SUPPLEMENTAL MATERIAL FOR GAO-25-107721: Summary of Key Changes in the 2025 Green Book Revision

Accessible Version

This product is a supplement to the 2025 revision of *Standards for Internal Control in the Federal Government* (GAO-25-107721), known as the Green Book.

Background

The 2025 revision of *Standards for Internal Control in the Federal Government* contains changes from, and supersedes, *Standards for Internal Control in the Federal Government* (GAO-14-704G), issued in September 2014.

The 2025 Green Book revision provides requirements, guidance, and resources to help management better address risk areas related to fraud; improper payments; information security; and the implementation of new or substantially changed programs, including emergency assistance programs. Key changes in the 2025 revision include the following:

- New requirement to consider risks related to improper payments and information security when identifying, analyzing, and responding to risks.
- New requirement to document risk assessment results, including the identification, analysis, and response to risks.
- New requirement to document a change assessment process for identifying, analyzing, and responding to risks related to significant changes.
- Two new appendixes that provide additional information related to control activities, examples of sources of data, and references to additional resources that management may leverage in designing, implementing, and operating effective internal control systems to address risks, including areas related to fraud, improper payments, and information security.

The 2025 Green Book revision updates emphasize prioritizing preventive control activities and highlight management's responsibility for internal control at all levels within the entity's organizational structure, such as program and financial managers. Other updates clarify the intent of the standards.

Key Changes by Section

The following table summarizes the key changes in the 2025 Green Book revision and follows the organizational structure of the Green Book (overview, five components, appendixes, and glossary), with paragraph numbers referenced to the right of each change.

Overview

Section 1: Fundamental Concepts of Internal Control	
Definition of Internal Control: Expanded guidance and added figure 3 to define and show the relationship between policies and procedures, controls, and control activities embedded in the internal control process.	Overview (OV)1.04
Definition of an Internal Control System: Clarified the description of an internal control system as well as who is responsible for the internal control system and the limitations of internal control.	OV1.05 - OV1.08
Section 2: Establishing an Effective Internal Control System	
Components, Principles, and Attributes: Clarified the relevance of attributes for establishing an effective internal control system.	OV2.08–OV2.09
Documentation Requirements: Introduced a new subsection to discuss and clarify guidance on minimum documentation requirements (previously located in Section 4, Additional Considerations). Introduced visual markers (a gear symbol and bracketed text) to identify minimum documentation requirements throughout the Green Book.	OV2.10–OV2.13
Internal Control and the Entity: Clarified guidance on functions, business processes, and objective categories.	OV2.14; OV2.16
Roles in an Internal Control System: Clarified that management at all levels within the entity's organizational structure (including program and financial managers) are involved with internal control, as appropriate. Emphasized the importance of collaboration on internal control system design, implementation, and operation.	OV2.19–OV2.20
Objectives of an Entity: Clarified that operation objectives include program, financial, and administrative goals.	OV2.25
Section 3: Evaluation of an Effective Internal Control System	
Evaluation of Internal Control: Expanded guidance related to management's assessment of whether a principle is designed, implemented, and operating effectively.	OV3.10

Section 4: Additional Considerations	
External Parties: Expanded and renamed this subsection (previously titled Service Organizations) to discuss not only service organizations but all external parties relevant to the internal control process.	OV4.01–OV4.07
Information Technology: Introduced a new subsection to discuss the pervasive nature of information technology in entities' business and internal control processes and the need to address evolving security risks to the entity's information technology.	OV4.08–OV4.12
Scalability: Renamed this subsection (previously titled Large versus Small Entities).	OV4.13–OV4.14
Benefits and Costs of Internal Control: Expanded guidance to consider an appropriate mix of preventive and detective control activities as part of management's cost-versus-benefit considerations.	OV4.15–OV4.17
Enterprise Risk Management and Internal Control: Introduced a new subsection to explain the relationship between enterprise risk management and internal control processes.	OV4.18–OV4.19
Control Environment	
Principle 1: Demonstrate Commitment to Integrity and Ethical Values	
Tone at the Top: Expanded the concept of "tone at the top" to emphasize the roles all personnel play in setting the tone of an entity.	1.03
Principle 3: Establish Structure, Responsibility, and Authority	
Organizational Structure: Expanded guidance on the entity's organizational structure and clarified that management adapts the organizational structure, as necessary, to respond to risks and identified deficiencies in the internal control system.	3.03; 3.05
Principle 5: Enforce Accountability	
Enforcement of Accountability: Clarified that management retains responsibility for the effectiveness of controls over the business processes assigned to service organizations.	5.05

Risk Assessment	
Principle 6: Define Objectives and Risk Tolerances	
Definitions of Risk Tolerances: Clarified how management defines and measures risk tolerances related to categories of objectives.	6.09
Principle 7: Identify, Analyze, and Respond to Risks	
Identify Risks: Expanded guidance related to identifying risk on a periodic and ongoing basis, inherent and residual risk, internal and external risk factors, and risk identification methods.	7.02–7.06
Respond to Risks: Expanded guidance related to management's response to risks, including management's consideration of residual risk after designing risk responses. Also added guidance to consider developing separate processes to manage certain risks as part of the entity's overall internal control system.	7.10–7.13
Respond to Risks (New Documentation Requirement): Introduced a new requirement for management to document risk assessment results—including the identification, analysis, and response to risks—that are completed on both a periodic and ongoing basis. This includes documenting the consideration of risks related to fraud, improper payments, information security, and significant internal and external changes that could impact the internal control system.	7.15
Principle 8: Assess Fraud, Improper Payment, and Information Security Risk	
Requirement: Expanded a principle requirement for management to consider risks related to improper payments and information security when identifying, analyzing, and responding to risks.	8.01
Identify Risks Related to Fraud, Improper Payments, and Information Security: Introduced a new section with guidance for identifying risks related to fraud, improper payments, and information security.	8.02–8.05
Types of Fraud and Fraud Risk Factors: Expanded guidance on types of fraud and internal and external fraud risk factors.	8.06–8.10
Types of Improper Payments and Improper Payment Risk Factors: Introduced a new section with guidance on types of improper payments and improper payment risk factors for management to consider.	8.11–8.13

Types of Information Security and Information Security Risk Factors: Introduced a new section with guidance on types of information security risks and information security risk factors for management to consider.	8.14–8.17
Analyze and Respond to Identified Risks: Added guidance on developing separate processes to manage risks related to fraud, improper payments, and information security.	8.20
Principle 9: Identify, Analyze, and Respond to Change	
Identify Significant Changes: Expanded guidance on internal and external conditions that could result in significant changes.	9.02–9.04
Establish a Change Assessment Process: Introduced a new section with guidance on establishing a change assessment process for identifying, analyzing, and responding to risks related to significant changes.	9.05–9.10
Establish a Change Assessment Process (New Documentation Requirement): Introduced a new requirement for management to document a change assessment process.	9.05
Identify, Analyze, and Respond to Risks Related to Significant Changes: Clarified guidance on identifying, analyzing, and responding to risks related to identified significant changes.	9.11–9.13
Control Activities	
Principle 10: Design Control Activities	
Requirement: Clarified that management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.	10.01
Response to Risks: Clarified the definition of control activities and how they support the internal control system.	10.02
Design of Appropriate Types of Control Activities: Clarified considerations for designing control activities. Also, clarified the descriptions of several common control activity categories and added new categories, such as • program-related control activities, • compliance-related control activities, • fraud-related control activities, and • improper payment-related control activities.	10.03–10.04

Design of Automated and Manual Control Activities: Introduced a new section with guidance on the design of automated and manual control activities, which includes a graphic of common categories of information technology control activities and how they align with information processing and information security objectives.	10.05–10.09
Design of Preventive and Detective Control Activities: Introduced a new section with guidance on designing an appropriate mix of preventive and detective control activities, including guidance on prioritizing preventive control activities where appropriate.	10.10–10.13
Design of Control Activities at Various Levels: Clarified guidance on designing entity-level and transaction control activities, including consideration of information processing objectives.	10.14–10.20
Principle 11: Design General Control Activities over Information Technology	
Requirement: Modified the requirement to focus on general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.	11.01
Response to Risks, Design of the Entity's Information Technology, and Design of Appropriate Types of General Control Activities: Significantly reorganized, modified, and expanded the guidance to focus on general control activities. Moved content not focused on general control activities to either principle 8, Assess Fraud, Improper Payment, and Information Security Risk, or principle 10, Design Control Activities.	11.02–11.17
Principle 12: Implement Control Activities	
Requirement: Clarified that management should implement control activities through both policies and procedures.	12.01
Information and Communication	
Principle 13: Use Quality Information	
Requirement: Clarified that management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system.	13.01
Data Processed into Quality Information: Clarified guidance on management processing relevant data obtained or generated from reliable sources into quality information through the entity's information system.	13.05–13.07

Principle 14: Communicate Internally	
Requirement: Clarified that management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the internal control system.	14.01
Communication Throughout the Entity: Clarified guidance on how communications support the internal control system and added examples of communications.	14.03–14.04
Principle 15: Communicate Externally	
Requirement: Clarified that management should communicate relevant and quality information with appropriate external parties regarding matters impacting the internal control system.	15.01
Communication with External Parties: Added examples of communications with external parties.	15.03–15.04
Monitoring	
Principle 16: Perform Monitoring Activities	
Establishment of a Baseline: Clarified that monitoring activities evaluate whether each of the five components of internal control is present and functioning or whether change is needed.	16.02
Internal Control System Monitoring: Clarified how management determines the scope and frequency of monitoring activities, including when programs are new or substantially changed. Expanded examples of monitoring activities, such as improper payment estimates.	16.04–16.06
Principle 17: Evaluate Issues and Remediate Deficiencies	
Evaluation of Issues and Corrective Actions (Documentation Requirements): Clarified that control deficiencies include those reported from internal and external audits and evaluations.	17.05–17.06
Corrective Actions: Added examples of how to document corrective actions and clarified that corrective actions may include changes to controls within each of the five components of internal control. Added that management updates risk assessments based on results of monitoring activities.	17.06–17.07

Appendix II: Examples of Preventive and Detective Control Activities and Sources of Data

New appendix. Supplemented the control activities component and provided additional information on types of activities, examples of preventive and detective control activities, and sources of data.	Not applicable

Appendix III: Additional Resources

New appendix. Provided 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, and information security. These resources may also be useful in addressing risk related to implementing new or substantially changed programs, including emergency assistance programs.	Not applicable

Glossary

Modified or added the following terms:

- application controls
- attributes
- baseline
- business processes
- competence
- complementary user entity controls
- configuration management
- contingency plans/planning
- controls
- control activities
- control objective
- deficiency
- detective control
- entity objective
- entity-level control activities
- general control activities
- improper payment
- information security
- information system
- information technology
- information technology infrastructure
- inherent risk
- internal control system
- likelihood of occurrence
- logical and physical access
- magnitude of impact
- monitoring activities
- organizational structure
- platforms
- policies
- preventive control
- principle
- procedures
- quality information
- security management
- segregation of duties
- service organization
- software
- transaction control activities
- user control activities

Contact

James R. Dalkin, Director, Financial Management and Assurance, DalkinJ@gao.gov

Copyright

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.