~the necessary~~ *relevant and* quality information, *including objectives and responsibilities for internal control, necessary* to ~~achieve the entity's objectives~~ *support the functioning of the internal control system*.
- Principle 15. Management should ~~externally~~ communicate ~~the necessary~~ *relevant and* quality information ~~to achieve the entity's objectives~~ *with appropriate external parties regarding matters impacting the functioning of the internal control system*.

The discussion on documentation requirements was moved from Overview 4 to Overview 2 (paragraph OV2.10), to align with the discussion on other requirements for establishing an effective internal control system. In addition, the following documentation requirements have been clarified; proposed new language is shown in italics and deletions in strikethrough font:

	• Management ~~documents~~ *establishes control activities by documenting* in policies ~~the internal control responsibilities of the organization.~~ *what is expected and in procedures the specified actions*. (paragraph 12.02) • Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies, *including those reported from external audits and evaluations*, on a timely basis. (paragraph 17.05) • Management completes and documents, as appropriate, corrective actions to remediate internal control deficiencies, *including those reported from external audits and evaluations*, on a timely basis. (paragraph 17.06)
Clarifies the Relevance of Attributes	The proposed revision clarifies the relevance of attributes to management properly applying the requirements and assessing whether the principles support the effective design, implementation, and operation of the internal control system (paragraphs OV2.08 through OV2.09). Furthermore, the proposed revision clarifies that management considers the related attributes in its summary determination of whether the principles are designed, implemented, and operating effectively (paragraph OV3.10).
Emphasizes Collaboration and the Responsibility of Management throughout the Entity for the Internal Control System	The proposed revision clarifies that the responsibility for the internal control system involves management at all levels and within all functions in the entity's organizational structure, including program and financial managers (paragraphs OV1.07 and OV2.17). The proposed revision promotes the collaboration among all levels of management on the design, implementation, and operation of the internal control system. It also emphasizes collaboration with the oversight body, personnel, appropriate functions within the organizational structure, and external parties as applicable, which is key to an effective internal control system (paragraphs OV2.18, 1.04, and 16.10). The proposed revision also emphasizes that personnel throughout the entity, in addition to management and the oversight body, play an important role in setting the tone that permeates the organizational culture (paragraph 1.03), which is fundamental to an effective internal control system and enables the entity to achieve its objectives, prevent and detect fraud and improper payments, and secure its information technology.
Expands Discussion of External Parties	The proposed revision in the Overview section 4 (paragraphs OV4.01 through OV4.06) replaced the extant discussion of service organizations with a discussion of external parties, which includes service organizations and other external parties that interact with the entity. The discussion of other external parties includes other parties for which the entity has

Commented [OMB3]: for a management decision, requirements for corrective action should align with the requirements and guidance of 5 USC Ch. 4, and OMB Circular A-50. For example, OMB Circular A-50 recognizes that written plans for correction action should be provided "where appropriate." Circular A-50 (1982 version).

See also 5 U.S.C. 405(a)(3) (Recognizing that a management decision reflects corrective actions "concluded to be necessary" by management).

	components of internal control related to these specific risks (paragraphs 7.12 and 8.20). Management may also identify discrete divisions, operating units, or functions with which to manage the entity's risk responses within the internal control system (paragraph 3.03).
Clarifies and Expands on Changes to Categories of Control Activities	The proposed revision clarifies and expands the common categories of control activities illustrated in principle 10 (paragraph 10.04). New categories that were added include activities related to oversight of service organizations and grant programs and activities to address specific risks, such as fraud and improper payments. Additionally, the new proposed appendix II, Examples of Preventive and Detective Control Activities, provides specific examples of control activities that may be useful to management.
Emphasizes Prioritizing Preventive Control Activities	The proposed revision expands the application guidance related to the design of preventive and detective control activities. It emphasizes that management designs an appropriate mix of preventive and detective control activities to mitigate risk to an acceptable level. It also emphasizes that management prioritizes preventive controls by considering them first, as they generally offer the most cost-efficient use of resources and are generally effective at mitigating fraud and improper payments (paragraphs 10.09 through 10.11). The proposed revision further discusses an appropriate mix of preventive and detective controls as part of management's cost versus benefit considerations (paragraphs OV4.14 through OV4.16). Additionally, the new proposed appendix II, Examples of Preventive and Detective Control Activities, provides examples of preventive and detective control activities that may be useful to management.
Updates Areas Related to Information Technology	The proposed revision seeks to modernize the discussion of information technology. Additions to the Overview section 4 (paragraphs OV4.07 through OV4.11) discuss the pervasive nature of information technology in entities' business and internal control processes and the need to address evolving risks to the security of the entity's information technology. The proposed expansion of principle 8 above discusses information security risk further. The proposed revision modifies the requirement in principle 11 to focus on general control activities (paragraph 11.01). Principle 11 has been modified and reorganized overall to focus on general control activities over information technology, which support the information security objectives: confidentiality, integrity, and availability (paragraph 11.07). The proposed revision reorganizes and clarifies application guidance

Commented [WSAE4]: The information security requirement, though logical in theory, may be difficult to implement in practice. IT controls are undoubtedly more important than ever. However, much of the work addressed by the green book falls under the CFO while IT controls typically reside in other offices. The new information security requirements may be a heavy lift for agencies considering the implementation date of this document.

Enclosure II: Questions for Commenters

The following questions are provided to guide users in commenting on the *Standards for Internal Control in the Federal Government* 2024 Revision. We encourage you to comment on these issues and any additional issues that you note.

Please associate your comments with specific references to question numbers, paragraph numbers in the proposed standards, or both, and provide the rationale for any modifications, along with suggested revised language.

Discussion Questions for Responses

New Documentation Requirements

1. Management would be required to document (1) the results of the risk assessment, including the identification, analysis, and response to risks that are completed on both a periodic and ongoing basis, including consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system (paragraph 7.15) and (2) a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur (paragraph 9.08).

   Are these documentation requirements sufficiently clear and understandable?

Relevance of Attributes

2. The proposed revision clarifies that management considers all attributes in properly applying the requirements and in assessing, including in summary documentation, whether the principles support the effective design, implementation, and operation of the internal control system (paragraphs OV2.08 through OV2.09 and OV3.10).

   Is this application guidance relating to management's consideration of the relevance of attributes sufficiently clear and understandable?

Collaboration and Responsibility within the Internal Control System

3. The proposed revision clarifies and adds application guidance emphasizing the importance of collaboration between all levels of management on the design, implementation, and operation of the internal control system. It also emphasizes collaboration with the oversight body, personnel, appropriate functions within the organizational structure, and external parties as applicable. It also emphasizes that the responsibility for the internal control system

Commented [WSAE5]: Please see separate attached document for OMB responses.

GAO Comment: the separate attached document starts on page 16.

- Management evaluates and documents the results of ongoing monitoring and separate evaluations, as appropriate, to identify internal control issues. (paragraph 16.09)
- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies, including those reported from external audits and evaluations, on a timely basis. (paragraph 17.05)
- Management completes and documents, as appropriate, corrective actions to remediate internal control deficiencies, including those reported from external audits and evaluations, on a timely basis. (paragraph 17.06)

OV2.11 These requirements represent the minimum level of documentation in an entity's internal control system. Management exercises judgment in determining what additional documentation may be necessary for an effective internal control system. If management identifies deficiencies in achieving these documentation requirements, the effect of the identified deficiencies is considered as part of management's summary determination of whether the related principle is designed, implemented, and operating effectively.

Commented [OMB6]: Risk is inherent to all activities and documentation of all ongoing monitoring and reviews should be documented as appropriate.

Commented [OMB7]: for a management decision, requirements for corrective action should align with the requirements and guidance of 5 USC Ch. 4, and OMB Circular A-50. For example, OMB Circular A-50 recognizes that written plans for correction action should be provided "where appropriate." Circular A-50 (1982 version).

See also 5 U.S.C. 405(a)(3) (Recognizing that a management decision reflects corrective actions "concluded to be necessary" by management).

Internal Control and the Entity

OV2.12 A direct relationship exists among an entity's objectives, the five components of internal control, and the organizational structure of an entity. Objectives are what an entity wants to achieve. Management uses internal control to help the organization achieve these objectives. The five components of internal control are what is required of the entity to achieve the objectives. Organizational structure encompasses the overall entity, divisions, operating units, functions, and other structures management uses to achieve the objectives. Functions include business processes, such as accounting and payroll processing, security services, or health care claims processing. Business processes are established across the entity to enable organizations to achieve their objectives and transform inputs into outputs through a series of transactions or activities. This relationship is depicted in the form of a cube that COSO developed (see fig. 4).[7]

[7]See paras. 3.02 through 3.05 for further discussion of organizational structure.

necessary for the entity to implement in addition to controls the service organization performs to achieve its control objectives. Other controls may include those related to monitoring the effectiveness of the design, implementation, and operation of the service organization's controls in achieving the entity's control objectives.

OV4.05 Management may consider the following when determining the extent of oversight for the business processes assigned to the service organization:

- the nature of services outsourced,
- the service organization's standards of conduct,
- the quality and frequency of the service organization's enforcement of adherence to standards of conduct by its personnel,
- the magnitude and level of complexity of the entity's operations and organizational structure, and
- the extent to which the entity's internal controls are sufficient to provide reasonable assurance that the entity achieves its control objectives and addresses risks related to the assigned process.

Commented [OMB8]: Propose insertion of an additional bullet focused on considerations of materiality.

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.

Information Technology

OV4.07 Information technology may be essential to achieving the entity's objectives and better controlling its business processes. Entities and individuals are becoming more interconnected using information

[13]See paras. 15.02 through 15.06 for further discussion of communication with external parties.

specific control activity.[44] Typically, controls are not needed when an entity chooses to either accept or avoid a risk. The nature and extent of risk response actions and any associated controls will depend, at least in part, on the defined level of risk tolerance.

7.12 When designing controls to mitigate risk, management may modify controls related to the entity's oversight responsibilities, organizational structure, and responsibilities and authorities throughout the entity. Management may also develop a separate and ongoing process, with separate oversight responsibilities, for managing certain risks as part of the entity's overall internal control system. This may be necessary to achieve objectives due to the nature of certain types of risks, such as for risks related to fraud, improper payments, or information security, or when a risk is pervasive or has an impact on multiple processes. This separate and ongoing process would cover all components of internal control related to these specific risks.

7.13 After designing risk responses, management then considers residual risk. The risk response need not necessarily result in the least amount of residual risk. But where a risk response would result in residual risk exceeding defined risk tolerances, management revisits and revises the response. Operating within the defined risk tolerance provides greater assurance that the entity will achieve its objectives.

7.14 Performance measures are used to assess whether risk response actions enable the entity to operate within the defined risk tolerances. When risk response actions do not enable the entity to operate within the defined risk tolerances, management may need to revise risk responses or reconsider defined risk tolerances. Management may need to conduct periodic risk assessments to evaluate the effectiveness of the risk response actions.

7.15 Management documents the results of the risk assessment, as appropriate, including the identification, analysis, and response to risks that are completed on both a periodic and ongoing basis. This includes documentation of the consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system.

[44]See para. 10.02 for further discussion of designing control activities in response to risks.

Principle 8 - Assess Fraud, Improper Payment, and Information Security Risk

8.01 Management should consider risks related to fraud, improper payments, and information security when identifying, analyzing, and responding to risks.[45]

Attributes

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

- Identification of Risks Related to Fraud, Improper Payments, and Information Security
- Types of Fraud and Fraud Risk Factors
- Types of Improper Payments and Improper Payment Risk Factors
- Types of Information Security Risk and Information Security Risk Factors
- Analysis of and Response to Identified Risks

Identification of Risks Related to Fraud, Improper Payments, and Information Security

8.02 Management identifies risks related to fraud, improper payments, and information security through the same risk identification process performed for all analyzed risks.[46] However, these risks are discussed further in this principle because they may be pervasive or have an impact on multiple processes and can often be inadequately addressed in the risk assessment process.

8.03 Management performs risk assessments related to fraud, improper payments, and information security on a periodic and ongoing basis, as appropriate. The scope and frequency of these assessments are determined through the same analysis performed for all analyzed risks,[47] and as required by any legal or regulatory requirements. However, management may determine that the risk assessments need to be performed more frequently than required by legal or regulatory requirements due to the significance of risks or other factors such as changes to programs. For example, to adequately identify risks related to improper payments for new programs, management may perform improper payment risk assessments for a

[45]See app. III for additional resources related to addressing risks related to fraud, improper payments, and information security.

[46]See paras. 7.02 through 7.15 for further discussion of identifying, analyzing, and responding to risks.

[47]See para. 7.02 for further discussion of scope and frequency of risk assessments.

Principle 10 - Design Control Activities

10.01 Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.

Attributes

The following attributes contribute to the design, implementation, and operating effectiveness of this principle:

- Response to Risks
- Design of Appropriate Types of Control Activities
- Design of Preventive and Detective Control Activities
- Design of Control Activities at Various Levels
- Segregation of Duties

Commented [WSAE9]:

In Principle 10 and 11 proposed new language, "to mitigate risks" is used instead of "respond to risks". In scenarios where management has chosen to accept or avoid the risk, the term mitigate may not be appropriate.

In addition, Principles 7-9 reference the response to risk, rather than the mitigation of risks. Recommend consistency throughout document.

Response to Risks

10.02 Management designs control activities in response to risks to achieve an effective internal control system. Control activities are the actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels.[61] Control activities support all the components of internal control but are particularly aligned with the risk assessment component. As part of ongoing and periodic risk assessments, management identifies objectives; the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities or modifies existing control activities to mitigate risks to acceptable levels within management's defined risk tolerance for which control activities are needed.[62] Typically, control activities are needed when an entity chooses to either reduce or share a risk. The nature and extent of the risk response and any associated control activities will depend, at least in part, on management's defined risk tolerance.

Design of Appropriate Types of Control Activities

10.03 Management designs appropriate types of control activities for the entity's internal control system, including the entity's information technology, by considering all aspects of its internal control components, relevant business processes, and operating environment. An entity's internal control is flexible to allow management to tailor control activities

[61] See para. OV1.04 for further discussion of policies and procedures, including controls and control activities.

[62] See paras. 7.10 through 7.11 for further discussion of risk response actions.

testing of internal control to help identify issues in the internal control system. These audits and other evaluations may be mandated by law and are performed by internal auditors, external auditors, inspectors general, and other external reviewers. Separate evaluations provide greater objectivity when performed by reviewers who do not have responsibility for the activities being evaluated.

16.08 Management retains responsibility for monitoring the effectiveness of internal control over the assigned processes that service organizations perform. Management uses ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of a service organization's internal controls over the assigned process.[97] Monitoring activities related to service organizations may include the use of work performed by external parties, such as service auditors, and reviewed by management.

Evaluation of Results

16.09 Management evaluates and documents, as appropriate, the results of ongoing monitoring and separate evaluations to identify internal control issues. Management uses this evaluation to determine the effectiveness of the internal control system. Differences between the results of monitoring activities and the previously established baseline may indicate internal control issues, including undocumented changes in the internal control system or potential internal control deficiencies.

16.10 Management identifies changes in the internal control system that either have occurred or are needed because of changes in the entity and its environment. External parties can also help management identify issues in the internal control system. For example, complaints from the public, regulator comments, and findings from investigations may indicate areas in the internal control system that need improvement. Other external parties that interact with the entity, including relevant suppliers, contractors, and service organizations, may collaborate with management to identify and respond to issues in the entity's business processes and related internal controls. Management considers whether current controls address the identified issues and modifies controls if necessary.

[97] See paras. OV4.03 through OV4.05 for further discussion of service organizations.

Evaluation of Issues

17.05 Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies, including those reported from external audits and evaluations, on a timely basis. Management evaluates issues identified through monitoring activities or reported by personnel to determine whether any of the issues rise to the level of an internal control deficiency. Internal control deficiencies require further evaluation and remediation by management. An internal control deficiency can be in the design, implementation, or operating effectiveness of the internal control and its related process.[100] Management determines from the type of internal control deficiency the appropriate corrective actions to remediate it on a timely basis. Management assigns responsibility and delegates authority for remediating the deficiency.

Corrective Actions

17.06 Management completes and documents, as appropriate, corrective actions to remediate internal control deficiencies, including those reported from external audits and evaluations, on a timely basis. Depending on the nature of the deficiency, either the oversight body or management oversees the prompt remediation of deficiencies by communicating the corrective actions to the appropriate level of the organizational structure and delegating authority for completing corrective actions to appropriate personnel. Documentation of corrective actions may include root-cause analysis, planned actions, interim milestones, completion dates, measurable indicators of compliance and resolution to assess and validate progress throughout the resolution cycle, and the entity official responsible for monitoring the status of the corrective actions.

17.07 Corrective actions may include changes to controls within each of the five components of internal control, such as providing training on identified risks or modifying or adding control activities. Management also updates the entity's periodic risk assessment based on the results of monitoring activities and may consider performing ongoing risk assessments when internal control deficiencies are identified.[101]

17.08 Corrective actions also include resolving audit and evaluation findings.[102] The audit resolution process begins when audit or other

[100]See paras. OV3.07 through OV3.11 for further discussion of evaluation of internal control deficiencies.

[101]See para. 7.02 for further discussion of periodic and ongoing risk assessments.

[102]See para. 16.07 for further discussion of separate evaluations of the internal control system that may result in audit and evaluation findings.

Commented [OMB10]: for a management decision, requirements for corrective action should align with the requirements and guidance of 5 USC Ch. 4, and OMB Circular A-50. For example, OMB Circular A-50 recognizes that written plans for correction action should be provided "where appropriate." Circular A-50 (1982 version).

See also 5 U.S.C. 405(a)(3) (Recognizing that a management decision reflects corrective actions "concluded to be necessary" by management).

information security, and significant internal and external changes that could impact the internal control system. (paragraph 7.15)

- Management documents a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur. (paragraph 9.08)
- Management establishes control activities by documenting in policies what is expected and in procedures specified actions. (paragraph 12.02)
- Management evaluates and documents, as appropriate, the results of ongoing monitoring and separate evaluations to identify internal control issues. (paragraph 16.09)
- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies, including those reported from external audits and evaluations, on a timely basis. (paragraph 17.05)
- Management completes and documents, as appropriate, corrective actions to remediate internal control deficiencies, including those reported from external audits and evaluations, on a timely basis. (paragraph 17.06)

Commented [OMB11]: for a management decision, requirements for corrective action should align with the requirements and guidance of 5 USC Ch. 4, and OMB Circular A-50. For example, OMB Circular A-50 recognizes that written plans for correction action should be provided "where appropriate." Circular A-50 (1982 version).

See also 5 U.S.C. 405(a)(3) (Recognizing that a management decision reflects corrective actions "concluded to be necessary" by management).

- *Information security log analytics* - Management performs log analytics to identify patterns, anomalies, and trends that may represent security incidents involving the entity's information technology. Tools may automatically generate incident alerts to notify management of actions that present a risk, such as changes, access at unusual times, bypassing security measures, or failures in the system.

Responding to Reported Risks and Incidents

Management establishes reporting lines, including separate reporting lines such as whistleblower hotlines, for internal and external parties to communicate information, elevate issues, and report instances of potential fraud, waste, or abuse. Management establishes activities to evaluate information obtained from these reporting lines and adapt the entity's internal control system as needed, including by correcting deficiencies and issues identified, responding to risks, recovering overpayments, and taking appropriate action to respond to fraudulent activity.

Sources of External Data

Management may leverage internal data or coordinate with other entities to obtain or access data to perform control activities, such as data analytics. Examples of data-sharing initiatives with other entities include the following:

- Social Security Administration's (SSA) Full File of Death Information[4] - SSA's compilation of death information it uses to administer its programs, which includes state death records, can provide an additional resource for federal benefit-paying agencies and states to help prevent improper payments and other benefits being incorrectly provided to deceased persons. The Public File of Death Information (also known as the public Death Master File) excludes state death records and is available to other agencies and private organizations.
- Do Not Pay[5] - The Do Not Pay initiative, authorized and governed by the Payment Integrity Information Act of 2019 (PIIA), codified at 31 U.S.C. §§ 3351-58~~operated by the Office of Management and Budget and the Department of the Treasury, provides~~ includes a variety of data-matching and other data-analytics services to all federal and many state agencies to support their efforts to

Commented [OMB12]: OMB does not operate the Do Not Pay Initiative

[4]For more information on the Social Security Administration's data exchange services and to request access to death information, see https://www.ssa.gov/dataexchange/request_dmf.html?tl=0.

[5]For more information on the Do Not Pay initiative and to access the portal, see https://fiscal.treasury.gov/DNP/.

risks. The framework also incorporates steps that PIIA requires program managers to take for certain programs, including routinely assessing how susceptible programs are to significant improper payments and estimating and analyzing improper payments. The framework should be used by federal agencies in conjunction with existing requirements related to managing improper payments, including those stemming from fraud.

OMB Memorandum M-21-19, Transmittal of Appendix C to OMB Circular A-123

In March 2021, OMB published Memorandum M-21-19, *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement*.[5] It provides a comprehensive set of requirements to research the underlying causes of improper payments, balance payment integrity risks and controls, and build the capacity to help prevent future improper payments.

Commented [OMB13]: OMB suggests GAO check whether the footnote remains accurate and up-to-date prior to finalizing the document.

Improper Payments and Fraud: How They Are Related but Different

In December 2023, GAO published *Improper Payments and Fraud: How They Are Related but Different*.[6] This Q&A report describes examples of the relationships and distinctions between improper payments and fraud. It also describes relevant GAO and other federal guidance and executive agency efforts since 2015 to manage and reduce the causes and impacts of improper payments and fraud.

GAO Improper Payments Topic Page

GAO's Improper Payments website provides an issue summary, multimedia resources, and recent reports on improper payments, including steps agencies can take to help reduce improper payments.[7]

[5]Office of Management and Budget, *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement*, OMB Memorandum M-21-19 (Washington, D.C.: Mar. 5, 2021). OMB circulars may periodically be updated, and the current version can be found at https://www.whitehouse.gov/omb/information-for-agencies/circulars/.

[6]GAO, *Improper Payments and Fraud: How They Are Related but Different*, GAO-24-106608 (Washington, D.C.: Dec. 7, 2023).

[7]See GAO, Improper Payments, https://www.gao.gov/improper-payments.

New Documentation Requirements

1. Management would be required to document (1) the results of the risk assessment, including the identification, analysis, and response to risks that are completed on both a periodic and ongoing basis, including consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system (paragraph 7.15) and (2) a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur (paragraph 9.08).

Are these documentation requirements sufficiently clear and understandable?

Risk is inherent to all activities and documentation of all ongoing monitoring and reviews should be documented as appropriate.

These new documentation requirements could be improved by including the phrase “as appropriate” particularly in order to retain the flexibility provided to Management in OV2.10.

This approach aligns with previous guidelines.

OMB suggests GAO consider the burden and impact not retaining flexibility, which may lead to a decreased ability to change risk response in an agile manner when unexpected risk is encountered, or a risk is possibly identified, but not rapidly addressed because of the cost or burden in documentation, versus taking corrective action.

Relevance of Attributes

2. The proposed revision clarifies that management considers all attributes in properly applying the requirements and in assessing, including in summary documentation, whether the principles support the effective design, implementation, and operation of the internal control system (paragraphs OV2.08 through OV2.09 and OV3.10).

Is this application guidance relating to management’s consideration of the relevance of attributes sufficiently clear and understandable?

The requirement for managers to consider all attributes when applying the requirements facilitates a thorough evaluation of the internal control system. This comprehensive approach aids in identifying potential weaknesses that might be missed if only selected attributes were considered. The focus on summary documentation enables management to effectively communicate their assessments and the overall effectiveness of the internal control system.

Collaboration and Responsibility within the Internal Control System

3. The proposed revision clarifies and adds application guidance emphasizing the importance of collaboration between all levels of management on the design, implementation, and operation of the internal control system. It also emphasizes collaboration with the

oversight body, personnel, appropriate functions within the organizational structure, and external parties as applicable. It also emphasizes that the responsibility for the internal control system involves management at all levels and within all functions in the entity's organizational structure (paragraphs OV1.07, OV2.17, 1.03 through 1.04, and 16.10).

Is the application guidance related to collaboration and responsibilities within the internal control system sufficiently clear and understandable?

The proposed revision clarifies and adds application guidance emphasizing the importance of collaboration between all levels of management on the design, implementation, and operation of the internal control system. It emphasizes collaboration with the oversight body, personnel, appropriate functions within the organizational structure, and external parties as applicable. It also emphasizes that the responsibility for the internal control system involves management at all levels and within all functions in the entity's organizational structure (paragraphs OV1.07, OV2.17, 1.03 through 1.04, and 16.10).

External Parties

4. The proposed revision replaced the extant discussion of service organizations with a discussion on external parties. The discussion includes service organizations and other external parties that interact with the entity, including those for which the entity has oversight responsibility (paragraphs OV4.01 through OV4.06). It also discusses control activities that management may perform to fulfill its oversight responsibilities and processes to communicate necessary information to appropriate external parties (paragraphs 10.04 and 15.03 through 15.04).

Is the application guidance sufficiently clear and understandable?

Yes. The guidance on communication processes and control activities involving external parties is detailed and practical. It promotes increased interaction between stakeholders and offers management well-defined steps to follow.

Throughout the Green Book GAO allows for management judgement. Paragraph OV4.05 does not mention judgement or materiality to determine the extent of oversight of service organizations. We suggest materiality be included as a factor to consider in oversight of external parties under paragraph OV4.05.

Application Guidance in the Risk Assessment Component

5. The proposed revision clarifies and adds application guidance throughout the risk assessment component for the following: (1) periodic and ongoing risk assessments (risk assessment overview, paragraphs 7.02, 7.07, 8.03, and 9.02 through 9.03); (2) internal and external risk factors, including examples (paragraphs 7.04 through 7.05, 8.05, 8.07,

8.12, and 8.15 through 8.16); (3) risk identification methods (paragraphs 7.06 and 8.04); and (4) evaluating residual risk (paragraphs 7.03 and 7.13).

Is the application guidance sufficiently clear and understandable?

Yes, the application guidance in the risk assessment component is clear and comprehensive. It provides detailed steps for conducting risk assessments, identifying risks, and evaluating residual risks, which enhances the overall risk management process.

The ongoing risk assessments in 7.02 suggest doing so in real-time and residual risk in 7.03, which should be reinforced. Correspondingly, management should be given continued flexibility on when to document such risk identification and corrective action, as appropriate.

Adds Requirement to Assess Improper Payment and Information Security Risks

6. 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?

As appropriate should be included in 8.03 to not direct agencies to perform assessments when their activities are not payment actions or susceptible to fraud or improper payments.

By explicitly including improper payments and information security risks, the revision targets critical vulnerabilities that can significantly impact an entity's operations and reputation. The detailed application guidance offers reasonable and actionable steps for assessing these risks, thereby enhancing the robustness of the internal control system. Including these requirements within Principle 8 is strategically sound as it consolidates guidance on fraud, improper payments, and information security into a single, comprehensive framework for risk management.

While the valuable intent is appreciated, OMB suggests GAO consider the potential the associated work burden may have to inadvertently reduce risk consideration in other areas not specifically called out as requiring analysis.

Application Guidance Related to Assessing Fraud Risk

7. The proposed revision clarifies and expands on application guidance

for management's consideration of fraud risks, including guidance related to the types of fraud and external fraud risks (paragraphs 8.06 through 8.07).

Is the application guidance sufficiently clear and understandable?

Yes, The expanded guidance aligns with best practices in fraud risk management, significantly enhancing the entity's capabilities to detect and respond to fraud effectively. This approach not only addresses the traditional areas of fraud but also considers the evolving nature of fraudulent activities, especially in a digital and globalized business environment. It provides detailed information on identifying different types of fraud, including external fraud risks, which is essential for robust risk management.

Identifying and Responding to Significant Changes

8. The proposed revision clarifies and expands on application guidance for management's analysis of and response to significant changes and requires documentation of a process for responding to significant changes and related risks so that the internal control system can be quickly adapted as needed to respond to changes once they occur (paragraphs 9.06 and 9.08 through 9.12).

Is the application guidance sufficiently clear and understandable?

Yes, the guidance on identifying and responding to significant changes is clear.

Discrete Processes to Manage Certain Entity Risks

9. The proposed revision promotes developing separate and ongoing processes for managing certain risks as part of the entity's overall internal control system (paragraphs 3.03, 7.12, and 8.20).

Is the application guidance sufficiently clear and understandable?

Yes, the guidance on developing discrete processes for managing certain entity risks is clear and understandable. This approach allows for specialized focus on high-risk areas, ensuring that they are managed effectively within the overall internal control system.

OMB suggests GAO consider the potential the associated work burden may have to inadvertently reduce risk consideration in other areas not specifically called out as requiring analysis.

Categories of Control Activities

10. The proposed revision clarifies and expands the categories of control activities illustrated in principle 10 (paragraph 10.04).

Are these categories of control activities sufficiently clear and understandable?

Yes, the expanded categories of control activities are clear. The detailed examples and explanations provided help to better understand and implement appropriate control activities for various risk scenarios.

Prioritizing Preventive Control Activities

11. The proposed revision emphasizes the importance of designing an appropriate mix of preventive and detective control activities and prioritizing preventive control activities where appropriate (paragraphs 10.09 through 10.11).

Is the application guidance sufficiently clear and understandable?

Yes, the guidance on prioritizing preventive control activities is well-structured. Emphasizing preventive controls ensures that risks are mitigated effectively before they can materialize, which is both cost-efficient and strategic.

However, in Principle 10 and 11 proposed new language, "to mitigate risks" is used instead of "respond to risks". In scenarios where management has chosen to accept or avoid the risk, the term mitigate may not be appropriate.

In addition, Principles 7-9 reference the response to risk, rather than the mitigation of risks. OMB suggests ensuring consistency throughout document.

Changes Related to Information Technology

12. The proposed revision modifies the requirement in principle 11 to focus on general control activities (paragraph 11.01) and modifies and reorganizes the application guidance included in principle 11 (paragraphs 11.02 through 11.17). Information technology control activities and objectives that are not related to general control activities have been moved to principle 10.

Is the application guidance related to information technology in principles 10 and 11 sufficiently clear and understandable?

Yes, the revised guidance on information technology is clear and appropriately detailed. The separation of IT-related control activities between principles 10 and 11 helps to clarify their specific roles and responsibilities within the internal control framework.

Focus of Information and Communication

13. Proposed changes to application guidance in the information and communication component clarify that relevant and quality information

and communication, including information requirements, support the five components of internal control (paragraphs 13.01 through 13.02, 14.01, 14.03, and 15.01).

Is the application guidance sufficiently clear and understandable?

Yes, the guidance on the information and communication component is clear and ensures that all relevant information supports the five components of internal control. This clarity enhances the overall effectiveness of information dissemination and communication within the entity.

Monitoring Component

14. The proposed revision clarifies that monitoring activities are used to evaluate whether each of the five components of internal control is present and functioning or if change is needed (paragraphs 16.02 and 17.07). It also (1) clarifies how management determines the scope and frequency of monitoring activities (paragraph 16.06), (2) explains the distinction between control activities and monitoring activities (see app. II), and (3) provides examples of methods and tools that management could use for monitoring activities (paragraphs 16.04 through 16.06).

Is the application guidance sufficiently clear and understandable?

Yes, the guidance on the monitoring component is clear and comprehensive. It provides detailed instructions on evaluating internal controls, determining the scope and frequency of monitoring, and distinguishing between control and monitoring activities.

New Appendixes

15. The proposed standard includes two new appendixes that provide (1) examples of preventive and detective control activities and (2) references to additional resources that management may leverage in designing, implementing, and operating effective internal control systems to address risk areas related to fraud, improper payments, information security, and the implementation of new or substantially changed programs, including emergency assistance programs.

Is the application guidance sufficiently clear and understandable?

Preventative Controls are important to emphasize as efforts there reduce the risk of fraud or improper payments.

The listing of the Do Not Pay Initiative should cite that it is authorized and governed by the Payment Integrity Information Act of 2019 (PIIA). It is not operated by OMB.

Detective Control Activities in Appendix II can include findings from periodic financial audits performed by OIG or independent auditors. Sources of External Data in the same appendix can be expanded to include Treasury's Invoice Processing Platform (IPP) that is used by federal agencies to pay their invoices with private service providers.