United States Government Accountability Office

By the Comptroller General of the United States

May 2025

Standards for Internal Control in the Federal Government

GAO-25-107721

United States Government Accountability Office

By the Comptroller General of the United States

May 2025

Standards for Internal Control in the Federal Government

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

The 2025 revision of *Standards for Internal Control in the Federal Government* is effective beginning with fiscal year 2026 and the FMFIA reports covering that year. Early adoption is permitted.

What is the Green Book and how is it used?

Important facts and concepts related to the Green Book and internal control

Internal control and the Green Book

What is internal control?

Internal control is a process used by management to help an entity achieve its objectives.

How does internal control work?

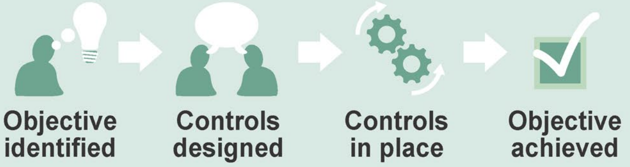
Internal control helps an entity

- Run its operations efficiently and effectively
- Report reliable information about its operations
- Comply with applicable laws and regulations

How is the Green Book related to internal control?

Standards for Internal Control in the Federal Government, known as the Green Book, sets internal control standards for federal entities.

How does an entity use the Green Book?



An entity uses the Green Book to design, implement, and operate internal controls to achieve its objectives related to operations, reporting, and compliance.

Who would use the Green Book?

A program manager at a federal agency

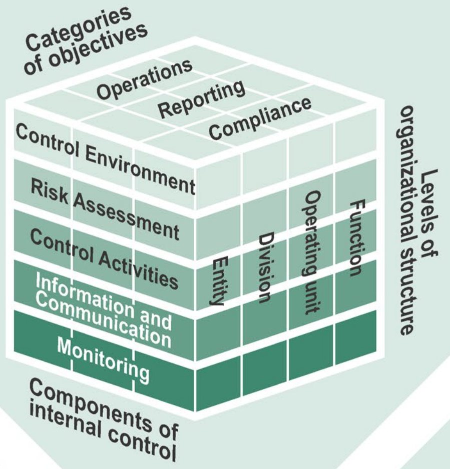
Inspector general staff conducting a financial or performance audit

An independent public accountant conducting an audit of expenditures of federal dollars to state agencies

A compliance officer responsible for making sure that personnel have completed required training

The cube

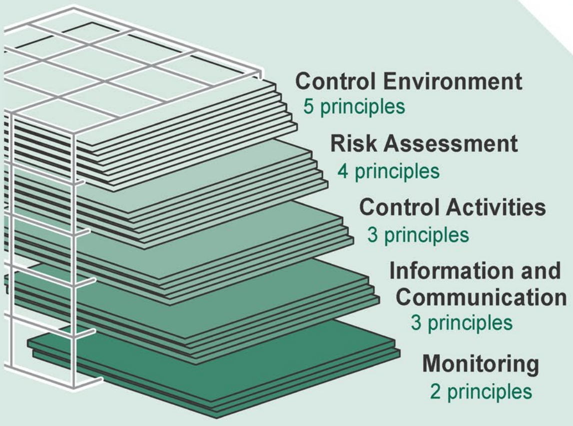
The standards in the Green Book are organized by the five components of internal control shown in the cube below. The five components apply to staff at all organizational levels and to all categories of objectives.



Principles

Principles are the requirements of each component.

There are 17 principles contained within the five components of internal control.

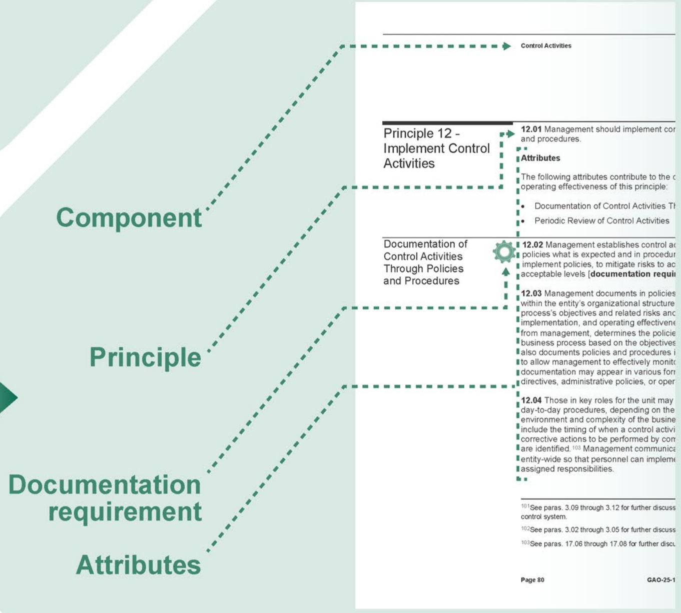


Attributes

Each principle has application guidance, called attributes, that provides further explanation of the principle.

Page structure

Example page showing how components, principles, attributes, and documentation requirements are presented.



Control Activities

Principle 12 - Implement Control Activities

12.01 Management should implement cor and procedures.

Attributes

The following attributes contribute to the c operating effectiveness of this principle:

- Documentation of Control Activities Th
- Periodic Review of Control Activities

Documentation of Control Activities Through Policies and Procedures

12.02 Management establishes control ac policies what is expected and in procedur implement policies, to mitigate risks to ac acceptable levels [**documentation requi**

12.03 Management documents in policies within the entity's organizational structure process's objectives and related risks anc implementation, and operating effectivene from management, determines the policie business process based on the objectives also documents policies and procedures i to allow management to effectively monit documentation may appear in various forr directives, administrative policies, or oper

12.04 Those in key roles for the unit may day-to-day procedures, depending on the environment and complexity of the busine include the timing of when a control activi corrective actions to be performed by con are identified.[103] Management communica entity-wide so that personnel can impleme assigned responsibilities.

[101] See paras. 3.09 through 3.12 for further discuss control system.

[102] See paras. 3.02 through 3.05 for further discuss

[103] See paras. 17.06 through 17.08 for further discu

Page 80 GAO-25-1

Sources: GAO and COSO.

gao.gov/greenbook

Contents

Figures and Table

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Comptroller General
of the United States

Policymakers and managers are continually seeking ways to improve accountability in achieving an entity’s mission. A key factor in this is to implement an effective internal control system. An effective internal control system helps an entity adapt to shifting environments, evolving demands, and changing risks. This includes the challenges managers face when addressing risks related to fraud, improper payments, information security, and implementation of new or substantially changed programs. As new programs are implemented, existing programs are substantially changed, and entities strive to improve processes and implement new information technology, management continually monitors its internal control system so that it is effective and updated when necessary.

Section 3512 (c) and (d) of Title 31 of the United States Code*,* commonly known as the Federal Managers’ Financial Integrity Act of 1982 (FMFIA), requires the Comptroller General to issue standards for internal control in the federal government. FMFIA requires federal executive branch entities to establish internal control in accordance with these standards. *Standards for Internal Control in the Federal Government* (known as the Green Book) provides the overall framework for establishing and maintaining an effective internal control system. The term internal control in this document covers all aspects of an entity’s objectives (operations, reporting, and compliance).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides internal control guidance in its *Internal Control - Integrated Framework*, which introduced the concept of principles related to the five components of internal control.[1] The Green Book adapts these principles for a government environment. Office of Management and Budget Circular A-123, *Management’s Responsibility for Enterprise Risk Management and Internal Control*, provides requirements for federal executive branch agencies to establish a process that management must implement to properly assess and improve internal control.

[1] See Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control - Integrated Framework* (New York: American Institute of Certified Public Accountants, 2013).

The Green Book may also be adopted by federal entities outside the executive branch and by nonfederal entities, such as state, local, and quasi-governmental entities and nonprofit organizations, as a framework for an internal control system. Management of an entity determines, based on applicable laws and regulations, how to appropriately adapt the standards presented in the Green Book as a framework for the entity.

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. This revision provides requirements, guidance, and resources to help managers 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 this 2025 revision include the following:

- The need to consider risks related to improper payments and information security when identifying, analyzing, and responding to risks.
- Documentation of the results of risk assessments, including the identification, analysis, and response to risks.
- Documentation of a change assessment process for identifying, analyzing, and responding to risk related to significant changes so that the internal control system can be quickly adapted as needed to respond to significant changes as they occur.
- 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.

Updates include an emphasis on prioritizing preventive control activities and highlighting management's responsibility for internal control at all levels within the entity's organizational structure, such as program and financial managers. Other updates were made to clarify the intent of the standards and to continue harmonization with COSO's *Internal Control – Integrated Framework*.

The 2025 revision of *Standards for Internal Control in the Federal Government* has gone through an extensive deliberative process, including public comments and input from the Comptroller General's Advisory Council on Standards for Internal Control in the Federal

Government. The advisory council consists of individuals knowledgeable about internal control, drawn from federal, state, and local government; the private sector; and academia. The views of all parties were thoroughly considered in finalizing the standards.

The 2025 revision of *Standards for Internal Control in the Federal Government* is effective beginning with fiscal year 2026 and the FMFIA reports covering that year. Early implementation is permitted.

An electronic version of this document can be accessed at https://www.gao.gov/greenbook.

I appreciate the efforts of government officials, public accounting professionals, and other members of the audit and academic communities who provided valuable assistance in developing these standards. I extend special thanks to the members of the Advisory Council on Standards for Internal Control in the Federal Government for their extensive input and feedback.

Gene L. Dodaro

Gene L. Dodaro
Comptroller General
of the United States

Overview

How to Use the Green Book

Standards for Internal Control in the Federal Government (known as the Green Book) provides managers criteria for designing, implementing, and operating an effective internal control system. It defines the standards through components and principles and explains why they are integral to an entity's internal control system. In a mature and highly effective internal control system, internal control may be indistinguishable from day-to-day activities personnel perform.

The Green Book is structured as follows:

1. An Overview, which includes the following sections:

   Section 1: an overview of the fundamental concepts of internal control
   Section 2: a discussion of internal control components, principles, attributes, and minimum documentation requirements; how these relate to an entity's objectives; and the three categories of objectives
   Section 3: a discussion of the evaluation of the entity's internal control system's design, implementation, and operation
   Section 4: additional considerations that apply to all components in an internal control system

2. A discussion of each of the five components and 17 principles and the related attributes.
3. Appendixes, as follows:

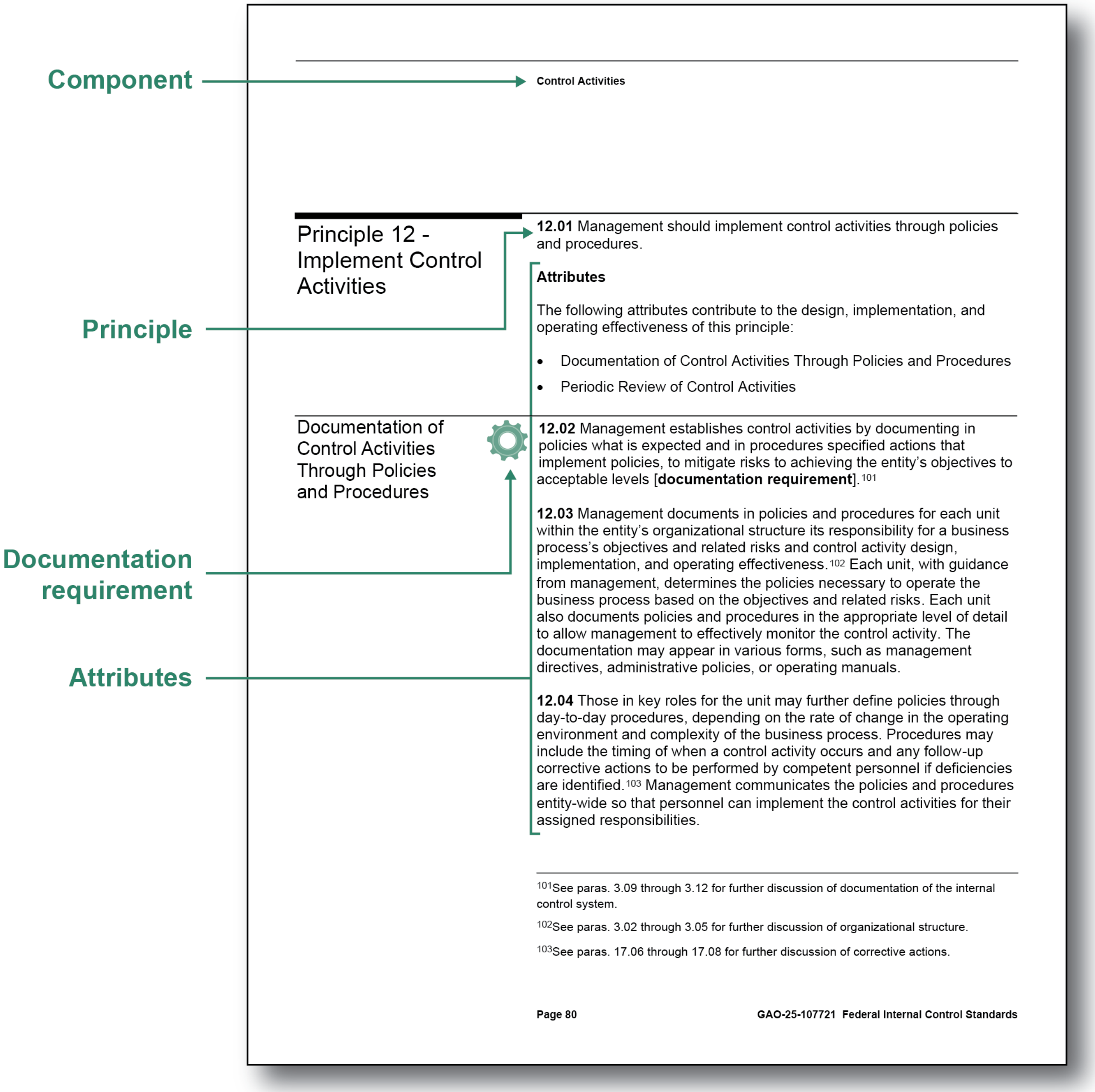
   Appendix I: Requirements
   Appendix II: Examples of Preventive and Detective Control Activities and Sources of Data
   Appendix III: Additional Resources
   Appendix IV: Acknowledgments

4. A Glossary, which includes terms to assist in clarifying the Green Book.

The Green Book indicates the component and principle requirements through the use of "must" and "should." Further discussion of these requirements, as well as documentation requirements, is included in section 2 of the Overview. All requirements are summarized in appendix I.

Figure 1 depicts a sample page from the Green Book. This illustration identifies the components, principles, attributes, and documentation requirements of the Green Book. Documentation requirements are identified throughout the Green Book with a symbol and the wording "[**documentation requirement**]" following the narrative as shown in figure 1.

Figure 1: Green Book Sample Page



Control Activities

Principle 12 - Implement Control Activities

12.01 Management should implement control activities through policies and procedures.

Attributes

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

- Documentation of Control Activities Through Policies and Procedures
- Periodic Review of Control Activities

Documentation of Control Activities Through Policies and Procedures

12.02 Management establishes control activities by documenting in policies what is expected and in procedures specified actions that implement policies, to mitigate risks to achieving the entity's objectives to acceptable levels [**documentation requirement**].[101]

12.03 Management documents in policies and procedures for each unit within the entity's organizational structure its responsibility for a business process's objectives and related risks and control activity design, implementation, and operating effectiveness.[102] Each unit, with guidance from management, determines the policies necessary to operate the business process based on the objectives and related risks. Each unit also documents policies and procedures in the appropriate level of detail to allow management to effectively monitor the control activity. The documentation may appear in various forms, such as management directives, administrative policies, or operating manuals.

12.04 Those in key roles for the unit may further define policies through day-to-day procedures, depending on the rate of change in the operating environment and complexity of the business process. Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified.[103] Management communicates the policies and procedures entity-wide so that personnel can implement the control activities for their assigned responsibilities.

[101] See paras. 3.09 through 3.12 for further discussion of documentation of the internal control system.

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

[103] See paras. 17.06 through 17.08 for further discussion of corrective actions.

Page 80 GAO-25-107721 Federal Internal Control Standards

Source: GAO. | GAO-25-107721

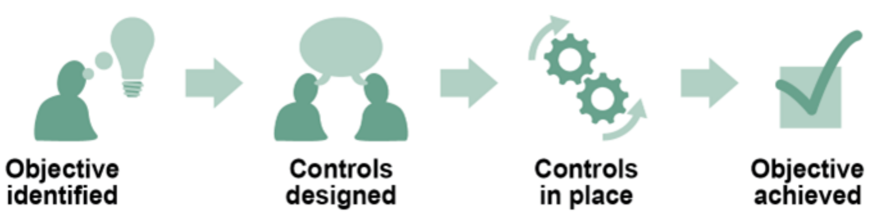
Section 1 - Fundamental Concepts of Internal Control

Definition of Internal Control

OV1.01 Internal control is a process effected by an entity's oversight body, management, and other personnel, designed to provide reasonable assurance that the objectives of an entity will be achieved (see fig. 2). These objectives and related risks can be broadly classified into one or more of the following three categories:

- **Operations -** Effectiveness and efficiency of operations
- **Reporting** - Reliability of reporting for internal and external use
- **Compliance** - Compliance with applicable laws and regulations

Figure 2: Achieving Objectives through Internal Control



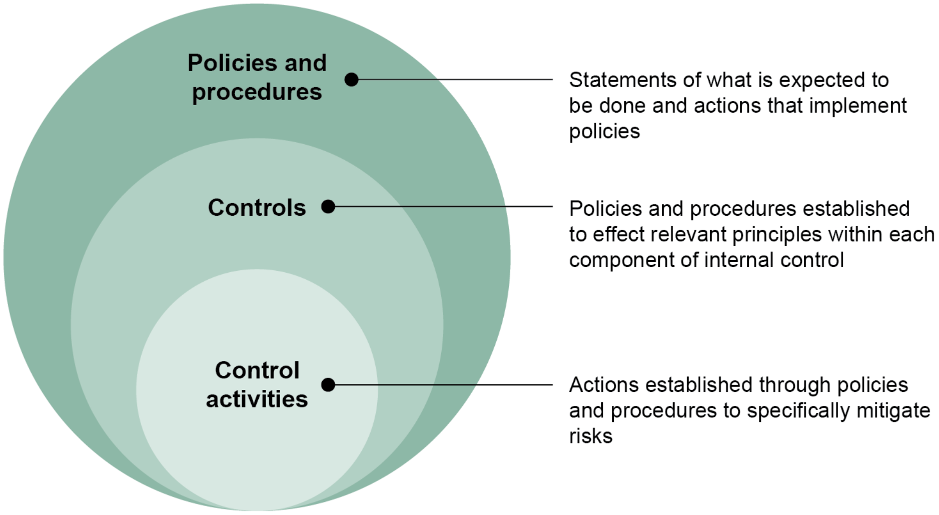
Source: GAO. | GAO-25-107721

OV1.02 These are distinct but overlapping categories. A particular objective can fall under more than one category, can address different needs, and may be the direct responsibility of different individuals.

OV1.03 Internal control comprises the plans, methods, policies, procedures, and other mechanisms used to fulfill the mission, strategic plan, goals, and objectives of the entity. Internal control serves as the first line of defense in safeguarding assets and securing information. In short, internal control helps managers achieve desired results through effective stewardship of the entity's resources.

OV1.04 Embedded in the internal control process are controls. Controls consist of policies and procedures that management establishes to effect relevant principles within each component of internal control. Controls are interrelated and may support multiple principles and entity objectives. Policies reflect management or oversight body statements of what is expected to be done. Procedures consist of actions that implement policies. Policies and procedures that establish controls are a subset of the entity's overall policies and procedures. Embedded within controls are control activities. Control activities are actions that management establishes through policies and procedures as part of the control activities component to specifically mitigate risks to achieving the entity's objectives to acceptable levels. The relationship between policies and procedures, controls, and control activities is depicted in figure 3.

Figure 3: Relationship Between Policies and Procedures, Controls, and Control Activities


Policies and procedures
Statements of what is expected to be done and actions that implement policies
Controls
Policies and procedures established to effect relevant principles within each component of internal control
Control activities
Actions established through policies and procedures to specifically mitigate risks

Source: GAO. | GAO-25-107721

Definition of an Internal Control System

OV1.05 An internal control system consists of integrated and continuous processes, effected by people, that are collectively designed to provide reasonable assurance, not absolute assurance, that an entity's objectives will be achieved.

OV1.06 Internal control is not one event, but a series of actions that occur throughout the entity's activities. Internal control is recognized as an integral part of the processes management uses to achieve its objectives rather than as a separate system within an entity. In this sense, internal control is built into the entity as a part of the organizational structure to help managers achieve the entity's objectives on an ongoing basis.

OV1.07 People are what make internal control work. Management—at all levels within the entity's organizational structure, including program and financial managers—is responsible for an effective internal control system. As part of this responsibility, management sets the entity's objectives, implements controls, and evaluates the internal control system. However, other personnel throughout an entity need to understand the importance of an effective internal control system and play important roles in designing, implementing, and operating an effective internal control system.

OV1.08 An effective internal control system increases the likelihood that an entity will achieve its objectives. However, no matter how well designed, implemented, or operated, an internal control system cannot provide absolute assurance that an entity will meet all its objectives. Factors that can affect the entity's ability to achieve its objectives include events outside the entity's control or influence, faulty or biased management judgments or decisions, human error, management overrides of internal control, collusion, or unsuitable objectives. Therefore, once in place, effective internal control provides reasonable, not absolute, assurance that an entity will achieve its objectives.

Section 2 - Establishing an Effective Internal Control System

Presentation of Standards

OV2.01 The Green Book defines the standards for internal control in the federal government. The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires federal executive branch entities to establish internal control in accordance with these standards. The standards provide criteria for assessing the design, implementation, and operating effectiveness of internal control in federal government entities to determine whether such systems are effective. Nonfederal entities may use the Green Book as a framework to design, implement, and operate an internal control system.[2]

OV2.02 The Green Book applies to all entity objectives: operations, reporting, and compliance. However, these standards are not intended to limit or interfere with duly granted authority related to legislation,

[2] See para. OV4.20 for further discussion of use by other entities.

rulemaking, or other discretionary policymaking in an organization. In implementing the Green Book, management is responsible for designing the internal control system to fit an entity's circumstances and building it in as an integral part of the entity's operations.

Components, Principles, and Attributes

OV2.03 An entity determines its mission, sets a strategic plan, establishes entity objectives, and formulates plans to achieve its objectives. Management, with oversight from the entity's oversight body, may set objectives for an entity as a whole or target activities within the entity. Management uses internal control to help the organization achieve these objectives. While there are different ways to present internal control, the Green Book approaches internal control through a hierarchical structure of five components and 17 principles. The hierarchy includes requirements for establishing an effective internal control system, including minimum documentation requirements.

OV2.04 The five components represent the highest level of the hierarchy of standards for internal control in the federal government. The five components of internal control must be effectively designed, implemented, and operating, and operating together in an integrated manner, for an internal control system to be effective. The five components of internal control are as follows:

- **Control Environment** - The foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives.
- **Risk Assessment** - The identification and analysis of risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.
- **Control Activities** - The actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels.
- **Information and Communication** - The quality information management and other personnel communicate and use to support the internal control system.
- **Monitoring** - Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews.

OV2.05 The 17 principles support the effective design, implementation, and operation of the associated components and represent requirements necessary to establish an effective internal control system.

OV2.06 In general, all components and principles are relevant for establishing an effective internal control system. In rare circumstances, there may be an operating or regulatory situation in which management has determined that a principle is not relevant for the entity to achieve its objectives and mitigate risks. If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale for how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively [**documentation requirement**].

OV2.07 Figure 4 lists the five components of internal control and 17 related principles.

Figure 4: The Five Components and 17 Principles of Internal Control

Control Environment

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider risks related to fraud, improper payments, and information security when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

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

11. Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.

12. Management should implement control activities through policies and procedures.

Information and Communication

13. Management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system.

14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.

15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.

Monitoring

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

17. Management should remediate identified internal control deficiencies on a timely basis.

Source: GAO. | GAO-25-107721

OV2.08 The Green Book also contains application guidance in the form of attributes. Management considers attributes when designing, implementing, and operating the associated principles. Attributes provide further explanation of the principles and may also contain minimum documentation requirements. Attributes may explain more precisely what a requirement means and what it is intended to cover or include examples of procedures that may be appropriate for an entity. Other than the minimum documentation requirements contained within attributes, an attribute does not impose a requirement.

OV2.09 Attributes are relevant to the proper application of the requirements and assessing whether the related principle is designed, implemented, and operating in a manner that supports an effective internal control system. Management has a responsibility to understand the attributes and how they support fulfilling the principle requirements. Management may also identify and consider additional attributes based on specific circumstances of the entity. The Green Book, however, does not prescribe how management designs, implements, and operates an internal control system.

Documentation Requirements

OV2.10 Documentation is a necessary part of an effective internal control system. The level and nature of documentation may vary based on the size of the entity and the complexity of the processes it performs. Management exercises judgment in determining the extent or type of documentation that is needed.

OV2.11 Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system. Management develops and maintains documentation of its internal control system.[3]

The Green Book also includes the following minimum documentation requirements:

- If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale for how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively. (paragraph OV2.06)
- Management documents the results of the risk assessments, including the identification, analysis, and response to risks, that are

[3] See para. 3.09 for this documentation requirement and paras. 3.10 through 3.12 for further discussion of documentation of the internal control system.

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. (paragraph 7.15)

- Management documents a change assessment process for identifying, analyzing, and responding to risks related to significant changes so that the internal control system can be quickly adapted as needed to respond to significant changes as they occur. (paragraph 9.05)
- Management establishes control activities by documenting in policies what is expected and in procedures specified actions that implement policies, to mitigate risks to achieving the entity's objectives to acceptable levels. (paragraph 12.02)
- Management evaluates and documents 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 internal and external audits and evaluations, on a timely basis. (paragraph 17.05)
- Management completes and documents corrective actions to remediate internal control deficiencies, including those reported from internal and external audits and evaluations, on a timely basis. (paragraph 17.06)

OV2.12 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.

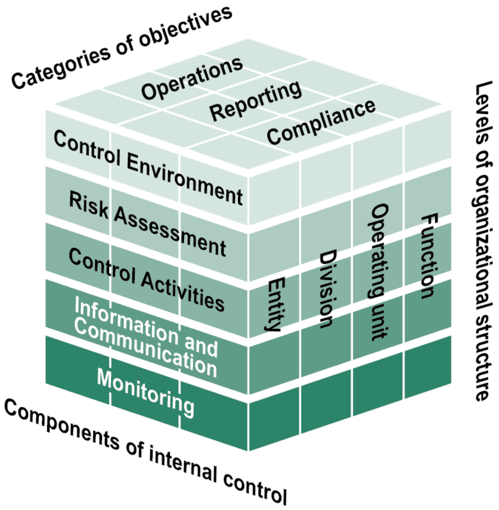
OV2.13 Minimum documentation requirements are identified throughout the Green Book with a symbol and the wording "[**documentation**

requirement]" following the narrative.[4] The minimum documentation requirements are also summarized in appendix I.

Internal Control and the Entity

OV2.14 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 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed (see fig. 5).[5]

Figure 5: The Components, Objectives, and Organizational Structure of Internal Control



Sources: COSO and GAO. | GAO-25-107721

[4] See fig. 1 for an illustration.

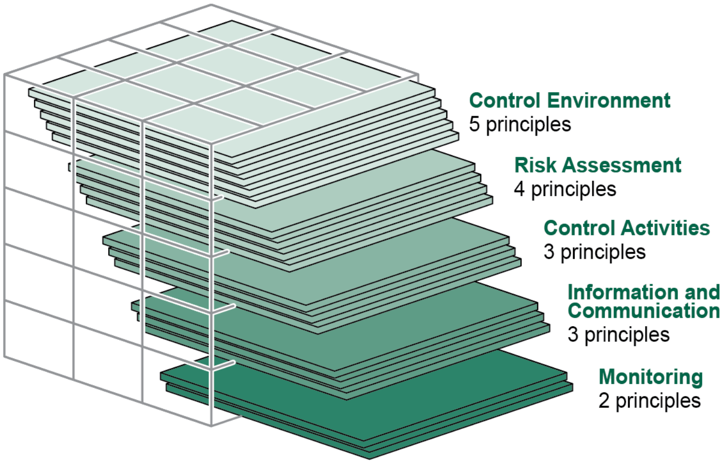
[5] See paras. 3.02 through 3.05 for further discussion of organizational structure.

OV2.15 The three categories into which an entity's objectives can be classified are represented by the columns labeled on top of the cube. The five components of internal control are represented by the rows. The organizational structure is represented by the third dimension of the cube.

OV2.16 The three categories of objectives are not parts of the entity's organizational structure. For instance, operations objectives relate to the effectiveness and efficiency of operations not specific operating units or functions, such as human resources or program offices.

OV2.17 Each component of internal control applies to all three categories of objectives and the organizational structure. The principles support the components of internal control (see fig. 6).

Figure 6: The 17 Principles Supporting the Five Components of Internal Control



Source: GAO. | GAO-25-107721

OV2.18 Internal control is a dynamic, iterative, and integrated process in which components impact the design, implementation, and operating effectiveness of each other. No two entities will have an identical internal control system because of differences in entity factors, such as mission, regulatory environment, strategic plan, size, risk tolerance, and information technology, and in the judgment needed in responding to these differing factors.

Roles in an Internal Control System

OV2.19 Because internal control is a part of management's overall responsibility, the five components are discussed in the context of the management of the entity. However, everyone in the entity has a responsibility for internal control. In general, roles in an entity's internal control system can be categorized as follows:

- **Oversight body** - The oversight body is responsible for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing management's design, implementation, and operation of an internal control system. For some entities, an oversight body might be one or a few members of senior management. For other entities, multiple parties may be members of the entity's oversight body. In the Green Book, oversight by an oversight body is implicit in each component and principle.
- **Management** - Personnel directly responsible for all activities of an entity, including the design, implementation, and operating effectiveness of an entity's internal control system. Management at all levels within the entity's organizational structure is involved as appropriate, including program and financial managers. Managers' responsibilities vary depending on their functions and level in the organizational structure.
- **Other personnel** - Those that help management design, implement, and operate an internal control system. They perform assigned internal control responsibilities and communicate issues noted in the entity's operations, reporting, or compliance objectives.[6]

OV2.20 Collaboration on the design, implementation, and operation of the internal control system is key to an effective internal control system. Collaboration involves the entity's oversight body, management at all levels within the entity's organizational structure, and other personnel, along with the participation of all appropriate functions within the organizational structure and external parties as applicable. For example, program managers, financial managers, and other personnel relevant to achieving an entity's objectives collaborate when designing control activities.

OV2.21 Oversight conducted by external auditors and, if applicable, the office of inspector general (OIG), is not considered a part of an entity's internal control system. While management may evaluate and incorporate recommendations from external auditors and the OIG, responsibility for an entity's internal control system resides with management.

Objectives of an Entity

OV2.22 Management, with oversight by the entity's oversight body, sets objectives to meet the entity's mission, strategic plan, and goals. Objectives are also set to meet requirements for the entity that are established in applicable laws and regulations. Management sets

[6] See paras. 17.02 through 17.04 for further discussion of identifying issues.

objectives before designing an entity's internal control system. Management may include setting objectives as part of the strategic planning process. When designing the internal control system, management balances allocating resources with the degree of risk, complexity, or other factors relevant to achieving the entity's objectives.[7]

OV2.23 Management, as part of designing an internal control system, defines the entity's objectives in specific and measurable terms that enable management to identify, analyze, and respond to risks related to achieving those objectives.

Categories of Objectives

OV2.24 Management groups objectives into one or more of the three categories of objectives:

- **Operations** - Effectiveness and efficiency of operations
- **Reporting** - Reliability of reporting for internal and external use
- **Compliance** - Compliance with applicable laws and regulations

Operations Objectives

OV2.25 Operations objectives relate to achieving an entity's mission, including program, financial, and administrative goals. An entity's mission may be defined in a strategic plan. Such plans set the goals and objectives for an entity along with the effective and efficient operations necessary to fulfill those objectives. Effective operations produce the intended results, while efficient operations do so in a manner that minimizes the waste of resources.

OV2.26 Management can develop, from the objectives, related subobjectives for units within the organizational structure. By linking objectives throughout the entity to the mission, management improves the effectiveness and efficiency of operations in achieving the mission.

Reporting Objectives

OV2.27 Reporting objectives relate to the preparation of reports for use by the entity, its stakeholders, or other external parties. Reporting objectives may be grouped further into the following subcategories:

[7] See paras. OV4.15 through OV4.17 for further discussion of the allocation of resources.

- **External financial reporting objectives** - Objectives related to the release of the entity's financial performance in accordance with professional standards and applicable laws and regulations, as well as expectations of stakeholders.
- **External nonfinancial reporting objectives** - Objectives related to the release of nonfinancial information in accordance with appropriate standards and applicable laws and regulations, as well as expectations of stakeholders.
- **Internal financial reporting objectives and nonfinancial reporting objectives** - Objectives related to gathering and communicating information that management needs to support decision-making and evaluation of the entity's performance.

Compliance Objectives

OV2.28 In the government, objectives related to compliance with applicable laws and regulations are often significant. Laws and regulations often prescribe a government entity's objectives, structure, methods to achieve objectives, and reporting of performance relative to achieving objectives. Management considers objectives in the category of compliance comprehensively for the entity and determines what controls are necessary to design, implement, and operate for the entity to achieve these objectives effectively.

OV2.29 Management conducts activities in accordance with applicable laws and regulations. As part of specifying compliance objectives, the entity determines which laws and regulations apply to the entity. Management is expected to set objectives that incorporate these requirements. Some entities may set objectives to a higher level of performance than established by laws and regulations. In setting those objectives, management can exercise discretion relative to the performance of the entity.

Safeguarding of Assets

OV2.30 A subset of the three categories of objectives is the safeguarding of assets, which is the protection and preservation of entity assets. Management designs an internal control system to provide reasonable assurance regarding prevention or prompt detection and correction of unauthorized acquisition, use, or disposition of an entity's assets.

Setting Subobjectives

OV2.31 Management can develop from objectives more specific subobjectives throughout the organizational structure. Management defines subobjectives in specific and measurable terms that can be communicated to the personnel who are assigned responsibility for achieving these subobjectives. Both management and other personnel require an understanding of an objective, its subobjectives, and defined levels of performance for accountability in an internal control system.

Section 3 - Evaluation of an Effective Internal Control System

OV3.01 The purpose of this section is to provide management with factors to consider in evaluating the effectiveness of an internal control system. The Green Book defines the standards for internal control in the federal government. FMFIA requires federal executive branch entities to establish internal control in accordance with these standards. For federal executive branch entities, Office of Management and Budget (OMB) Circular A-123 provides requirements and guidance on how to evaluate and report on internal control in the federal government. Entities outside the federal executive branch may refer to applicable laws and regulations as well as input from key external stakeholders when determining how to appropriately evaluate and report on internal control.

Factors of Effective Internal Control

OV3.02 An effective internal control system is designed to provide reasonable assurance that the organization will achieve its objectives. As stated in section 2 of the Overview, an effective internal control system has

- each of the five components of internal control effectively designed, implemented, and operating and
- the five components operating together in an integrated manner.

OV3.03 To determine whether an internal control system is effective, management assesses the design, implementation, and operating effectiveness of the five components and 17 principles. If a principle or component is not effective, or the components are not operating together in an integrated manner, then an internal control system cannot be effective.

Evaluation of Internal Control

OV3.04 In the federal government, FMFIA mandates that the head of each executive branch agency annually prepare a statement as to whether the agency’s systems of internal accounting and administrative controls comply with FMFIA requirements. If the systems do not comply, the head of the agency will prepare a report in which any material weaknesses in the agency’s system of internal accounting and administrative controls are identified and the plans and schedule for correcting them are described. OMB issues guidance for evaluating the agency’s systems of internal accounting and administrative controls in OMB Circular A-123. Entities outside the federal executive branch may refer to applicable laws and regulations for guidance in preparing statements regarding internal control.

Design and Implementation

OV3.05 When evaluating the design of a control, management determines whether the control individually and in combination with other controls can address risks related to achieving an entity’s objectives. When evaluating implementation, management determines if the control exists and if the entity has placed the control into operation. A control cannot be effectively implemented if it was not effectively designed. A deficiency in design exists when (1) a control necessary to achieve a control objective is missing or (2) an existing control is not properly designed so that even if the control operates as designed, the control objective would not be achieved. A control objective is the aim or purpose of specified controls to effect relevant principles within each component of internal control. A deficiency in implementation exists when a properly designed control is not implemented correctly in the internal control system.

Operating Effectiveness

OV3.06 In evaluating operating effectiveness, management determines if controls were applied at relevant times during the period under evaluation, the consistency with which they were applied, by whom or by what means they were applied, and whether they were applied as designed. If substantially different controls were used at different times during the period under evaluation, management evaluates operating effectiveness separately for each unique control system. A control cannot be effectively operating if it was not effectively designed and implemented. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

Effect of Deficiencies on the Internal Control System

OV3.07 Management evaluates control deficiencies identified through its ongoing monitoring of the internal control system as well as any separate evaluations that internal and external parties perform. A deficiency in internal control exists when the design, implementation, or operation of a control does not allow management or other personnel, in the normal course of performing their assigned responsibilities, to achieve the entity's objectives.

OV3.08 Management evaluates the significance of identified deficiencies. Significance refers to the relative importance of a deficiency to the entity's achieving a defined objective. To evaluate the significance of the deficiency, management assesses its effect on achieving the defined objectives at both the entity and transaction levels.[8] Management evaluates the significance of a deficiency by considering the following:

- **Magnitude of impact -** The likely effect that the deficiency could have on the entity achieving its objectives and is affected by factors such as the size, pace, and duration of the deficiency's impact. A deficiency may be more significant to one objective than another.
- **Likelihood of occurrence -** The possibility of a deficiency impacting an entity's ability to achieve its objectives.
- **Nature of the deficiency -** Factors such as the degree of subjectivity involved with the deficiency and whether the deficiency arises from potential fraud or misconduct.

The oversight body oversees management's evaluation of the significance of deficiencies so that deficiencies have been properly considered.

OV3.09 Deficiencies are evaluated both on an individual basis and in the aggregate. Management considers the correlation among different deficiencies or groups of deficiencies when evaluating their significance. Deficiency evaluation varies by entity because of differences in entities' objectives.

OV3.10 For each principle, management makes a summary determination of whether the principle is designed, implemented, and operating effectively. If a principle is not designed, implemented, or operating effectively, then the respective component cannot be effective. Management considers attributes in assessing whether the related principle is designed, implemented, and operating effectively, as attributes are relevant to the proper application of the principle

[8] See paras. 10.14 through 10.20 for further discussion of entity-level and transaction-level control activities.

requirements.[9] Management also considers the impact of deficiencies identified in achieving documentation requirements as part of this summary determination.[10]

OV3.11 Based on the results of the summary determination for each principle, management concludes on the design, implementation, and operating effectiveness of each of the five components of internal control. Management also considers whether the five components operate together effectively. If one or more of the five components are not effectively designed, implemented, or operating, or if they are not operating together in an integrated manner, then an internal control system is ineffective. Judgment is used in making such determinations, which includes exercising reasonable care.

Section 4 - Additional Considerations

External Parties

OV4.01 Management interacts with external parties regarding matters impacting the functioning of the internal control system. External parties can be service organizations that manage business processes on behalf of the entity, organizations for which the entity has oversight responsibilities, and other parties interacting with the entity.

OV4.02 Management involves external parties, as necessary, or uses information obtained from external parties when designing, implementing, and operating an effective internal control system. Open communication with external parties allows information to be shared to identify risks, trends, events, or circumstances that may impact achieving the entity's objectives.[11]

Service Organizations

OV4.03 Management may engage external parties to perform certain business processes for the entity, such as accounting and payroll processing, security services, or health care claims processing.

[9] See paras. OV2.03 through OV2.09 for further discussion on the relationship of components, principles, and attributes.

[10] See paras. OV2.10 through OV2.13 for further discussion of documentation requirements.

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

Management may also engage external parties to provide services in support of business processes, such as information systems services and information technology procurement and maintenance services. In the Green Book, these external parties are referred to as service organizations.[12] Management retains responsibility for the effectiveness of controls over business processes assigned to service organizations. When controls performed by a service organization are necessary for the entity to achieve its control objectives, these controls are considered part of the entity's system of internal control. Therefore, management needs to understand the controls that service organizations design, implement, and operate for assigned business processes. The entity may also implement its own controls to achieve control objectives that are related to the processes performed by the service organization.

OV4.04 If controls a service organization performs are necessary to achieve the entity's control objectives, the entity implements any complementary user entity controls and other controls, as appropriate, related to the use of the service organization. Complementary user entity controls are those controls that a service organization identifies as necessary for the entity to implement to achieve the control objectives specified by the service organization. Other controls may include those related to establishing two-way communication with service organizations and monitoring the effectiveness of the design, implementation, and operation of service organizations' controls in achieving the entity's control objectives.[13]

OV4.05 Management exercises judgment in determining the extent of oversight for the business processes assigned to a service organization. Management may consider the following in making this determination:

- the nature and significance of services outsourced;
- previous experience with the service organization;
- the service organization's standards of conduct;

[12] Service organizations may further outsource assigned business processes to other organizations. These organizations may be referred to as subservice organizations. The Green Book does not distinguish between service organizations and subservice organizations. References to service organizations include organizations to which business processes are further assigned.

[13] See para. 16.08 for further discussion of monitoring the business processes and related controls that service organizations perform.

- the quality and frequency of the service organization’s enforcement of adherence to standards of conduct by its personnel;
- the scale and level of complexity of the service organization’s operations and organizational structure;
- the service organization’s adoption of, and compliance with, relevant standards, such as those relating to quality management, supply chain management, and information security;
- available information on service organization operational and control effectiveness and related risks, such as that in attestation reports, performance audit reports, and performance metrics; 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.

Organizations for Which the Entity Has Oversight Responsibilities

OV4.06 Management also interacts with external parties for which the entity has oversight responsibilities. These may include those that are regulated by the entity, administer programs on behalf of the entity, or receive federal financial assistance (such as loans or 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.

Other Parties Interacting with the Entity

OV4.07 Management may interact with other external parties to obtain or share information relevant to the entity’s internal control system. These external parties include suppliers, contractors, regulators, external auditors, federal entities, state and local governments, and the public. This may include information from legal or regulatory requirements or data-sharing agreements with other government entities.[14]

Information Technology

OV4.08 Information technology may be essential to achieving the entity’s objectives and better controlling its business processes. Entities and individuals are increasingly interconnected through the use of information

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

technology, while the types of information technology and the ways it is used evolve rapidly.

OV4.09 The information technology used in the entity's automated processes is often referred to by other terms, such as information systems or technology. In the Green Book, information technology refers to the infrastructure, platforms, and software used to automate processes.[15] In the Green Book, information system refers more broadly to 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.[16] The protection of information and information technology is also referred to by multiple terms, including information security and cybersecurity. In the Green Book, information security refers to the protection of information or information technology from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. Information security includes protecting the entity against cyberattacks.

OV4.10 Information technology may be incorporated into business processes to reduce the risk of human error and enhance efficiency. 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. Information technology may also be used to automate control activities to enhance internal control over the processing and security of information.[17]

OV4.11 The use of information technology—particularly new or emerging technologies—by an entity creates both opportunities and risks. It can enable innovation and generate efficiencies through automation. It may also increase complexity, which makes identifying and managing risks more difficult.[18] Management allocates appropriate resources, including personnel, to maintain and secure the entity's information technology. Management designs appropriate general control activities to mitigate

[15] See paras. 11.03 through 11.06 for further discussion of the entity's information technology.

[16] See para. 13.05 for further discussion of the entity's information system.

[17] See paras. 10.05 through 10.07 for further discussion of automated control activities.

[18] See paras. 8.14 through 8.17 for further discussion of risks related to information security.

information security risks. General control activities support the proper operation of the entity’s information technology by creating a suitable environment for effective operation of application and user control activities.[19]

OV4.12 The principles presented in the Green Book do not change with the application of information technology; however, technology may change how internal control is designed. Management considers the greater availability of information and the use of automated processes as it designs, implements, and operates the entity’s internal control system. Information technology may be integrated into all components of internal control to achieve the entity’s objectives.

Scalability

OV4.13 The 17 principles apply to both large and small entities. However, smaller entities may have different implementation approaches than larger entities. Smaller entities typically have unique advantages, which can contribute to an effective internal control system. These may include a higher level of involvement by management in processes and direct interaction with personnel. Smaller entities may find informal staff meetings effective for communicating quality information to support the internal control system, whereas larger entities may need more formal mechanisms—such as written reports, intranet portals, or periodic formal meetings—to communicate with the organization.

OV4.14 A smaller entity, however, faces greater challenges in segregating duties because of its concentration of responsibilities and authorities in the organizational structure.[20] Management can respond to this increased risk through the design of the internal control system, for example, by adding additional levels of review for key processes, reviewing randomly selected transactions and their supporting documentation, taking periodic asset counts, or checking supervisor reconciliations.

Benefits and Costs of Internal Control

OV4.15 Internal control provides many benefits to an entity. It provides management with added confidence regarding the achievement of objectives, provides feedback on how effectively an entity is operating, and helps reduce risks affecting the achievement of the entity’s objectives. Management considers a variety of cost factors in relation to expected benefits when designing and implementing internal controls.

[19] See paras. 11.07 through 11.17 for further discussion of general control activities over information technology and para. 10.07 for further discussion of application and user control activities.

[20] See paras. 10.21 through 10.23 for further discussion of segregation of duties.

Cost factors may include the time and resources required to design, implement, and operate effective internal controls. The complexity of the cost-benefit determination is compounded by the interrelationship of controls with processes. Where controls are integrated within processes, it is difficult to isolate either their benefits or costs.

OV4.16 When designing control activities, management selects an appropriate mix of preventive and detective control activities to adequately and timely mitigate risks. Management prioritizes preventive control activities where appropriate and considers the benefits and costs of either preventing or detecting and correcting an unintended event or result in the entity's operations.[21] Preventive control activities generally offer the most cost-efficient use of resources and help management avoid difficult and expensive remediation efforts, such as the "pay and chase model," where efforts are made to detect and correct an unintended event or result after it occurs. There may be more monetary or nonmonetary costs to the entity when correcting an unintended event or result that has already occurred, rather than trying to prevent it, and the recovery of losses, such as improper payments, may not be possible.

OV4.17 Management decides how an entity evaluates the benefits versus costs of various approaches to implementing an effective internal control system. However, cost alone is not an acceptable reason to avoid implementing internal controls. The costs versus benefits considerations support management's ability to effectively design, implement, and operate an internal control system that balances allocating resources with the degree of risk, complexity, or other factors relevant to achieving the entity's objectives.

Enterprise Risk Management and Internal Control

OV4.18 Enterprise risk management is a strategic process applied across the entity designed to identify potential events that may affect the entity, manage risk, and provide reasonable assurance that an entity's objectives will be achieved. It is part of an entity's overall governance and accountability process and encompasses more than internal control.

OV4.19 Internal control is an integral part of enterprise risk management that focuses on achieving specified operations, reporting, and compliance

[21] See paras. 10.10 through 10.13 for further discussion of preventive and detective control activities.

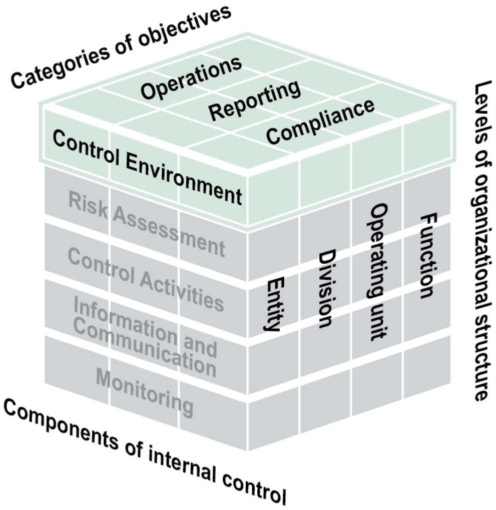
objectives.[22] The Green Book does not prescribe how management implements an enterprise risk management process.

Use by Other Entities

OV4.20 The Green Book may be applied as a framework for an internal control system by federal entities outside the executive branch and by nonfederal entities, such as state, local, and quasi-governmental entities and nonprofit organizations. Management of the entity determines, based on applicable laws and regulations, how to appropriately adapt the standards presented in the Green Book as a framework for the entity. If entity management elects to adopt the Green Book as criteria, management follows all relevant requirements presented in these standards.

[22] See para. OV1.01 for further discussion of the entity's objectives.

Control Environment



Sources: COSO and GAO. | GAO-25-107721

Overview

The control environment is the foundation for an effective internal control system. It provides the discipline and structure, which affect the overall quality of internal control. It influences how objectives are defined and how control activities are structured. The oversight body and management establish and maintain an environment throughout the entity that sets a positive attitude toward internal control.

Principles

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.
2. The oversight body should oversee the entity's internal control system.
3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Principle 1 - Demonstrate Commitment to Integrity and Ethical Values

1.01 The oversight body and management should demonstrate a commitment to integrity and ethical values.

Attributes

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

- Tone at the Top
- Standards of Conduct
- Adherence to Standards of Conduct

Tone at the Top

1.02 The oversight body and management demonstrate the importance of integrity and ethical values through their directives, attitudes, and behavior.

1.03 The oversight body and management lead by an example that demonstrates the organization’s values, philosophy, and operating style. The oversight body and management set the tone at the top and throughout the organization by their example, which is fundamental to an effective internal control system. In larger entities, the various layers of management in the organizational structure may also set the “tone in the middle.” Although it is the oversight body and management’s responsibility to set the tone at the top, other personnel throughout the entity play an important role in supporting the tone that permeates the organizational culture.

1.04 The oversight body’s and management’s directives, attitudes, and behaviors reflect the integrity and ethical values expected throughout the entity. The oversight body and management reinforce the commitment to doing what is right, not just maintaining a minimum level of performance necessary to comply with applicable laws and regulations, so that these priorities are understood by all stakeholders, such as regulators, service organizations, employees, and the public.

1.05 Tone at the top can be either a driver, as shown in the preceding paragraphs, or a barrier to internal control. Without a strong tone at the top to support an internal control system, the entity’s risk identification may be incomplete, risk responses may be inappropriate, control activities may not be appropriately designed or implemented, information and communication may falter, and results of monitoring may not be understood or acted upon to remediate deficiencies.

Standards of Conduct

1.06 Management establishes standards of conduct to communicate expectations concerning integrity and ethical values. The entity uses ethical values to balance the needs and concerns of different stakeholders, such as regulators, service organizations, employees, and the public. The standards of conduct guide the directives, attitudes, and behaviors of the organization in achieving its objectives.

1.07 Management, with oversight from the oversight body, defines the organization’s expectations of ethical values in the standards of conduct. Management may consider using policies, operating principles, guidelines, or training to regularly communicate and reinforce the standards of conduct to the organization.

Adherence to Standards of Conduct

1.08 Management establishes processes to evaluate performance against the entity’s expected standards of conduct and address any deviations in a timely manner.

1.09 Management uses established standards of conduct as the basis for evaluating adherence to integrity and ethical values across the organization. Management evaluates the adherence to standards of conduct across all levels of the entity. To gain assurance that the entity’s standards of conduct are implemented effectively, management evaluates the directives, attitudes, and behaviors of individuals and teams. Evaluations may consist of ongoing monitoring or separate evaluations.[23] Individual personnel can also report issues through reporting lines, such as regular staff meetings, upward feedback processes, a whistleblowing program, or an ethics hotline.[24] The oversight body evaluates management’s adherence to the standards of conduct as well as the overall adherence by the entity.

1.10 Management determines tolerance levels for deviations from standards of conduct. For instance, management may determine that the entity will have zero tolerance for deviations from certain expected standards of conduct, while deviations from others may be addressed with warnings to personnel. Management establishes a process for evaluations of individual and team adherence to standards of conduct that escalates and remediates deviations timely and consistently. Management, with oversight from the entity’s oversight body and with

[23] See paras. 16.04 through 16.09 for further discussion of ongoing monitoring and separate evaluations.

[24] See paras. 14.04 through 14.06 for further discussion of upward and separate reporting lines.

consideration of applicable laws and regulations, takes appropriate actions to remediate deviations.

Principle 2 - Exercise Oversight Responsibility

2.01 The oversight body should oversee the entity's internal control system.

Attributes

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

- Oversight Structure
- Oversight for the Internal Control System
- Input for Remediation of Deficiencies

Oversight Structure

2.02 The entity determines an oversight structure to fulfill responsibilities set forth by applicable laws and regulations, relevant government guidance, and feedback from key stakeholders. The entity will select, or if mandated by law will have selected for it by an applicable body, an oversight body. When the oversight body is composed of entity management, activities referenced in the Green Book as performed by “management” exclude these members of management when in their roles as the oversight body.

Responsibilities of an Oversight Body

2.03 When the oversight structure of an entity is led by senior management, senior management may distinguish itself from divisional or functional management by establishing an oversight body. An oversight body oversees the entity's operations; provides constructive criticism to management; and where appropriate, makes oversight decisions so that the entity achieves its objectives in alignment with its integrity and ethical values. Members of an oversight body review management's activities, present alternative views, and act when faced with actual or suspected wrongdoing.

Qualifications for an Oversight Body

2.04 In selecting members for an oversight body, the entity or applicable body defines the entity knowledge, relevant expertise, number of members, and possible independence needed to fulfill the oversight responsibilities for the entity.

2.05 Members of an oversight body understand the entity's objectives, its related risks, and expectations of its stakeholders. In addition to an oversight body, an organization within the federal government may have several bodies that are key stakeholders for the entity, such as the White House, Congress, the Office of Management and Budget, and the Department of the Treasury. An oversight body works with key stakeholders to understand their expectations and help the entity fulfill these expectations if appropriate.

2.06 The entity or applicable body also considers the expertise members need to oversee, question, and evaluate management. Capabilities expected of all members of an oversight body include integrity and ethical values, leadership, critical thinking, and problem-solving abilities.

2.07 Further, in determining the number of members of an oversight body, the entity or applicable body considers the need for members of the oversight body to have specialized skills to enable discussion, offer constructive criticism to management, and make appropriate oversight decisions. Some specialized skills may include the following:

- Internal control mindset (e.g., professional skepticism and perspectives on approaches for identifying and responding to risks and assessing the effectiveness of the internal control system).
- Programmatic expertise, including knowledge of the entity's mission, programs, and business processes (e.g., procurement, human capital, and functional management expertise).
- Financial expertise, including financial reporting (e.g., accounting standards and financial reporting requirements and budgetary expertise).
- Relevant information technology expertise (e.g., understanding critical systems, information security practices, and technology risks and opportunities).
- Legal and regulatory expertise (e.g., understanding of applicable laws and regulations).

2.08 If authorized by applicable laws and regulations, the entity may also consider including independent members as part of an oversight body.[25] Independent members with relevant expertise provide value through their

[25] See GAO, *Government Auditing Standards: 2024 Revision,* GAO-24-106786 (Washington, D.C.: February 2024), para. 3.21, for further discussion of independence.

impartial evaluation of the entity and its operations in achieving objectives.

Oversight for the Internal Control System

2.09 The oversight body oversees management's design, implementation, and operation of the entity's internal control system. The oversight body's responsibilities for the entity's internal control system include the following:

- **Control Environment** - Establish integrity and ethical values, develop expectations of competence, and maintain accountability to all members of the oversight body and key stakeholders.
- **Risk Assessment** - Oversee management's assessment of risks to achieving objectives, including risks related to fraud, improper payments, information security, identified and potential changes, and management override of internal control.
- **Control Activities** - Provide oversight to management in the development and performance of control activities.
- **Information and Communication** - Analyze and discuss information relating to the entity's achievement of objectives.
- **Monitoring** - Scrutinize the nature and scope of management's monitoring activities as well as its evaluation and remediation of identified deficiencies.

2.10 These responsibilities are supported by the organizational structure that management establishes.[26] The oversight body oversees management's design, implementation, and operation of the entity's organizational structure so that the processes necessary to enable the oversight body to fulfill its responsibilities exist and are operating effectively.

Input for Remediation of Deficiencies

2.11 The oversight body provides input to management's plans for remediation of deficiencies in the internal control system as appropriate.

2.12 Management reports deficiencies identified in the internal control system to the oversight body. The oversight body oversees and provides direction to management on the remediation of these deficiencies. The oversight body also provides direction when a deficiency crosses organizational boundaries or units, or when the interests of management may conflict with remediation efforts. When appropriate and authorized,

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

the oversight body may direct the creation of teams to address or oversee specific matters critical to achieving the entity’s objectives.

2.13 The oversight body is responsible for overseeing the remediation of deficiencies as appropriate and for providing direction to management on appropriate time frames for correcting these deficiencies.[27]

Principle 3 - Establish Structure, Responsibility, and Authority

3.01 Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity’s objectives.

Attributes

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

- Organizational Structure
- Assignment of Responsibility and Delegation of Authority
- Documentation of the Internal Control System

Organizational Structure

3.02 Management establishes the organizational structure necessary to enable the entity to plan, execute, control, and assess the organization in achieving its objectives. Management develops the overall responsibilities from the entity’s objectives that enable the entity to achieve its objectives and address related risks.

3.03 Management develops an organizational structure with an understanding of the overall responsibilities and assigns these responsibilities to enable the organization to operate efficiently and effectively, comply with applicable laws and regulations, and reliably report information. Based on the nature of the assigned overall responsibility and related risks, management chooses the type and number of discrete divisions, operating units, functions, and other structures needed to achieve the entity’s objectives. Management may identify discrete divisions, operating units, or functions, such as program offices and related subunits, to manage the entity’s risk responses within the internal control system.

3.04 As part of establishing an organizational structure, management considers how divisions, operating units, functions, and other structures interact to fulfill their overall responsibilities. Management establishes

[27] See para. 17.06 for further discussion of timely remediation of findings.

reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities to support the internal control system.[28] Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure.[29] Management also considers the entity's overall responsibilities to external stakeholders and establishes reporting lines that allow the entity to both communicate with and obtain information from external stakeholders.[30]

3.05 Management periodically evaluates the organizational structure so that it meets the entity's objectives and has adapted to any new entity objectives, such as to comply with a new law or regulation. Management also adapts the organizational structure as necessary to respond to risks and identified deficiencies in the internal control system.

Assignment of Responsibility and Delegation of Authority

3.06 To achieve the entity's objectives and address related risks, management assigns responsibility and delegates authority to key roles throughout the entity. A key role is a position in the organizational structure that is assigned an overall responsibility of the entity. Generally, key roles relate to senior management positions within an entity.

3.07 Management considers the overall responsibilities assigned across the organizational structure, determines what key roles are needed to fulfill the assigned responsibilities, and establishes the key roles. Those in key roles can further assign responsibility for internal control to roles below them in the organizational structure, but they retain ownership for fulfilling the overall responsibilities assigned to them.

3.08 Management determines what level of authority each key role needs to fulfill a responsibility. Management delegates authority only to the extent required to achieve the entity's objectives. As part of delegating authority, management evaluates each delegation for proper segregation of duties within the organizational structure. Segregation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure.[31] As with assigning responsibility, those in key roles can

[28] See principle 13 for further discussion of the use of quality information.

[29] See paras. 14.02 through 14.06 for further discussion of internal reporting lines.

[30] See paras. 15.02 through 15.06 for further discussion of external reporting lines.

[31] See paras. 10.21 through 10.23 for further discussion of segregation of duties.

delegate their authority for internal control to roles below them in the organizational structure.

Documentation of the Internal Control System

3.09 Management develops and maintains documentation of its internal control system [**documentation requirement**].

3.10 Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, and to communicate that knowledge as needed to external parties, such as external auditors.

3.11 Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

3.12 The extent of documentation needed to support the design, implementation, and operating effectiveness of the five components of internal control is a matter of judgment for management. Management considers the benefits and costs of documentation for the entity as well as the size, nature, and complexity of the entity and its objectives. Some level of documentation, however, is necessary so that the components of internal control can be designed, implemented, and operating effectively.[32]

Principle 4 - Demonstrate Commitment to Competence

4.01 Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

Attributes

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

- Expectations of Competence
- Recruitment, Development, and Retention of Individuals
- Succession and Contingency Plans and Preparation

[32] See paras. OV2.10 through OV2.13 for further discussion of minimum documentation requirements.

Expectations of Competence

4.02 Management establishes expectations of competence for key roles, and other roles at management's discretion, to help the entity achieve its objectives. Competence is the capability to carry out assigned responsibilities. It requires relevant knowledge, skills, and abilities, which are gained largely from professional experience, training, and certifications. It is demonstrated by the behavior of individuals as they carry out their responsibilities.

4.03 Management considers standards of conduct, assigned responsibility, and delegated authority when establishing expectations. Management establishes expectations of competence for key roles. Management may also establish expectations of competence for all personnel through policies within the entity's internal control system.

4.04 Personnel need to possess and maintain a level of competence that allows them to accomplish their assigned responsibilities, as well as understand the importance of effective internal control. Holding personnel accountable to established policies by evaluating their competence is integral to attracting, developing, and retaining individuals. Management evaluates competence of personnel across the entity in relation to established policies. Management acts as necessary to address any deviations from the established policies. The oversight body evaluates the competence of management as well as the competence overall of entity personnel.

Recruitment, Development, and Retention of Individuals

4.05 Management recruits, develops, and retains competent personnel to achieve the entity's objectives. Management considers the following:

- **Recruit -** Conduct procedures to determine whether a particular candidate fits the organizational needs and has the competence for the proposed role.
- **Train -** Enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.
- **Mentor -** Provide guidance on the individual's performance based on standards of conduct and expectations of competence, align the individual's skills and expertise with the entity's objectives, and help personnel adapt to an evolving environment.
- **Retain -** Provide incentives to motivate and reinforce expected levels of performance and desired conduct, including training and credentialing as appropriate.

Succession and Contingency Plans and Preparation

4.06 Management defines succession and contingency plans for key roles to help the entity continue achieving its objectives. Succession plans address the entity's need to replace competent personnel over the long term, whereas contingency plans address the entity's need to respond to sudden personnel changes that could compromise the internal control system.

4.07 Management defines succession plans for key roles, chooses succession candidates, and trains succession candidates to assume the key roles. If management relies on a service organization to fulfill the assigned responsibilities of key roles in the entity, management assesses whether the service organization can continue in these key roles, identifies other candidate organizations for the roles, and implements processes to enable knowledge sharing with the succession candidate organization.

4.08 Management defines contingency plans for assigning responsibilities if a key role in the entity is vacated without advance notice. The importance of the key role in the internal control system and the impact to the entity of its vacancy dictates the formality and depth of the contingency plan.

Principle 5 - Enforce Accountability

5.01 Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Attributes

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

- Enforcement of Accountability
- Consideration of Excessive Pressures

Enforcement of Accountability

5.02 Management enforces accountability of individuals performing their internal control responsibilities. Accountability is driven by the tone at the top and supported by commitment to integrity and ethical values, organizational structure, and expectations of competence, which influence the control culture of the entity. Accountability for performance of internal control responsibility supports day-to-day decision-making, attitudes, and behaviors. Management holds personnel accountable through mechanisms such as performance appraisals and disciplinary actions.

5.03 Management holds personnel accountable for performing their assigned internal control responsibilities. The oversight body, in turn, holds both management and the entire organization accountable for its internal control responsibilities.

5.04 If management establishes incentives, management recognizes that such actions can yield unintended consequences and evaluates incentives so that they align with the entity's standards of conduct.

5.05 Management holds service organizations accountable for their assigned internal control responsibilities. Management may contract with service organizations to perform roles in the organizational structure. Management communicates to each service organization the objectives of the entity and their related risks, the entity's standards of conduct, the role of the service organization in the organizational structure, the assigned responsibilities and authorities of the role, and the expectations of competence for its role that will enable a service organization to perform its internal control responsibilities. Management, however, retains responsibility for the effectiveness of controls over the business processes assigned to service organizations.

5.06 Management, with oversight from the oversight body, takes corrective action as necessary to enforce accountability for internal control in the entity. These actions can range from informal feedback provided by the direct supervisor to disciplinary action taken by the oversight body, depending on the significance of the deficiency to the internal control system.[33]

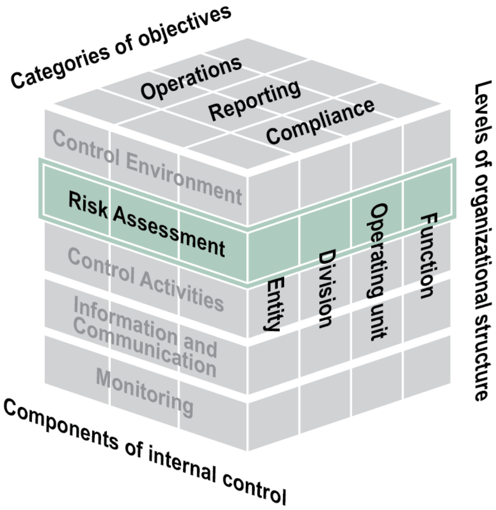
Consideration of Excessive Pressures

5.07 Management adjusts excessive pressures on personnel in the entity. Pressure can appear in an entity because of goals management established to meet objectives or cyclical demands of various processes the entity performs, such as year-end financial statement preparation. Excessive pressure can result in personnel "cutting corners" to meet the established goals.

5.08 Management is responsible for evaluating pressure on personnel to help personnel fulfill their assigned responsibilities in accordance with the entity's standards of conduct. Management can adjust excessive pressures using many different tools, such as rebalancing workloads or increasing resource levels.

[33] See para. OV3.08 for further discussion of significance of deficiencies.

Risk Assessment



Sources: COSO and GAO. | GAO-25-107721

Overview

Management assesses internal and external risks and performs risk assessments on a periodic and ongoing basis to achieve its objectives. These assessments provide the basis for identifying risks and developing appropriate risk responses.

Principles

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.
7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.
8. Management should consider risks related to fraud, improper payments, and information security when identifying, analyzing, and responding to risks.
9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Principle 6 - Define Objectives and Risk Tolerances

6.01 Management should define objectives clearly to enable the identification of risks and define risk tolerances.

Attributes

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

- Definitions of Objectives
- Definitions of Risk Tolerances

Definitions of Objectives

6.02 Management defines objectives, and related subobjectives, in specific and measurable terms to enable the design of internal control for related risks.[34] Specific terms are fully and clearly set forth so they can be easily understood. Measurable terms allow for the assessment of performance toward achieving objectives. Objectives are initially set as part of the objective-setting process and then refined as they are incorporated into the internal control system when management uses them to establish the control environment.

6.03 Management defines objectives in specific terms, so that they are understood at all levels of the entity. This involves clearly defining what is to be achieved, who is to achieve it, how it will be achieved, and the time frames for achievement. All objectives can be broadly classified into one or more of three categories: operations, reporting, or compliance. Reporting objectives are further categorized as being either internal or external and financial or nonfinancial. Management defines objectives in alignment with the organization’s mission, strategic plan, and performance goals.

6.04 Management defines objectives in measurable terms so that performance toward achieving those objectives can be assessed. Measurable objectives are generally free of bias and do not require subjective judgments to dominate their measurement. Measurable objectives are also stated in a quantitative or qualitative form that permits reasonably consistent measurement.

6.05 Management considers external requirements and internal expectations when defining objectives to enable the design of internal control. Legislators, regulators, and standard-setting bodies set external

[34] See paras. OV2.22 through OV2.31 for further discussion of setting objectives and subobjectives.

requirements by establishing the laws, regulations, and standards with which the entity is required to comply. Management identifies, understands, and incorporates these requirements into the entity's objectives. Management sets internal expectations and requirements through the established standards of conduct,[35] oversight structure,[36] organizational structure,[37] and expectations of competence[38] as part of the control environment.

6.06 Management evaluates and, if necessary, revises defined objectives so that they are consistent with external requirements and internal expectations. This consistency enables management to identify and analyze risks associated with achieving the defined objectives.

6.07 Management determines whether performance measures for the defined objectives are appropriate for evaluating the entity's performance in achieving those objectives. For quantitative objectives, performance measures may be a targeted percentage or numerical value. For qualitative objectives, management may need to design performance measures that indicate a level or degree of performance, such as milestones.

Definitions of Risk Tolerances

6.08 Management defines risk tolerances for the defined objectives. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerances are initially set as part of the objective-setting process. Management defines the risk tolerances for defined objectives by ensuring that the set levels of variation for performance measures are appropriate for the design of an internal control system.

6.09 Management defines risk tolerances in specific and measurable terms so that they are clearly stated and can be measured. For example, for an objective to process all benefit applications within 10 business days of receipt, management may determine that a risk tolerance of a range of 8–12 business days would be an acceptable level of variation. Depending on the category of objectives, risk tolerances may be expressed as follows:

[35] See paras. 1.06 through 1.07 for further discussion of standards of conduct.

[36] See paras. 2.02 through 2.08 for further discussion of oversight structure.

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

[38] See paras. 4.02 through 4.04 for further discussion of expectations of competence.

- **Operations objectives** - Acceptable levels of variation in performance relative to the achievement of operations objectives.
- **Nonfinancial reporting objectives** - Level of precision and accuracy suitable for user needs, involving both qualitative and quantitative considerations to meet the needs of the nonfinancial report user.
- **Financial reporting objectives** - Judgments about materiality that consider surrounding circumstances, involve both qualitative and quantitative considerations, and are affected by the needs of financial report users and size or nature of a misstatement.
- **Compliance objectives** - Acceptable levels of variation in performance relative to the achievement of compliance objectives, within the context of applicable laws, regulations, and external standards.

6.10 Management also evaluates whether risk tolerances enable the appropriate design of internal control by considering whether they are consistent with requirements and expectations for the defined objectives. As in defining objectives, management considers the risk tolerances in the context of the entity's applicable laws, regulations, and standards as well as the entity's standards of conduct, oversight structure, organizational structure, and expectations of competence. If risk tolerances for defined objectives are not consistent with these requirements and expectations, management revises the risk tolerances to achieve consistency.

Principle 7 - Identify, Analyze, and Respond to Risks

7.01 Management should identify, analyze, and respond to risks related to achieving the defined objectives.

Attributes

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

- Identify Risks
- Analyze Risks
- Respond to Risks

Identify Risks

7.02 Management identifies risks throughout the entity on a periodic and ongoing basis to provide a basis for analyzing risks.[39] Risk is the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses. Periodic risk assessments are performed at specific times and at regular intervals, such as annually. Management considers entity objectives, risk tolerances, and other factors when determining the scope and frequency of these assessments. Ongoing risk assessments are performed as needed, on a real-time basis, such as when significant internal or external change occurs or significant emerging risks are identified.[40] Management also considers performing ongoing risk assessments when internal control deficiencies,[41] improper payments, potential fraud, or information security breaches are detected.[42]

7.03 To identify risks, management considers the types of risks that impact the entity. This includes both inherent and residual risk. Inherent risk is the risk to an entity in the absence of management's response to the risk. Residual risk is the risk that remains after management's response to inherent risk. Once risk responses have been developed to address inherent risk, management then considers the impact or significance of the residual risk that remains and whether it is at an acceptable level within the defined risk tolerances. Assessing inherent and residual risk can assist management in understanding the extent of risk responses needed. Management's lack of response to either type of risk could cause deficiencies in the internal control system.

7.04 Management considers all significant interactions within the entity and with external parties,[43] changes within the entity's internal and external environments,[44] and other internal and external factors to identify risks throughout the entity. Management considers these factors at both

[39] See para. 7.15 for further discussion of documenting the identification of risk.

[40] See paras. 9.02 through 9.04 for further discussion of identifying change.

[41] See principle 17 for further discussion of internal control deficiencies.

[42] See paras. 8.02 through 8.17 for further discussion of fraud, improper payments, and information security risks.

[43] See paras. OV4.01 through OV4.07 for additional considerations related to external parties.

[44] See paras. 9.03 through 9.04 for further discussion of changes in the internal control system.

the entity and transaction levels to comprehensively identify risks that affect defined objectives.[45] Entity-level risk factors have a pervasive effect on an entity's internal control system and are generally considered at a relatively high level. Transaction-level risk factors affect specific business processes within all levels of the organizational structure and are generally considered at a more detailed level.

Internal risk factors may include

- the complex nature of an entity's programs;
- the level and experience of, and quality of training for, personnel;
- the entity's organizational structure;
- limitations of the entity's information system;
- availability and quality of data;
- use of new technology in business processes; and
- use of emerging technologies, such as artificial intelligence.

External risk factors may include

- new or amended laws, regulations, or standards;
- economic instability and crises;
- developments in information technology and related security threats;
- outsourcing of business processes to external parties;
- threats to national security; and
- public health emergencies, natural and human-caused disasters, and other catastrophic events.

7.05 Management's consideration of risk factors related to fraud, improper payments, and information security is discussed further in principle 8. Management's consideration of significant internal and external changes that could impact the internal control system is discussed further in principle 9.

[45] See paras. 10.14 through 10.20 for further discussion of entity-level and transaction-level control activities.

7.06 Risk identification methods may include qualitative and quantitative ranking activities, forecasting and strategic planning, data analytics, and consideration of internal control deficiencies identified through monitoring activities or reported by internal or external parties. Performing an analysis to identify the root causes of internal control deficiencies can assist management in identifying risks. Management also collaborates with relevant internal and external parties to identify risks. Internal parties include appropriate management and other personnel from all appropriate units within the entity's organizational structure, including program and financial managers. External parties may include service organizations, suppliers, contractors, regulated entities, federal entities, state and local governments, and grantees.

Analyze Risks

7.07 Management analyzes the identified risks, on a periodic and ongoing basis, to estimate their significance, which provides a basis for responding to the risks.[46] Significance refers to a risk's impact on achieving a defined objective.

7.08 Management estimates the significance of the identified risks to assess their impact on achieving the defined objectives at both the entity and transaction levels. Management estimates the significance of a risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk. Magnitude of impact refers to the likely magnitude of the effect of the risk on the entity's ability to achieve its objectives. It is affected by factors such as the size, pace, and duration of the risk's impact. Likelihood of occurrence refers to the level of possibility that an unintended event or result will occur. The nature of the risk involves factors such as the degree of subjectivity involved with the risk and whether the risk arises from fraud or from complex or unusual transactions.

7.09 Risks may be analyzed individually or grouped into categories with related risks and analyzed collectively. Regardless of whether risks are analyzed individually or collectively, management considers the correlation among different risks or groups of risks when estimating their significance. The specific risk analysis methodology used can vary by entity because of differences in entities' missions and the difficulty in qualitatively and quantitatively defining risk tolerances.

[46] See para. 7.15 for further discussion of documenting the analysis of risk.

Respond to Risks

7.10 Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective.[47] Management designs overall risk responses for the analyzed risks based on the significance of the risk, defined risk tolerance, and cost-benefit determination.[48] These risk responses may include the following:

- **Acceptance** - No action is taken to respond to the risk.
- **Avoidance** - Action is taken to stop the business process or the part of the business process causing the risk.
- **Reduction** - Action is taken to reduce the likelihood or magnitude of the risk.
- **Sharing** - Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.

7.11 Based on the selected risk response, management designs controls to effectively mitigate the analyzed risks on a timely basis. If management has chosen to reduce or share a risk, then management designs controls, which may exist within each component of internal control or constitute a specific control activity.[49] 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 separate processes within the periodic and ongoing risk assessment process[50] with separate oversight responsibilities, to manage 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

[47] See para. 7.15 for further discussion of documenting the response to risk.

[48] See paras. OV4.15 through OV4.17 for further discussion of the benefits and costs of internal control.

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

[50] See para. 7.02 for further discussion of the periodic and ongoing risk assessment process.

has an impact on multiple processes. These separate processes would cover all components of internal control related to these specific risks.

7.13 After designing risk responses, management then considers residual risk. In instances where a risk response results in the 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 assessments, 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 [**documentation requirement**].[51]

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.[52]

Attributes

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

- Identify Risks Related to Fraud, Improper Payments, and Information Security
- Types of Fraud and Fraud Risk Factors

[51] See paras. 3.09 to 3.12 for further discussion of documentation of the internal control system.

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

- Types of Improper Payments and Improper Payment Risk Factors
- Types of Information Security Risk and Information Security Risk Factors
- Analyze and Respond to Identified Risks

Identify 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.[53] 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 identifies risks related to fraud, improper payments, and information security on a periodic and ongoing basis to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses. To determine the scope and frequency of these assessments, management considers the entity's objectives, risk tolerances, any legal or regulatory requirements, and other factors.[54] 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 certain program or activity on a more frequent and recurring basis, regardless of the required frequency in legal or regulatory requirements for such risk assessments.

8.04 Management considers the types of fraud, improper payments, and information security breaches that may occur, along with relevant risk factors, when identifying risks related to these areas. While risks may be greater when multiple risk factors are present, the presence of one factor may still indicate a risk. Performing an analysis to identify the root cause of identified internal control deficiencies can assist management in identifying risks.

[53] See paras. 7.02 through 7.06 for further discussion of identifying risks.

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

8.05 Management considers information that internal and external parties provide to identify risks related to fraud, improper payments, and information security. This may include information reported by the office of inspector general, internal auditors, personnel, service organizations, and other external parties that interact with the entity. Information may include emerging information security threats, identified instances of improper payments, or adjudicated cases of fraud as well as suspected or alleged fraud.

Types of Fraud and Fraud Risk Factors

8.06 Management considers the types of fraud that could impact the entity to provide a basis for identifying and analyzing fraud. Fraud involves obtaining something of value through willful misrepresentation.[55] Types of fraud may include the following:

- **Fraudulent reporting**[56] **-** Intentional misstatements or omissions of amounts or disclosures in financial or nonfinancial reports through willful misrepresentation to deceive report users. For fraudulent financial reports, this could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles. For fraudulent nonfinancial reports, this could include intentional misrepresentation of information.
- **Misappropriation of assets -** The unauthorized acquisition, use, or disposal of an entity's assets through willful misrepresentation. This could include efforts to conceal theft of property, embezzlement of receipts, bid rigging, fraudulent payments,[57] or misrepresentation of eligibility to obtain benefits.
- **Other illegal acts -** Intentional violations of laws or regulations through willful misrepresentation that may be related to financial or nonfinancial activities. This could include certain types of corruption, bribery, extortion, and cybercrimes.

8.07 As part of a risk assessment, management considers the risk of fraud that could impact the entity from both within the entity and from

[55] Misrepresentation includes material false statements of fact, as well as the omission or concealment of material fact. Willful misrepresentation may involve actual knowledge, deliberate ignorance (being aware of a substantial risk of misrepresentation but intentionally avoiding steps to confirm truth or falsity), or reckless disregard (to be conscious of a substantial and unjustifiable risk of falsity but make the representations anyway). A judicial or other adjudicative system determines whether an act is in fact fraud; this determination is beyond management's professional responsibility for assessing risk.

[56] See para. OV2.27 for further discussion of reporting objectives.

[57] All fraudulent payments are considered improper payments.

external parties. For example, external fraud risk may arise when an entity relies on service organizations' internal control systems to perform business processes for the entity. External parties that present fraud risk may also include program beneficiaries who fraudulently obtain benefits.

8.08 In addition to fraud, management considers other forms of misconduct that can occur, such as waste and abuse. Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances. Abuse may include corruption through the misuse of authority or position for personal gain or for the benefit of another. Waste and abuse do not necessarily involve fraud, though fraudulent misrepresentations may be made to conceal such misconduct. The presence of waste and abuse may indicate potential fraud and an environment that is conducive to fraud. Waste and abuse may also impact the achievement of defined objectives.

8.09 In addition to fraud, management also considers the risk of management override of controls.[58] Management override of controls does not necessarily involve fraud but may indicate potential fraud and increases fraud risk.

8.10 Management considers fraud risk factors. Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs. Fraud risk factors may include the following:

- **Incentive/pressure** - Management, other personnel, or external parties have an incentive or are under pressure, which provides a motive to commit fraud.[59]
- **Opportunity** - Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.
- **Attitude/rationalization** - Individuals involved can rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to commit dishonest acts knowingly and intentionally.

[58] See para. 10.22 for further discussion of management override.

[59] See paras. 5.07 through 5.08 for further discussion of pressure.

Types of Improper Payments and Improper Payment Risk Factors

8.11 Management considers the types of improper payments that could impact the entity to provide a basis for identifying and analyzing improper payment risks. Improper payments are any payments that should not have been made or that were made in an incorrect amount.[60] Payments are also considered improper when there is insufficient or lack of documentation. Improper payments can result from lack of oversight, mismanagement, errors, deficiencies in internal control, abuse, or fraud. While all payments resulting from fraudulent activity are considered improper, not all improper payments are the result of fraud. Types of improper payments may include the following:

- **Overpayments** - These payments are those in excess of the amount due to be paid to recipients. They include payments to ineligible recipients, any payment for an ineligible good or service, payments for goods or services not received, and any duplicate payment. They could be either intentional—such as fraudulent payments—or unintentional.
- **Underpayments** - These payments are those in which recipients did not receive some or all the funds to which they were entitled.

8.12 Management considers improper payment risk factors, both internal and external, which may include the following:

- whether the program or activity is new to the entity;
- the complexity of the program or activity;
- the volume of payments made through the program or activity;
- whether the payments or payment eligibility decisions are made through external parties;
- recent major changes in program funding, legal authorities, practices, or procedures;
- the level and experience of and quality of training for personnel responsible for making payment eligibility determinations or verifying that payments made are accurate;
- the extent to which the entity relies on potential recipients self-certifying their own eligibility;

[60] This definition of improper payments is only for the purposes of the Green Book and not for the purposes of any legal authority.

- identified internal control deficiencies that might hinder accurate payment processing;
- similarities to other programs or activities that have reported improper payment estimates or been deemed susceptible to significant improper payments;
- improper payment estimates previously reported for the program or activity, or other indicator of potential susceptibility to improper payments;
- whether the program or activity lacks the information or database to confirm eligibility or verify the accuracy of the payment; and
- the risk of fraud related to the program or activity.

8.13 Management considers existing improper payment estimates, if available, when determining the significance of risks and the effectiveness of the internal control system in responding to improper payment risks. These estimates may come from management's annual improper payment estimates as part of its monitoring activities, which may be mandated by law.[61] Management may also develop estimates more frequently than mandated by law, such as for programs that are new, substantially changed, or rapidly implemented to facilitate a timely risk assessment.

Types of Information Security Risk and Information Security Risk Factors

8.14 Management considers the types of risks that could impact the entity's information and information technology to provide a basis for identifying and analyzing risks related to information security.[62] Information security risk is the risk to entity operations, assets, and personnel, as well as external parties, due to unauthorized access, use, disclosure, disruption, modification, or destruction of information or information technology. These risks may impact the information security objectives of confidentiality, integrity, and availability.[63] Types of information security risk impacting each of these three objectives may include the following:

- **Unauthorized access** - End users, developers, or unrelated attackers may compromise the confidentiality of a platform or software system

[61] See para. 16.06 for further discussion of monitoring activities related to improper payments.

[62] See para. OV4.09 for further discussion of information security.

[63] See para. 11.07 for further discussion of information security objectives.

by overriding controls to gain unauthorized access to the entity's information technology or use capabilities that exceed their rights in those systems.

- **Exploitation of personnel** - Attacks, such as phishing attempts, that trick users into revealing information or giving an attacker access to a platform or software system.
- **Installation of malicious software** - Installation of a program or file that intentionally attacks the entity's information technology by corrupting or stealing data, overwhelming a system with traffic, or locking the entity out. The objective of a malicious software (malware) attack may be to harm the entity, gain information, or obtain a financial gain.
- **Automated attacks** - Attacks on information technology may be automated through mechanisms, such as bots, artificial intelligence, and machine learning software.
- **Undetected errors** - End users, developers, or unrelated attackers may improperly alter data in the entity's information technology without visible evidence. Erroneous changes resulting from corrupted systems may not be readily detectable by users.
- **Threats to physical environment** - Threats to the physical environment, such as fire, loss of electricity, loss of climate controls, or natural disasters, can result in the loss of information or information technology system damage or disruption. In addition, failure to appropriately limit physical access to information or an information technology system may also allow a malicious attacker to access or modify information.

8.15 Internal risks include unintentional acts by employees, whose vigilance is a key defense against external threats and user error. Internal threats may also come from intentional malicious acts by former or disgruntled employees. They pose unique risks because these individuals may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the entity's information technology and business processes.

8.16 External risks may come from external parties that connect with or operate the entity's information technology or from unrelated attackers. External parties that connect with the entity's operating systems and databases in the normal course of operations may include end users, such as program beneficiaries; federal, state, and local government entities; and service organizations. External parties that operate the entity's information technology may include developers to which the entity outsources the design of information technology or service organizations or location-independent technology services that operate the systems on behalf of the entity.[64] External information security risks may arise when an entity relies on these external parties' internal control systems as they perform business processes for the entity.

8.17 Management considers information security risk factors, which may include the following:

- the complexity of the entity's information technology;
- new or emerging technologies;
- information technology that may be outdated or incompatible with new technologies;
- decentralized operating systems and communications networks;
- external-party access to the entity's operating systems and communications networks;
- information technology personnel not having the knowledge, skills, or abilities to maintain the entity's information technology and respond to related risks; and
- personnel being unfamiliar with technology and related risks.

Analyze and Respond to Identified Risks

8.18 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.[65] Management analyzes the identified risks by estimating their significance to assess their impact on achieving the defined objectives.

8.19 Management responds to fraud, improper payment, and information security risks consistent with the risk response process performed for all analyzed risks.[66] Based on the selected risk response, management determines the specific actions to effectively mitigate each risk. It may be

[64] See paras. 11.06 and 11.13 for further discussion of information technology that may be outsourced to external parties.

[65] See paras. 7.07 through 7.09 for further discussion of analyzing risks.

[66] See paras. 7.10 through 7.15 for further discussion of responding to risks.

possible to reduce or avoid certain fraud, improper payment, or information security risks by making changes to the entity's activities and processes. These changes may include stopping or reorganizing certain operations, modifying the entity's information technology, reallocating roles among personnel to enhance segregation of duties, or designing or modifying control activities. Management may also need to develop further responses to address the risk of management override of controls, particularly when considering fraud risks.

8.20 Management may develop separate processes within the periodic and ongoing risk assessment process[67] with separate oversight responsibilities, to manage risks related to fraud, improper payments, or information security as part of the entity's overall internal control system. These separate processes would cover all components of internal control related to these specific risks.[68]

Principle 9 - Identify, Analyze, and Respond to Change

9.01 Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Attributes

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

- Identify Significant Changes
- Establish a Change Assessment Process
- Identify, Analyze, and Respond to Risks Related to Significant Changes

Identify Significant Changes

9.02 As part of periodic and ongoing risk assessments, management identifies, on a timely basis, significant internal and external changes that could impact the entity's internal control system. Identifying, analyzing, and responding to significant changes is similar to, if not part of, the entity's periodic and ongoing risk assessment process. However, change is discussed separately because it is critical to an effective internal control

[67] See para. 7.02 for further discussion of the periodic and ongoing risk assessment process.

[68] See para. 7.12 for further discussion of separate processes to manage certain risks as part of the entity's internal control system, and para. 11.09 for discussion of a separate process for managing risks related to information security in the context of general control activities.

system and can often be overlooked or inadequately or not timely addressed in the normal course of operations.

9.03 Conditions affecting the entity and its environment continually change. Management identifies, on a timely basis, significant changes to internal and external conditions that have already occurred or are expected to occur. Management anticipates and plans for significant changes that are expected to occur by using a forward-looking process to identify expected changes. This enables management to timely identify and analyze the impact of related risks.

9.04 Changes in internal conditions may include changes to the entity's programs or activities, oversight structure, organizational structure, personnel, and technology. Changes in external conditions may include changes in the governmental, economic, technological, legal, regulatory, and physical environments. Changes in external conditions may also include economic instability or crises, public health emergencies, natural and human-caused disasters, and other catastrophic events.

Establish a Change Assessment Process

9.05 Management documents a change assessment process for identifying, analyzing, and responding to risks related to significant changes so that the internal control system can be quickly adapted as needed to respond to significant changes as they occur [**documentation requirement**].[69]

9.06 As significant changes that an entity may need to respond to can occur quickly and unexpectedly, establishing a change assessment process in advance of significant changes occurring is essential to maintaining an effective internal control system as change occurs.[70] This is especially important in situations where management may need to rapidly implement a new program or substantially change an existing program. For example, management may need to implement an emergency assistance program in response to public health emergencies, natural or human-caused disasters, or other catastrophic events.

9.07 Management develops and documents a change assessment process based on the risk assessment process described in principle 7.[71]

[69] See paras. 3.09 through 3.12 for further discussion of documentation of the internal control system.

[70] See para. 7.08 for further discussion of management's estimation of significance of risk.

[71] See principle 7 for further discussion of the risk assessment process.

The process includes procedures for identifying, analyzing, and responding to risks related to significant changes.

9.08 Management's change assessment process includes steps for timely identifying risks related to significant change, which may include the following:

- the need to provide complex or different services quickly, which may result in increased risks overall, including those related to fraud, improper payments, information security, and noncompliance with applicable laws and regulations;
- ability to design and implement preventive control activities timely due to legal requirements or urgency to deliver a service quickly;
- ability to timely communicate relevant and quality information both internally and externally to support the internal control system, such as changes to identified risks, internal control responsibilities, and training on how to administer new internal controls;
- availability of existing resources, such as workforce capacity or availability of data (i.e., data-sharing agreements for external data), to adequately and timely adapt the entity's internal control system to address new or increased risks; and
- known internal control deficiencies that could increase risks related to significant change.

9.09 Management's change assessment process includes considerations for management to effectively analyze risk related to significant change, which may include the following:

- how to determine the appropriate scope and extent of initial risk assessment related to a significant change—management considers entity objectives, risk tolerances, and other factors when making this determination—and
- how to determine the timing of subsequent ongoing risk assessments as the entity responds to significant changes.

9.10 Management's change assessment process includes considerations to facilitate its ability to quickly adapt the entity's internal control system and effectively respond to a significant change once it occurs, such as the following:

- modifying the organizational structure, responsibilities, and authorities to address identified risks;

- determining whether to create a separate process, with separate oversight responsibilities, to manage risks related to the change as part of the entity's overall internal control system;[72]
- identifying any existing control activities, policies and procedures, or other processes in existing or similar programs that could be leveraged or modified;
- identifying preventive control activities that could be implemented prior to the distribution of program benefits, even if time or resources are constrained;
- identifying monitoring and detective control activities that could be enhanced or performed more frequently if preventive controls to mitigate certain risks are not feasible;
- considering lessons learned from past programs to inform future practices;
- identifying and establishing communications with external parties that may contribute to the operational effectiveness of the entity's internal control system when implementing the change; and
- identifying and establishing data-sharing, data-matching, and data-analytics opportunities, including considering known data access issues.

Identify, Analyze and Respond to Risks Related to Significant Changes

9.11 Changes in conditions affecting the entity and its environment often require changes to the entity's internal control system, as existing controls may not be effective for meeting objectives or addressing risks under changed conditions. Once significant changes are identified, management uses its change assessment process to identify and analyze the impact of risks related to the identified significant changes on the internal control system and responds by revising the system on a timely basis, when necessary, to maintain its effectiveness. This risk assessment,[73] and revision to the internal control system when necessary, is completed before the entity responds to changing conditions, for example, before it implements a new program or makes significant changes to existing programs or activities.

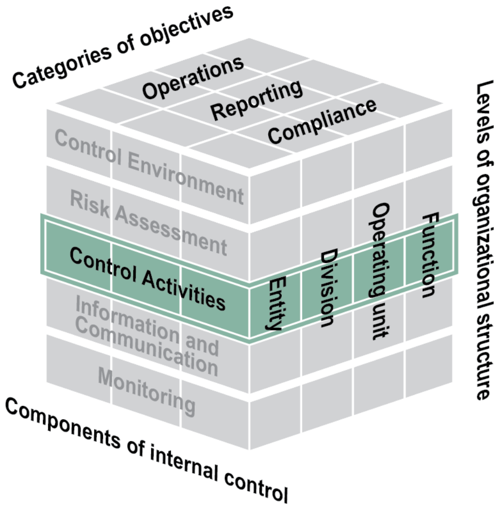
[72] See para. 7.12 for further discussion of separate processes to manage certain risks as part of the entity's internal control system.

[73] See para. 9.09 for further discussion of the scope and extent of the risk assessment.

9.12 Management also performs ongoing risk assessments as the entity responds to changing conditions to analyze and respond to risks on a real-time basis.

9.13 Further, changing conditions often prompt new risks or changes to existing risks that need to be assessed. As part of analyzing and responding to significant change, management performs a risk assessment to identify, analyze, and respond to any new risks prompted by the changes. Additionally, existing risk assessments may need to be updated to determine whether the defined risk tolerances and risk responses need to be revised.

Control Activities



Sources: COSO and GAO. | GAO-25-107721

Overview

Control activities are the actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels.

Principles

10. Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.
11. Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.
12. Management should implement control activities through policies and procedures.

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 Automated and Manual Control Activities
- Design of Preventive and Detective Control Activities
- Design of Control Activities at Various Levels
- Segregation of Duties

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 specifically mitigate risks to achieving the entity's objectives to acceptable levels.[74] Control activities support all the components of internal control but are particularly aligned with the risk assessment component. As part of periodic and ongoing 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.[75] 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

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

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

to meet the entity’s unique needs. The specific control activities used by a given entity may be different from those used by others based on several factors. These factors could include specific threats the entity faces and the risks involved, differences in objectives, managerial judgment, size and complexity of the entity, operational environment, and sensitivity and value of data.

10.04 The common categories of control activities listed in table 1 illustrate the range and variety of control activities that may be useful to management. The list is not all inclusive and may not include all categories of control activities that an entity may need.[76]

Table 1: Common Categories of Control Activities

- Top-level reviews of actual performance
- Reviews by management at the functional or activity level
- Establishment and review of performance measures and indicators
- Management of human capital
- Control activities over information processing
- Physical control activities over vulnerable assets
- Access restrictions to and accountability for resources and records
- Authorization of transactions
- Control activities over complete, accurate, and timely recording of valid transactions
- Appropriate documentation of transactions and control activities
- Oversight of entity business processes assigned to service organizations
- Segregation of duties
- Program-related control activities
- Fraud-related control activities
- Improper-payment-related control activities
- Compliance-related control activities

Source: GAO. | GAO-25-107721

- **Top-level reviews of actual performance -** Management tracks major entity achievements and compares these to the plans, goals, and objectives set by the entity.
- **Reviews by management at the functional or activity level -** Management compares actual performance to planned or expected results throughout the organization and analyzes significant differences.

[76] See app. II for examples of control activities that may be useful to management.

- **Establishment and review of performance measures and indicators -** Management establishes control activities to monitor performance measures and indicators that it has established for its defined objectives. These may include comparisons and assessments relating different sets of data to one another so that management can analyze the relationships and take appropriate actions. Management designs control activities aimed at validating the propriety and integrity of both entity and individual performance measures and indicators.

- **Management of human capital -** Management establishes control activities to manage and supervise the entity's workforce. Effective management and supervision of an entity's workforce, its human capital, is essential to achieving results. The entity can successfully carry out its business processes when competent personnel are on board and are provided the right training, tools, structure, incentives, and responsibilities.

  Management continually assesses the needs of the entity so that it can maintain a workforce that has the required knowledge, skills, and abilities to meet these needs and achieve entity objectives. Training is aimed at developing and retaining employee knowledge, skills, and abilities to meet changing organizational needs. Management provides qualified and continuous supervision so that entity objectives are achieved. Management designs a performance evaluation and feedback system, supplemented by an effective rewards system, to help employees understand the connection between their performance and the entity's success. As part of its human capital planning, management also considers how best to retain valuable employees, plan for their eventual departure, and maintain a continuity of needed skills and abilities.

- **Control activities over information processing -** A variety of control activities are used to achieve effective information processing for the completeness, accuracy, and validity of data.[77] Examples include data validation rules designed to detect erroneous data values before processing, accounting for transactions in numerical and logical sequences, processing of transactions timely, and comparing file totals with control accounts.

[77] Information processing may be manual or automated. Where these control activities are incorporated into automated business processes, they are considered application or user control activities. See paras. 10.05 through 10.09 for further discussion of automated and manual control activities, and para. 10.18 for further discussion of information processing objectives.

- **Physical control activities over vulnerable assets -** Management establishes physical control activities to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment (including information technology infrastructure) that might be vulnerable to risk of loss or unauthorized use. Management periodically counts and compares such assets to control records. Management may also establish physical control activities over facilities housing vulnerable assets. Entrance points may be secured by physical barriers, such as turnstiles, gates, and locked doors. Restricted areas containing sensitive information may include additional security, such as alarms, fencing, cameras, and motion- or sensor-triggered lighting to prevent or deter unauthorized access.

- **Access restrictions to and accountability for resources and records -** Management limits access to physical and digital resources and records to authorized individuals; it also assigns and maintains accountability for their custody and use. Management may periodically inspect evidence demonstrating accountability for resources and records (such as custodial records and access logs) to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

- **Authorization of transactions -** Transactions are authorized and executed only by persons acting within the scope of their authority.[78] This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources are initiated or entered into. Management clearly communicates authorizations to personnel, for example, by assigning the capabilities to their credentials in an information technology system, or by signature or other methods of express approval. Management may require approval from multiple levels or units (multilevel authorization) to authorize unique or recurring transactions that present a greater risk to the entity. Management regularly reviews and updates system credentials and access rights related to authorizations for continued appropriateness.

- **Control activities over complete, accurate, and timely recording of valid transactions -** Management establishes control activities so that valid transactions are completely and accurately recorded on a timely basis. Transactions are promptly recorded to maintain their

[78] See para. 11.11 for further discussion of logical and physical access controls that prevent unauthorized transactions in the entity's information technology.

relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event, from its initiation and authorization through its final classification in summary records.

- **Appropriate documentation of transactions and control activities -** Management clearly documents the performance of control activities and all transactions and other significant events that occur in a manner that allows the documentation to be readily available for examination. Documentation and records are properly managed and maintained.

- **Oversight of entity business processes assigned to service organizations -** Management establishes control activities to oversee business processes that service organizations perform on behalf of the entity.[79] Examples include control activities to obtain, review, and appropriately respond to information regarding relevant service organization operations and controls, including information from audits, evaluations, and performance metrics. Management establishes processes for communicating necessary information with service organizations, such as relevant risks, internal control practices to consider, information requirements, and circumstances that may impact achieving the entity's objectives.[80] The entity may also establish complementary user entity controls that the service organization identified as being necessary for the entity to achieve its objectives.

- **Segregation of duties -** Management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets so that no one individual controls all key aspects of a transaction or event.

- **Program-related control activities -** Management establishes control activities to achieve program-related objectives, which are the operations objectives most directly aligned with the entity's mission. Examples of program-related objectives include providing services, awarding federal financial assistance, and performing regulatory

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

[80] See paras. 13.04 and 15.02 through 15.06 for further discussion of information and communication with external parties.

responsibilities. Control activities may include verifying that services are provided timely and in accordance with program policies, reviewing for proper awarding of program benefits or federal financial assistance, and reviewing to identify when regulated entities have not complied with applicable laws and regulations.

- **Fraud-related control activities -** Control activities may be designed to minimize the ability to conduct or conceal fraud. Examples of such activities include data validation, supervisory approval, and supporting documentation to verify identity and eligibility before executing transactions. Since the inherent motive of fraud is to commit and conceal the misrepresentation, detecting occurrences of fraud can be difficult. Management may use data analytics to identify trends and anomalies that indicate fraudulent activity, such as amounts or types of goods and services that are outside of the expected range for normal operations. Additionally, increasing fraud awareness through training can enable management and other personnel to better detect potential fraud.

  Management identifies and reports detected occurrences of potential fraud to the appropriate investigatory body and implements corrective actions, including payment or asset recovery, and disciplinary actions. Control activities that increase the likelihood of detection and prosecution can also serve as a deterrent to potential perpetrators of fraud.

- **Improper-payment-related control activities -** Management designs control activities to prevent and detect improper payments. These control activities may include verification of identity and eligibility requirements through data matching, data validation, supervisory approval, and obtaining supporting documentation before making payments. They may also include recovery audits and activities, such as postpayment reviews and data analytics to identify improper payments. Management designs activities to recover overpayments and report improper payment estimates to regulatory bodies and stakeholders as required.[81]

- **Compliance-related control activities -** Management designs control activities to achieve compliance with applicable laws and regulations and to respond when noncompliance is identified. Compliance objectives may include protecting confidential

[81] See para. 16.06 for further discussion of improper payment estimates.

information, including privacy and sensitive information; retaining communications; and completing various reporting requirements. Management responds to noncompliance by reporting occurrences to the appropriate regulatory body as required and taking corrective action to recover from the event and achieve compliance in the entity's processes going forward.

Design of Automated and Manual Control Activities

10.05 Control activities can be designed and implemented in an automated, partially automated, or a manual manner. Automated control activities may be wholly or partially performed using the entity's information technology. Manual control activities are performed by individuals without relying on the entity's information technology. Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient.

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, application, and user control activities.

10.07 Application and user control activities rely on the entity's information technology. 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 control activities 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.[82] 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 General control activities are designed to mitigate information security risks and are the actions established through policies and procedures that apply to all or a large segment of an entity's information technology.[83] General control activities support the proper operation of the entity's information technology by creating a suitable environment for

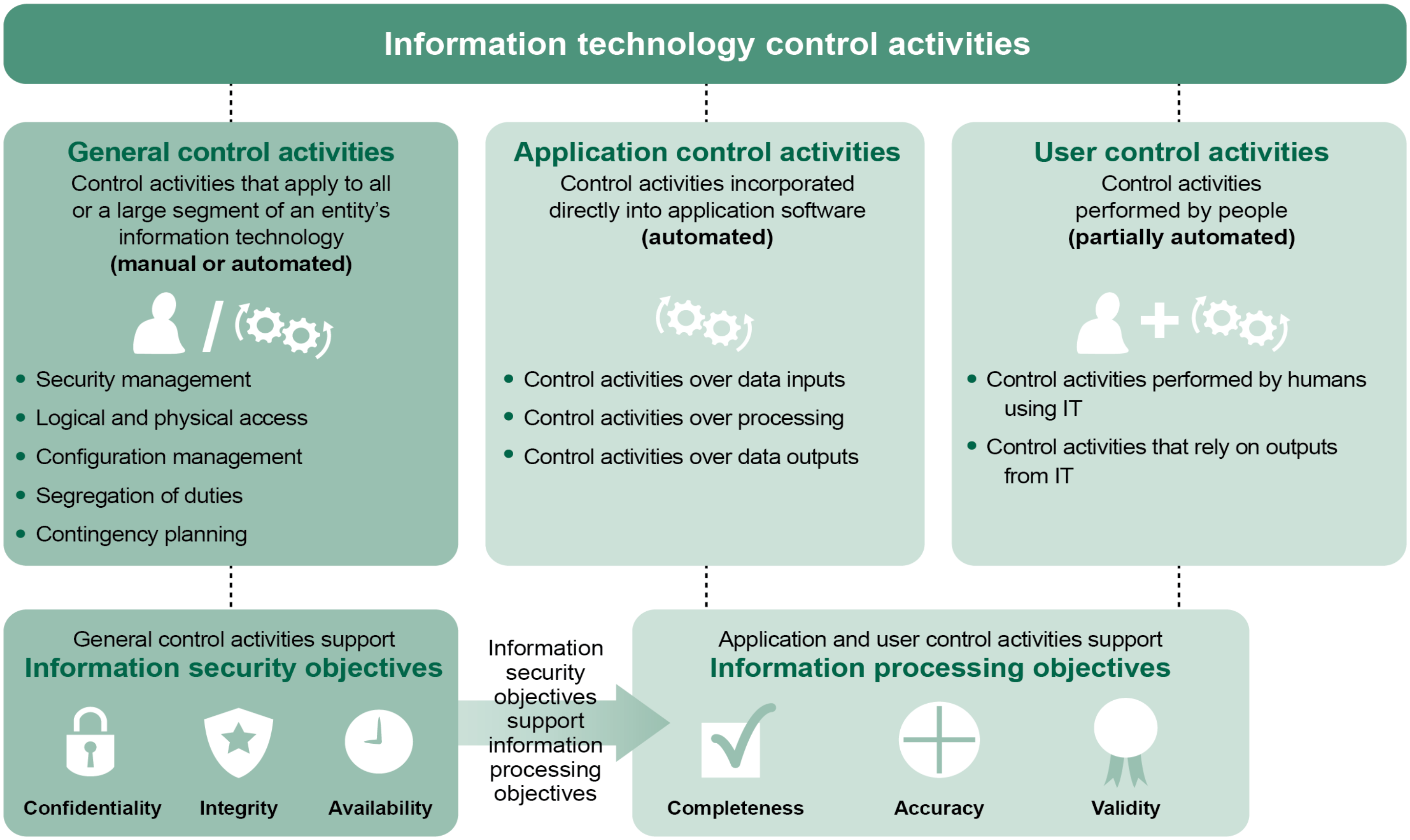
[82] User control activities may also be considered two separate control activities, with a manual control activity that relies on an automated control activity.

[83] See paras. 11.07 through 11.17 for further discussion of general control activities over information technology.

effective operation of application and user control activities. General control activities can be designed and implemented in either an automated or a manual manner.

10.09 Common categories of information technology control activities and how they align with information processing and information security objectives are illustrated in figure 7.[84] 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.

Figure 7: Common Categories of Information Technology Control Activities


Information technology control activities
General control activities
Control activities that apply to all or a large segment of an entity's information technology
(manual or automated)
Security management
Logical and physical access
Configuration management
Segregation of duties
Contingency planning
Application control activities
Control activities incorporated directly into application software
(automated)
Control activities over data inputs
Control activities over processing
Control activities over data outputs
User control activities
Control activities performed by people
(partially automated)
Control activities performed by humans using IT
Control activities that rely on outputs from IT
General control activities support
Information security objectives
Confidentiality
Integrity
Availability
Information security objectives support information processing objectives
Application and user control activities support
Information processing objectives
Completeness
Accuracy
Validity

Source: GAO. | GAO-25-107721

[84] See para. 10.18 for further discussion of information processing objectives and para. 11.07 for further discussion of information security objectives.

Design of Preventive and Detective Control Activities

10.10 Control activities can be either preventive or detective.[85] The main difference between preventive and detective control activities is timing, that is, when the control activity occurs within an entity's operations. A preventive control activity is designed to avoid an unintended event or result before it occurs. A detective control activity is designed to discover and timely correct an unintended event or result after it occurs. The effectiveness of a detective control activity depends on timeliness of the corrective action to address the unintended event or result. Corrective action may address the event that occurred or may correct the deficiencies in the process that led to the event.[86]

10.11 Management evaluates the purpose of the control activity as well as the likelihood of an unintended event or result occurring and the magnitude of impact it would have on the entity in achieving its objectives. Management may design both preventive and detective control activities to effectively mitigate the risks to achieving the objectives, particularly in circumstances where the risk of an unintended event or result occurring is high. Generally, the higher the risk of an unintended event or result occurring, the stronger or more robust the control activities need to be to effectively mitigate the higher risk to acceptable levels.

10.12 Management designs an appropriate mix of preventive and detective control activities to mitigate risks to an acceptable level, prioritizing preventive control activities where appropriate. When designing control activities, management first considers preventive control activities, as they generally offer the most cost-efficient use of resources and are generally effective at mitigating fraud and improper payment risks.[87] Management next considers detective control activities and may design both preventive and detective control activities when necessary to mitigate a particular risk.

10.13 There may be rare situations where management determines through its evaluation that a preventive control activity would better mitigate a particular risk but is unable to implement it. In these situations, management strengthens and expedites detective control activities and may also expedite monitoring activities to enable the entity to effectively mitigate the risk to acceptable levels, considering the risk related to the

[85] See app. II for examples of preventive and detective control activities.

[86] See principle 17 for further discussion of remediating deficiencies in internal control.

[87] See paras. OV4.15 through OV4.17 for further discussion of the benefits and costs of internal control.

likelihood of an unintended event or result occurring and the magnitude of impact it would have on the entity in achieving its objectives.[88]

Design of Control Activities at Various Levels

10.14 Management designs control activities at the appropriate levels in the organizational structure.

10.15 Management designs control activities for appropriate mitigation of risks in the entity's business processes. Business processes transform inputs into outputs through a series of transactions or activities to achieve the entity's objectives. Management designs entity-level control activities, business process-level control activities (commonly referred to as transaction control activities), or both depending on the level of precision needed so that the entity mitigates risks to an acceptable level related to its business processes. Entity-level and transaction control activities can be implemented in an automated, partially automated, or a manual manner.

10.16 Entity-level control activities are controls designed to mitigate risks that have a pervasive effect on an entity's internal control system and may pertain to multiple components. Entity-level control activities may include controls related to the entity's risk assessment process, control environment, service organizations, management override, and performance or analytical reviews.

10.17 Transaction control activities are controls that directly mitigate information processing risks in the entity's business processes. The term transaction tends to be associated with business processes addressing reporting objectives (e.g., financial transactions), while the term activity is more often associated with business processes addressing operations or compliance objectives. In the Green Book, "transactions" and "transaction control activities" can cover both transactions and activities. Management may design a variety of transaction control activities for business processes, which may include verifications, reconciliations, authorizations and approvals, physical control activities, and supervisory control activities.

[88] See principle 16 for further discussion of monitoring activities.

10.18 When designing transaction control activities, management evaluates information processing objectives to meet the entity’s objectives and mitigate related risks.[89] Information processing objectives may include the following:

- **Completeness** - All transactions and events that occur have been properly recorded.
- **Accuracy** - Data relating to transactions and events are properly and timely recorded.
- **Validity** - All recorded transactions and events actually occurred, are related to the entity, and were executed according to prescribed procedures.

10.19 While the information processing objectives are most often associated with financial processes and transactions, information processing objectives can be applied to any activity in an organization. For example, information processing objectives and related control activities can be applied to management’s decision-making processes that use nonfinancial data.

10.20 When designing entity-level and transaction control activities, management evaluates the level of precision needed for the business processes to meet the entity’s objectives and mitigate related risks. The precision of a control activity refers to how exact the control activity will be in preventing or detecting an unintended event or result. Control activity precision is closely linked to the entity’s risk tolerance for a particular objective; a lower risk tolerance will require a more precise control activity. In determining the necessary level of precision for a control activity, management evaluates the following:

- **Level of aggregation** - A control activity that is performed at a more granular level generally is more precise than one performed at a higher level. For example, an analysis of obligations by budget object class normally is more precise than an analysis of total obligations for the entity.
- **Consistency and timing of performance** - A control activity that is performed routinely, consistently, and timely generally is more precise than one performed sporadically.

[89] See para. 11.07 for further discussion of information security objectives, which support the achievement of information processing objectives.

- **Correlation to relevant business processes** - A control activity that is directly related to a business process generally is more likely to prevent or detect and correct an error than a control activity that is only indirectly related.

Segregation of Duties

10.21 Management considers segregation of duties in designing control activities so that incompatible duties are segregated. Where such segregation is not practical, management designs alternative control activities to mitigate the risk.[90]

10.22 Segregation of duties helps prevent fraud, waste, and abuse in the internal control system.[91] Management considers the need to separate control activities related to authority, custody, and accounting of operations to achieve adequate segregation of duties within the entity's business processes. Segregation of duties can mitigate the risk of management override. Management override circumvents existing control activities and increases risk of fraud, waste, and abuse. Management mitigates this risk through segregation of duties but cannot absolutely prevent it because of the risk of collusion, where two or more employees act together to commit fraud, waste, or abuse.

10.23 If segregation of duties is not practical within a business process because of limited personnel or other factors, management designs alternative control activities to mitigate the risk of fraud, waste, or abuse in the business process.

Principle 11 - Design General Control Activities over Information Technology

11.01 Management should design general control activities over information technology 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 the Entity's Information Technology
- Design of Appropriate Types of General Control Activities

[90] See para. 11.16 for further discussion of segregation of duties related to general control activities.

[91] See paras. 8.06 through 8.10 for further discussion of fraud, waste, and abuse.

Response to Risks

11.02 Management designs general control activities over the entity's information technology to mitigate risks to information security.[92] Information security is the protection of information or information technology from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. The reliability of information technology used within business processes, including automated controls, depends on the selection, development, and implementation of general control activities over information technology.

Design of the Entity's Information Technology

11.03 Management designs information technology to support the entity's information system and business processes.[93] The entity's information system includes both manual and automated processes. Automated processes are wholly or partially performed using information technology.

11.04 Management designs the entity's use of information technology in the information system by considering the defined information requirements for each of the entity's business processes. Information technology incorporated into business processes enables information related to those processes to become available to the entity on a timelier basis. Additionally, information technology may be incorporated into control activities to enhance internal control over the processing and security of information. Although information technology implies specific types of control activities, information technology is not a "stand-alone" control consideration. It is an integral part of most control activities.

11.05 Information technology consists of the infrastructure, platforms, and software used to automate processes. Infrastructure comprises the physical information technology resources necessary to run software, including the hardware and devices used for information processing, data storage, and network communication. Infrastructure also includes the logical information technology resources necessary to run multiple virtual machines on shared physical information technology resources. Platforms comprise the logical information technology resources necessary to run application software, including operating systems and related computer programs, tools, and utilities. Software comprises application software,

[92] See para. 8.14 for further discussion of information security risks.

[93] See para. 13.05 for further discussion of the information system. The term information technology as used in this document is sometimes referred to as information systems or technology. See para. OV4.09 for clarification of the Green Book's use of these terms.

access control software, and other software used to perform specific functions of the entity's business processes.

11.06 Management designs the information technology infrastructure to support the entity's business processes. Information technology requires a physical infrastructure in which to operate, including communication networks for linking information technologies, computing resources for software and platforms to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be owned and operated by the entity, shared by different units within the entity, or outsourced either to service organizations or to location-independent technology (e.g., cloud computing and storage) services. In designing the information technology infrastructure, management considers factors such as the expertise required to develop and maintain the information technology, costs to develop information technology internally or outsource, desired level of control over resources, and impact on continuity of operations.

Design of Appropriate Types of General Control Activities

11.07 Management designs appropriate types of general control activities to mitigate information security risks.[94] General control activities are the actions established through policies and procedures that apply to all or a large segment of an entity's information technology. They support the proper operation of the entity's information technology by creating a suitable environment for effective operation of application and user control activities.[95] When designing general control activities, management evaluates information security objectives to meet the defined information requirements. General control activities are designed to achieve one or more of the following information security objectives:

- **Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting privacy and sensitive information.
- **Integrity** - Guarding against improper information modification or destruction, which includes ensuring information's nonrepudiation and authenticity.

[94] See paras. 10.06 through 10.09 for further discussion of information technology control activities, including general control activities.

[95] See para. 10.18 for further discussion of information processing objectives.

- **Availability** - Ensuring timely and reliable access to and use of information, thus preventing the disruption of access to or use of information or information technology.

11.08 The nature, timing, and precision of general control activities will depend on various factors, such as the complexity of the technology, sensitivity of information, use of service organizations, use of shared service or data centers, and risk of the underlying business process being supported.

11.09 General control activities may be applied at the entity, system, and business process levels. General control activities include the following:

- **Security management** - A separate process, addressing all components of internal control, for responding to risks related to information security.
- **Logical and physical access** - Control activities that restrict access to information technology to authorized users.
- **Configuration management** - Control activities to develop and maintain the operating and security features of information technology and control changes to their configuration.
- **Segregation of duties** - Separating control activity responsibilities related to information technology to prevent individuals from controlling all critical stages of a process or overriding automated processes.
- **Contingency planning** - Control activities that maintain the continuity of operations and rely on information technology, including contingency plans for recovery after a disruption of service.

11.10 Security management is the ongoing process for mitigating information security risks as part of the entity's overall internal control system (sometimes referred to as a security management program). This ongoing process covers all components of internal control related to information security risks.[96]

11.11 Logical and physical access control activities include restricting access or detecting inappropriate access to information and information

[96] See para. 8.20 for further discussion of establishing a separate process for responding to information security risks.

technology.[97] They protect information technology resources against unauthorized access, use, disclosure, disruption, modification, or destruction, whether from malicious intent or error. Logical access control activities require users to authenticate themselves and restrict them to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties.[98] Management may grant different permissions to employees and end users, including the rights to create, read, edit, or delete a file; execute a program; and retrieve or update information in a database. Management designs other control activities to promptly update access rights when employees change job functions or leave the entity. Physical access control activities involve restricting physical access to information and information technology, including the physical infrastructure, and protecting it from intentional or unintentional loss or impairment.

11.12 Configuration management control activities involve the identification and management of operating and security features for information technology (i.e., infrastructure, platforms, and software) throughout the technology development process. Management may use a technology development methodology to provide a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the development, maintenance, and change of technology. Management evaluates the objectives and risks of the new technology in designing control activities over its technology development methodology.

11.13 Control activities for developing information technology, commonly referred to as systems development controls, prevent the use of unauthorized or untested systems. Management may internally develop information technology, acquire it from suppliers, or outsource its development to service organizations. Management incorporates methodologies for acquisition into its development process and designs control activities over the selection, ongoing development, and maintenance of information technology. For a system developed internally, management designs control activities to mitigate risks in outsourced technology before it is incorporated into the entity’s business processes. Management evaluates the unique risks that using a service organization, search engine, or artificial intelligence software present to

[97] See app. II for further discussion of network security measures when information technologies connect or interact.

[98] See app. II for further discussion of authentication control activities.

the completeness, accuracy, and validity of information submitted to and received from the organization or software system.[99]

11.14 Control activities for maintaining information technology include identifying vulnerabilities to patch and other functional updates to be made. Management continuously monitors the entity's information technology to establish a baseline for evaluating performance, detecting underlying deficiencies before they negatively impact users, collecting data when risks occur, and enabling continuous improvement. Vulnerability management is the process of identifying system vulnerabilities where change may be necessary for remediation. Management may identify vulnerabilities through continuous monitoring of characteristics such as the type of technology used, physical entry points, and trends in user activity. Management may use monitoring software that automatically notifies appropriate personnel when a breach or irregularity is identified. Management may also perform penetration testing of the system to identify vulnerabilities that a hacker might exploit. Patch management is the process of applying platform and software updates to close security vulnerabilities and improve functionality. Management implements control activities to periodically or automatically update antivirus software, apply patches to correct security issues, and scan for and remove unauthorized access points.

11.15 Control activities for changing information technology prevent unauthorized or untested modifications to existing systems. To reasonably assure that changes to the configuration of information technology are necessary, work as intended, and do not cause loss of data or program integrity, changes go through a formal change management process in which they are authorized, documented, tested, and independently reviewed. This may involve requiring authorization of change requests; reviewing the changes, approvals, and testing results; and designing protocols to determine whether changes are made properly. Depending on the size and complexity of the entity, initial development or acquisition of information technology and subsequent changes to the information technology may be included in one methodology or two separate methodologies.

[99] Artificial intelligences (AI) are systems that are taught to solve problems, execute tasks, or generate content that normally require human intelligence by using inputs from a dataset to produce the requested outputs. Where entities rely on AI to inform, influence, or execute decisions or actions, management designs control activities to manage risks related to the data sources and subsequent data processing.

11.16 Segregation of duties control activities help prevent fraud, waste, and abuse from being executed using information technology in the internal control system and mitigate the risk of management override of automated processes. Management considers the need to separate responsibilities for control activities related to the entity's information technology so that one individual does not control all critical stages of a process. This may include separating responsibilities for designing, testing, and implementing new systems or for processing transactions and managing databases.[100]

11.17 Contingency planning protects critical and sensitive data against loss and allows for critical operations to continue without disruption or be promptly resumed when unexpected events occur. Maintaining technology through contingency planning often includes backup and recovery procedures, as well as continuity of operations plans, depending on the risks and consequences of a full or partial power systems outage or other disruption of service. Recovery plans are tested periodically in disaster simulation exercises to determine whether they will work as intended.

[100] See paras. 10.21 through 10.23 for further discussion of segregation of duties.

Principle 12 - Implement Control Activities

12.01 Management should implement control activities through policies and procedures.

Attributes

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

- Documentation of Control Activities Through Policies and Procedures
- Periodic Review of Control Activities

Documentation of Control Activities Through Policies and Procedures

12.02 Management establishes control activities by documenting in policies what is expected and in procedures specified actions that implement policies, to mitigate risks to achieving the entity's objectives to acceptable levels [**documentation requirement**].[101]

12.03 Management documents in policies and procedures for each unit within the entity's organizational structure its responsibility for a business process's objectives and related risks and control activity design, implementation, and operating effectiveness.[102] Each unit, with guidance from management, determines the policies necessary to operate the business process based on the objectives and related risks. Each unit also documents policies and procedures in the appropriate level of detail to allow management to effectively monitor the control activity. The documentation may appear in various forms, such as management directives, administrative policies, or operating manuals.

12.04 Those in key roles for the unit may further define policies through day-to-day procedures, depending on the rate of change in the operating environment and complexity of the business process. Procedures may include the timing of when a control activity occurs and any follow-up corrective actions to be performed by competent personnel if deficiencies are identified.[103] Management communicates the policies and procedures entity-wide so that personnel can implement the control activities for their assigned responsibilities.

[101] See paras. 3.09 through 3.12 for further discussion of documentation of the internal control system.

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

[103] See paras. 17.06 through 17.08 for further discussion of corrective actions.

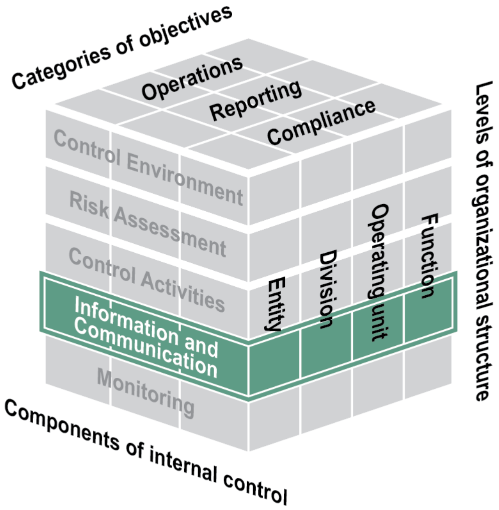
Periodic Review of Control Activities

12.05 Management reviews policies, procedures, and related control activities on a periodic and ongoing basis for continued relevance and effectiveness in achieving the entity’s objectives or mitigating related risks.[104] If there is a significant change in an entity’s process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, business processes, or information technology. A new law or regulation may change an entity’s objectives or how an entity is to achieve an objective. Further, in the federal environment, this may occur through government-wide policy or guidance issued by entities like the Office of Management and Budget, Office of Personnel Management, and the Department of the Treasury. Management considers these changes in its periodic and ongoing reviews. Management also considers the results of its monitoring activities to determine whether control activities are designed and implemented effectively.[105]

[104] See paras. 16.04 through 16.08 for further discussion of monitoring the effectiveness of internal control.

[105] See paras. 16.09 and 17.05 for further discussion of management’s evaluation of the results of monitoring and identified internal control issues.

Information and Communication



Sources: COSO and GAO. | GAO-25-107721

Overview

Management uses quality information to support the internal control system. Effective information and communication are vital for an entity to achieve its objectives. Entity management needs access to relevant and reliable communication related to internal as well as external events. Information and communication support the functioning of all components of internal control and achieving the entity's operations, reporting, and compliance objectives.

Principles

13. Management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system.
14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.
15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.

Principle 13 - Use Quality Information

13.01 Management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system.

Attributes

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

- Identification of Information Requirements
- Relevant Data from Reliable Sources
- Data Processed into Quality Information

Identification of Information Requirements

13.02 Management designs a process that uses the entity's objectives and related risks to identify the information requirements needed to support the internal control system. Information requirements consider the needs of both internal and external users. Management defines the identified information requirements at the relevant level and requisite specificity for appropriate personnel.

13.03 Management identifies information requirements in an iterative and ongoing process that occurs throughout the design, implementation, and operation of an effective internal control system. An entity's controls within the five components of internal control establish information requirements. As change in the entity and its objectives and risks occurs, management changes information requirements as needed to meet these modified objectives and address these modified risks. Management establishes information requirements through policies and procedures, with clear responsibility and accountability for the quality of information. These information requirements are communicated both internally and externally, such as with service organizations.

Relevant Data from Reliable Sources

13.04 Management obtains or generates relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Relevant data have a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. Management obtains relevant data through a variety of forms, including using manual input or compilation, using information technology, or coordinating with other entities to obtain or access data.[106] Sources of data can be operational, reporting, or compliance related. Management obtains data on a timely basis so that they can be used for effective monitoring.

Data Processed into Quality Information

13.05 Management processes relevant data obtained or generated from reliable sources into quality information through the entity's information system. The entity's 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.

13.06 Management develops the entity's information system to obtain, generate, and process relevant data into quality information to meet the identified information requirements needed to support the internal control system. Information processing can be manual, automated through the use of information technology, or a combination of both.

13.07 Management evaluates the processed information to determine whether it is quality information. Quality information meets the identified information requirements when relevant data from reliable sources are used. Quality information is appropriate, current, complete, accurate, accessible, verifiable, retained as appropriate, and provided on a timely basis. Management considers these characteristics and the information processing and information security objectives in evaluating processed information, and makes revisions when necessary, so that the information is quality information.[107] Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives, addressing risks, and fulfilling internal control responsibilities.

[106] See app. II for examples of sources of data that may be helpful to management.

[107] See paras. 10.18 and 11.07 for further discussion of information processing and information security objectives.

Principle 14 - Communicate Internally

14.01 Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.

Attributes

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

- Communication Throughout the Entity
- Appropriate Methods of Communication

Communication Throughout the Entity

14.02 Management communicates relevant and quality information throughout the entity using established reporting lines. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Quality information is communicated down, across, up, and around reporting lines to all levels of the entity.

14.03 Management communicates relevant and quality information down and across reporting lines to enable personnel to understand and perform key roles in achieving objectives, addressing risks, and supporting the internal control system. In these communications, management assigns the internal control responsibilities for key roles. Communications support the functioning of all five components of internal control and the achievement of the entity’s objectives. Communications may include legal and regulatory requirements, ethical values, the entity’s objectives, identified risks, policies and procedures that support personnel in performing their internal control responsibilities, and the results of monitoring activities that may include corrective actions to remediate internal control deficiencies.

14.04 Management obtains relevant and quality information about the entity’s business processes that flows up the reporting lines from personnel to help management achieve the entity’s objectives. Information communicated by personnel may include internal control issues; this communication helps management identify internal control deficiencies and take corrective action.

14.05 The oversight body obtains relevant and quality information that flows up the reporting lines from management and other personnel. Information relating to internal control communicated to the oversight body includes significant matters about adherence to, changes in, or issues arising from the internal control system. This upward communication is necessary for the effective oversight of internal control.

14.06 Personnel use separate reporting lines to go around upward reporting lines when these lines are compromised. Laws and regulations may require entities to establish separate lines of communication, such as whistleblower and ethics hotlines, for communicating confidential information. Management informs employees of these separate reporting lines, how they operate, how they are to be used, and how the information will remain confidential.

Appropriate Methods of Communication

14.07 Management selects appropriate methods for communicating internally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider follow:

- **Audience** - The intended recipients of the communication.
- **Nature of information** - The purpose and type of information being communicated.
- **Availability** - Information readily available to the audience when needed.
- **Cost** - The resources used to communicate the information.
- **Legal or regulatory requirements** - Requirements in laws and regulations that may impact communication.

14.08 Based on consideration of the factors, management selects appropriate methods of communication. Management evaluates the entity’s methods of communication on a periodic and ongoing basis so that the organization has the appropriate tools to communicate quality information throughout the entity on a timely basis.

Principle 15 - Communicate Externally

15.01 Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.[108]

Attributes

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

- Communication with External Parties
- Appropriate Methods of Communication

Communication with External Parties

15.02 Management communicates with, and obtains relevant and quality information from, appropriate external parties using established reporting lines. Open two-way external reporting lines allow for this communication. External parties may include service organizations, suppliers, contractors, regulators, regulated entities, external auditors, federal entities, state and local governments, grantees, and the public.

15.03 Management communicates relevant and quality information externally through reporting lines so that appropriate external parties can help the entity achieve its objectives, address related risks, and support its internal control system. Information communicated by management includes significant matters relating to the entity’s events and activities that impact its internal control system. For instance, information communicated to service organizations may include information on the entity’s objectives and ethical values, identified risks, internal control practices to consider, and performance metrics. Information communicated for the entity to achieve program-related objectives may include information on eligibility, reporting, and audit requirements for recipients of federal financial assistance and legal and regulatory requirements to regulated entities.

15.04 Management obtains information through reporting lines from external parties. Information communicated to management includes significant matters relating to risks, changes, or issues that impact the entity’s internal control system. Communication may also include

[108] External communication is viewed distinctly from the external reporting objective, as discussed in para. 6.03. Reporting objectives require all five components of internal control. In contrast, the information and communication component supports the functioning of all components of reporting objectives, as well as operations and compliance objectives.

information for the entity to achieve program-related objectives. These communications are necessary for the effective operation of internal control. Management evaluates external information obtained against the characteristics of quality information and information processing objectives and takes any necessary actions so that the information is quality information.[109]

15.05 The oversight body obtains information through reporting lines from external parties. Information communicated to the oversight body includes significant matters relating to risks, changes, and issues that impact the entity's internal control system. This communication is necessary for the effective oversight of internal control.

15.06 External parties use separate reporting lines when external reporting lines are compromised. Laws and regulations may require entities to establish separate lines of communication, such as whistleblower and ethics hotlines, for communicating confidential information. Management informs external parties of these separate reporting lines, how they operate, how they are to be used, and how the information will remain confidential.

Appropriate Methods of Communication

15.07 Management selects appropriate methods for communicating externally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider follow:

- **Audience** - The intended recipients of the communication.
- **Nature of information** - The purpose and type of information being communicated.
- **Availability** - Information readily available to the audience when needed.
- **Cost** - The resources used to communicate the information.
- **Legal or regulatory requirements** - Requirements in laws and regulations that may impact communication.

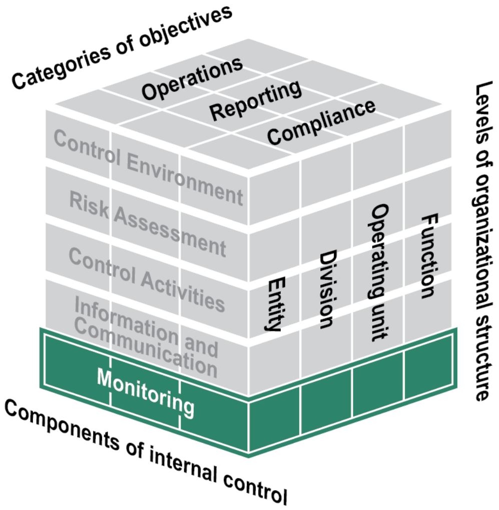
15.08 Based on consideration of the factors, management selects appropriate methods of communication. Management evaluates the entity's methods of communication on a periodic and ongoing basis so

[109] See para. 10.18 for further discussion of information processing objectives.

that the organization has the appropriate tools to communicate quality information throughout and outside of the entity on a timely basis.

15.09 Government entities not only report to the head of the government, legislators, and regulators but to the public as well. In the federal government, entities not only report to the President and Congress but also to the public. Entities consider appropriate methods for communicating with such a broad audience.

Monitoring



Sources: COSO and GAO. | GAO-25-107721

Overview

Since internal control is a dynamic process that has to be adapted continually to the risks and changes an entity faces, monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environments, laws, resources, and risks from both internal and external sources. Internal control monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews. Corrective actions are a necessary complement to monitoring activities for achieving objectives.

Principles

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
17. Management should remediate identified internal control deficiencies on a timely basis.

Principle 16 - Perform Monitoring Activities

16.01 Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

Attributes

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

- Establishment of a Baseline
- Internal Control System Monitoring
- Evaluation of Results

Establishment of a Baseline

16.02 Monitoring activities evaluate whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning or if change is needed. Management establishes a baseline to monitor the internal control system. The baseline is the current state of the internal control system compared against management's design of the internal control system. The baseline represents the difference between the criteria for the design of the internal control system and the condition of the internal control system at a specific point in time. In other words, the baseline consists of issues and deficiencies identified in an entity's internal control system.

16.03 Once established, management can use the baseline as criteria in evaluating the internal control system and make changes to reduce the difference between the criteria and condition. Management reduces this difference in one of two ways. Management either changes the design of the internal control system to better address the objectives and risks of the entity or improves the operating effectiveness of the internal control system. As part of monitoring, management determines when to revise the baseline to reflect changes in the internal control system.

Internal Control System Monitoring

16.04 Management monitors the internal control system through ongoing monitoring and separate evaluations.[110] Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change. Separate evaluations are performed periodically and may provide feedback on the effectiveness of ongoing monitoring. Many of the

[110] Monitoring the internal control system includes monitoring the effectiveness of any separate processes within the system that management establishes as part of its risk response, such as those over improper payments, fraud, information security, and rapidly implemented or substantially changed programs.

methods and tools described below may be used for both ongoing monitoring and separate evaluations, depending on when and how they are implemented.[111]

16.05 Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, trend analysis, data analytics, activities to identify improper payments or potential fraud, testing, and other routine actions. Ongoing monitoring may include automated tools, which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions or by automating data analytics.

16.06 Management uses separate evaluations to monitor the design and operating effectiveness of the overall internal control system at a specific time or of a specific function or process. The scope and frequency of separate evaluations depend primarily on the assessment of risks, risk responses, evolving technology, identification of new risks or deficiencies, results of ongoing monitoring, and rate of change within the entity and its environment. Management may also increase the frequency of separate evaluations when management rapidly implements a new program or substantially changes an existing one, such as emergency assistance programs. Separate evaluations include observations, inquiries, reviews, improper payment estimates,[112] and other examinations, as appropriate. These evaluate whether controls to effect principles across the entity are designed, implemented, and operating effectively. Separate evaluations may also take the form of self-assessments, which include cross-operating unit or cross-functional evaluations.

16.07 Management also uses the results of separate evaluations performed in connection with internal and external audits, investigations, and other evaluations that may involve the review of internal control

[111] Some types of control activities can also be used as a monitoring activity, depending on when and how they are implemented. See para. 10.04 for examples of common categories of control activities and app. II for guidance on distinguishing between monitoring activities and control activities and examples of control activities that may also be implemented as monitoring activities.

[112] Management estimates improper payments to understand the scope of the problem and evaluate the effectiveness of internal controls in addressing improper payment risk. Management may estimate improper payments more frequently than mandated by law or when programs are rapidly implemented or substantially changed. See para. 8.13 for further discussion of improper payment risk assessments.

design and testing of internal controls 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 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 controls performed by service organizations that are necessary for the entity to achieve its control objectives. 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.[113] 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 the results of ongoing monitoring and separate evaluations to identify internal control issues [**documentation requirement**].[114] 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.

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

[114] See paras. 3.09 through 3.12 for further discussion of documentation of the internal control system.

Principle 17 - Evaluate Issues and Remediate Deficiencies

17.01 Management should remediate identified internal control deficiencies on a timely basis.

Attributes

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

- Reporting of Issues
- Evaluation of Issues
- Corrective Actions

Reporting of Issues

17.02 Personnel report internal control issues through established reporting lines to the appropriate internal and external parties on a timely basis to enable the entity to promptly evaluate those issues and complete corrective action to remediate issues that rise to the level of internal control deficiencies.[115]

17.03 Personnel may identify internal control issues while performing their assigned internal control responsibilities. Personnel communicate these issues internally to the person in the key role responsible for the internal control or associated process and, when appropriate, to at least one level of management above that individual. Depending on the nature of the issues, personnel may consider reporting certain issues to the oversight body or an established hotline. Such issues may include

- issues that cut across the organizational structure or extend outside the entity to service organizations, contractors, or suppliers and
- issues that may not be remediated because of the interests of management, such as sensitive information regarding fraud or other illegal acts.[116]

17.04 Depending on the entity’s regulatory or compliance requirements, the entity may also be required to report issues externally to appropriate external parties, such as the legislators, regulators, and standard-setting

[115] See paras. 14.02 through 14.06 for further discussion of internal reporting lines and paras. 15.02 through 15.06 for further discussion of external reporting lines.

[116] See paras. 8.06 through 8.07 for further discussion of fraud.

bodies that establish laws, rules, regulations, or standards to which the entity is subject.

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 internal and external audits and evaluations, on a timely basis [**documentation requirement**].[117] 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.[118] 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 corrective actions to remediate internal control deficiencies, including those reported from internal and external audits and evaluations, on a timely basis [**documentation requirement**].[119] 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,

[117] See paras. 3.09 through 3.12 for further discussion of documentation of the internal control system.

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

[119] See paras. 3.09 through 3.12 for further discussion of documentation of the internal control system.

- measurable indicators of compliance and remediation to assess and validate progress throughout the remediation process, 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.[120]

17.08 Corrective actions also include remediating audit and evaluation findings.[121] The remediation process begins when audit or other review results are reported to management. It is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates that the findings and recommendations do not warrant management action. Management, with oversight from the oversight body, monitors the status of remediation efforts so that they are completed on a timely basis.

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

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

Appendix I: Requirements

The following is a list of the requirements included in the Green Book.

The five components of internal control must be effectively designed, implemented, and operating, and operating together in an integrated manner, for an internal control system to be effective. (paragraph OV2.04)

Principle Requirements

The 17 principles support the effective design, implementation, and operation of the associated components and represent requirements necessary to establish an effective internal control system. The 17 principles required by the Green Book are as follows:

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.
2. The oversight body should oversee the entity’s internal control system.
3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity’s objectives.
4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.
6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.
7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.
8. Management should consider risks related to fraud, improper payments, and information security when identifying, analyzing, and responding to risks.
9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.
10. Management should design control activities to mitigate risks to achieving the entity’s objectives to acceptable levels.
11. Management should design general control activities over information technology to mitigate risks to achieving the entity’s objectives to acceptable levels.

12. Management should implement control activities through policies and procedures.
13. Management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system.
14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.
15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.
16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
17. Management should remediate identified internal control deficiencies on a timely basis.

Documentation Requirements

Documentation is a necessary part of an effective internal control system. The level and nature of documentation may vary based on the size of the entity and the complexity of the processes it performs. Management exercises judgment in determining the extent or type of documentation that is needed. Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system. (paragraph OV2.11) Management develops and maintains documentation of its internal control system. (paragraph 3.09) Documentation of the internal control system is further discussed at principle 3.

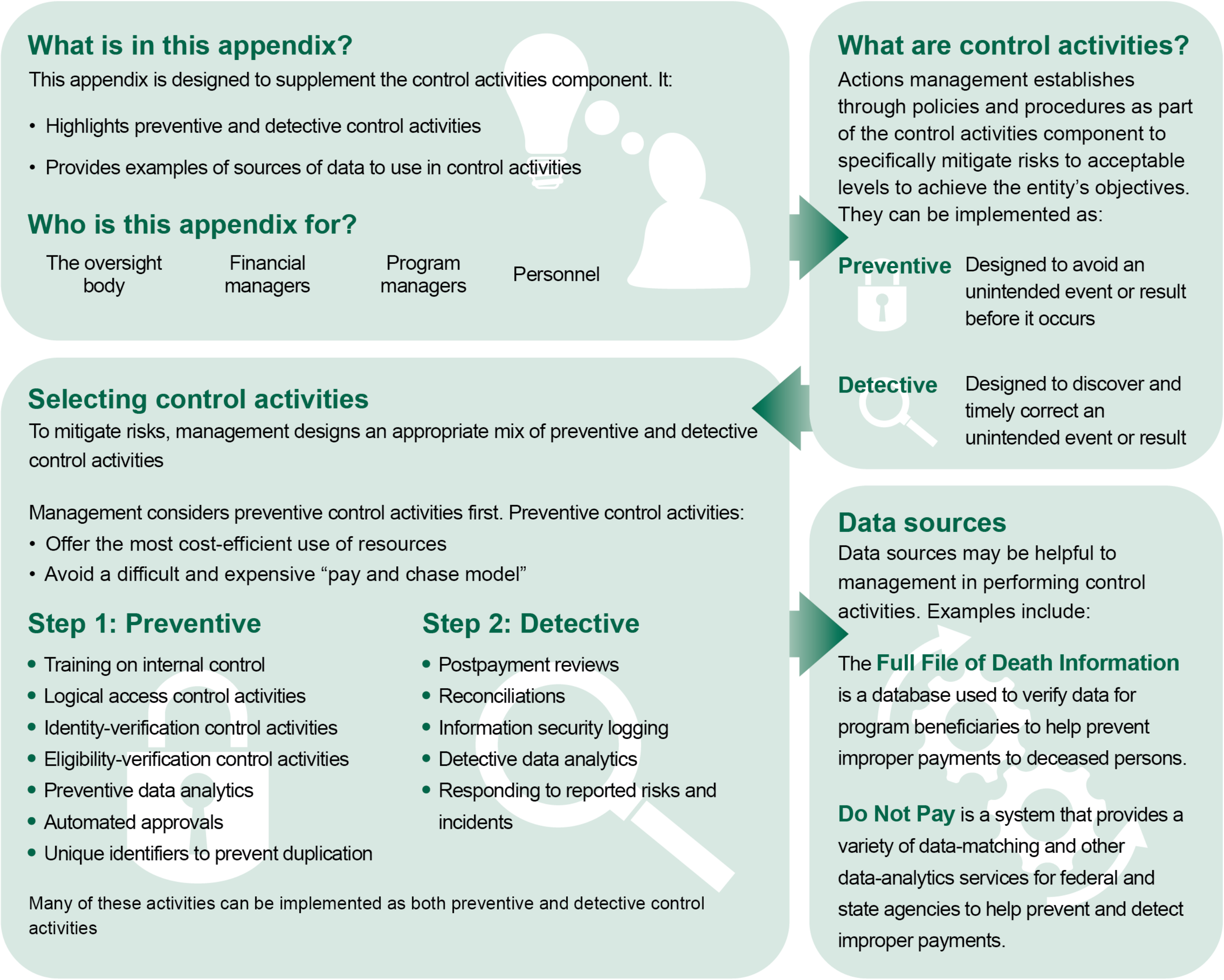
The Green Book also includes the following minimum documentation requirements:

- If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale for how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively. (paragraph OV2.06)
- Management documents the results of the risk assessments, 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. (paragraph 7.15)

- Management documents a change assessment process for identifying, analyzing, and responding to risks related to significant changes so that the internal control system can be quickly adapted as needed to respond to significant changes as they occur. (paragraph 9.05)
- Management establishes control activities by documenting in policies what is expected and in procedures specified actions that implement policies, to mitigate risks to achieving the entity’s objectives to acceptable levels. (paragraph 12.02)
- Management evaluates and documents 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 internal and external audits and evaluations, on a timely basis. (paragraph 17.05)
- Management completes and documents corrective actions to remediate internal control deficiencies, including those reported from internal and external audits and evaluations, on a timely basis. (paragraph 17.06)

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



How do I use this appendix?

Important facts and concepts related to preventive and detective control activities

What is in this appendix?

This appendix is designed to supplement the control activities component. It:

- Highlights preventive and detective control activities
- Provides examples of sources of data to use in control activities

Who is this appendix for?

The oversight body

Financial managers

Program managers

Personnel

What are control activities?

Actions management establishes through policies and procedures as part of the control activities component to specifically mitigate risks to acceptable levels to achieve the entity's objectives. They can be implemented as:

Preventive Designed to avoid an unintended event or result before it occurs

Detective Designed to discover and timely correct an unintended event or result

Selecting control activities

To mitigate risks, management designs an appropriate mix of preventive and detective control activities

Management considers preventive control activities first. Preventive control activities:

- Offer the most cost-efficient use of resources
- Avoid a difficult and expensive "pay and chase model"

Step 1: Preventive

- Training on internal control
- Logical access control activities
- Identity-verification control activities
- Eligibility-verification control activities
- Preventive data analytics
- Automated approvals
- Unique identifiers to prevent duplication

Step 2: Detective

- Postpayment reviews
- Reconciliations
- Information security logging
- Detective data analytics
- Responding to reported risks and incidents

Many of these activities can be implemented as both preventive and detective control activities

Data sources

Data sources may be helpful to management in performing control activities. Examples include:

The **Full File of Death Information** is a database used to verify data for program beneficiaries to help prevent improper payments to deceased persons.

Do Not Pay is a system that provides a variety of data-matching and other data-analytics services for federal and state agencies to help prevent and detect improper payments.

Source: GAO. | GAO-25-107721

Overview

This appendix provides examples of preventive and detective control activities that management may consider to mitigate risks to achieving the entity's objectives to acceptable levels. It also provides examples of data sources that may be helpful in implementing the control activities.

This appendix is designed to supplement the control activities component and includes the following:

- Types of Activities
- Examples of Preventive and Detective Control Activities
- Sources of Data

Types of Activities

As part of the control activities component, management designs an appropriate mix of preventive and detective control activities to mitigate risks to achieving the entity's objectives to acceptable levels, prioritizing preventive control activities where appropriate.[1] A preventive control activity is designed to avoid an unintended event or result before it occurs. A detective control activity is designed to discover and timely correct an unintended event or result after it occurs.

The control activities component lists common categories of control activities.[2] This appendix provides examples of control activities that, for purposes of illustration, are categorized as either preventive or detective control activities. However, activities can often be implemented as preventive control activities, as detective control activities, or even as monitoring activities, depending on when or how they are implemented.[3]

Control activities and monitoring activities serve different purposes. Control activities are the actions management establishes through policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels. Monitoring activities evaluate whether each of the five components of internal control, including control activities to effect the principles within each component, is present and functioning, or if change is needed. For example, personnel may perform a control activity to reconcile inventory, which identifies, investigates, and resolves

[1] See paras. 10.10 through 10.13 for further discussion of the design of preventive and detective control activities.

[2] See para. 10.04 for further discussion of common categories of control activities.

[3] See principle 16 for further discussion of monitoring activities.

individual discrepancies. Meanwhile, management may perform a corresponding monitoring activity to inspect documentation that the reconciliation was performed appropriately, which evaluates the effectiveness of the control activity and notes any trends in the discrepancies identified to address a deficiency in the process.

When distinguishing between a control activity and a monitoring activity, management considers the underlying details of the activity, especially where the activity involves some level of supervisory review. Supervisory reviews are not automatically classified as monitoring activities, and it may be a matter of judgment whether a review is classified as a control activity or a monitoring activity.

Examples of Preventive and Detective Control Activities

The preventive and detective control activities listed below illustrate a variety of activities that may be useful to management and are designed to supplement the control activities component. The examples presented in this appendix are not all inclusive and may not include all control activities that an entity may need. The control activities listed below are categorized as either preventive or detective for the purposes of illustration, but they can often be implemented as either, depending on when or how they are implemented. Each entity tailors its control activities based on its specific needs and assessed risks, which may include activities not listed below.

Preventive Control Activities

Training on Internal Control

Management provides periodic and ongoing training to develop the knowledge, skills, and abilities of its personnel to meet changing organizational needs and to fulfill their internal control responsibilities. Training may be provided on how internal control contributes to program objectives, internal control responsibilities, how to administer internal controls, security of information technology and data, and other specialized areas as needed. Management also provides training to increase awareness of identified risks, such as fraud awareness training or training on the entity’s plan to address risks related to potential changes, such as emergency assistance programs. Management trains those in specialized information technology roles in addition to those who perform various processes using information technology. For example, management may provide information security training to all personnel interacting with information technology, which may be tailored to the specific processes they perform.

Logical Access Control Activities

Management uses logical access control activities to prevent unauthorized use of and changes to the system. Examples of these controls include network segmentation, use of passwords or other authentication mechanisms, and granting of different levels and types of permissions to different types of system users and administrators.

Identity-Verification Control Activities

Management uses identity-verification control activities to confirm that personnel and external parties are who they say they are before providing services or benefits. Management can choose from a range of identity-verification control activities and apply them uniformly to all verifications or adjust control activities based on risks that each verification presents. Management may consider offering multiple methods for authorized individuals to verify their identities, such as in person, remote physical verification, and through knowledge-based questions. Management may also require applicants for program benefits to submit photo identification, documentation, and other personal information to verify against each other and with authoritative databases before distributing funds to the individuals.

Eligibility-Verification Control Activities

Prior to providing services to program beneficiaries, management uses verification control activities to confirm the eligibility of individual applicants based on established criteria. The entity may leverage data collected internally or from external sources to determine eligibility and confirm self-certified information.

Preventive Data Analytics

Management uses preventive data analytics to identify relationships, patterns, discrepancies, and anomalies in data to make decisions and identify potential issues, such as indicators of fraudulent activity or improper payments, to avoid unintended events or results before they occur. Examples of preventive data analytics follow.

- *Data matching* - Management may apply data matching to verify key information, such as self-reported data, information necessary to determine identity or eligibility, and the validity of transactions. Data matching is a process in which information from one source is compared with information from another, such as government or third-party databases, to identify any inconsistencies.

- *Reasonableness checks* - Management may apply reasonableness checks to a dataset to determine whether the data fall within an accepted range or consist of accepted values. For example, an entity verifies that an applicant's residence is located within a disaster area before providing disaster relief assistance. Additionally, users using foreign addresses, internet protocol addresses, or bank accounts may also be subject to further review.
- *Data validation* - Data validation control activities (also known as system edit checks) are instructions programmed into an information technology system to help reasonably assure that data meet requirements before being accepted for further processing and before payments are made. Management establishes requirements that data be complete, accurate, valid, and recorded in the proper format, and may implement checks to identify missing data, incorrect data, or erroneous dates. Data validation control activities can be used to compare data entries to requirements and automatically deny entries that do not meet requirements or flag them for further review.
- *Predictive analytics* - Predictive-analytics technologies include a variety of automated processes and tools that can be used to identify particular types of behavior, including potential for fraud or improper payments, before transactions are completed.

Automated Approvals

Management uses automated approvals to authorize transactions without human intervention, which may provide consistency in the review process and expedite approvals that present a lower risk to the entity. Management updates the rules or coding of data analytics performed within the automated process as needed, such as when changes are made to a program or to eligibility criteria. Management also incorporates manual review in order to exercise appropriate judgment in addressing any issues flagged.

Unique Identifiers to Prevent Duplication

Management establishes a unique identifier for each transaction or beneficiary to reduce the possibility of providing duplicative services or benefits. Unique identifiers for transactions may include using unique invoice numbers and purchase order numbers to help identify transactions. Unique identifiers for beneficiaries may include an individual's Social Security number; employer identification number; or other identification number, such as a state driver's license or passport number. Management can then put controls in place to only process the appropriate number of claims per unique identifier and limit the possibility of an individual receiving duplicative services or benefits in one eligible period.

Detective Control Activities

Postpayment Reviews

Management uses postpayment reviews to determine whether payments were made appropriately to eligible recipients in correct amounts and whether recipients used them in accordance with law and applicable agreements. Examples of postpayment reviews include the following:

- *Recovery audits* - Management may review disbursements or financial transactions of the entity, and the related data, to identify and recover overpayments.
- *Confirmation of self-certified information* - For self-certified information that was relied on to determine eligibility or identity, management may subsequently collect supporting documentation and conduct a postpayment review. Supporting documents might include personal or business identification, tax information, employment confirmation, or income verification documents.
- *Data matching* - Management may conduct postpayment data matching to verify information, such as self-certified data and other key data, and confirm eligibility for those who have been enrolled in programs or received benefits to detect potential fraud or improper payments. Management conducts data matching using internal or external sources to verify data electronically. In addition to verifying initial eligibility, ongoing data matching can enable programs that provide recurring benefits to identify changes in key information that could affect continued eligibility and prevent future improper payments.

Reconciliations

Management performs reconciliations to confirm that transactions are processed, recorded, and accounted for completely and accurately. Reconciliations include identifying and comparing transactions from two sets of records to determine whether the transactions are recorded properly, have yet to be recorded, or were recorded improperly and require correction. Reconciliations also serve to identify unauthorized transactions and explain differences. Reconciliations may be performed by comparing internal records or by verifying the entity's records against external data, such as with a bank reconciliation.

Information Security Logging

A log is a record of events that occur within the entity's information technology, including physical and virtual platforms, networks, services, and cloud environments. Management uses logs for many functions, such as optimizing system and network performance, recording the actions of users, and providing useful data for investigating malicious activity. Many logs contain records that are relevant for information security, such as operating system logs that capture system events and audit records; application logs that capture operational and security events; and security software logs that record routine events, adverse events, and possible malicious activity.

Detective Data Analytics

Management uses detective data analytics to identify patterns, discrepancies, and anomalies in data to identify potential issues, such as fraudulent activity or improper payments, to detect and correct an unintended event or result after it occurs. Examples of detective data analytics include the following:

- *Data mining* - Management uses data mining to identify activities or transactions that deviate from expected patterns, which may indicate significant events or suspicious activity. For example, management may look for unusual transactions or data entries that do not fit an expected pattern by applying filters or predefined rules to transactions to identify those that exhibit signs of fraud. Management may automate data mining to scan data for outliers and irregularities on a continuous, real-time basis.
- *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 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 sources 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 certain federal and state agencies 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 a broader range of certified users.
- *Do Not Pay*[5] - The Do Not Pay initiative, authorized and governed by the Payment Integrity Information Act of 2019, provides a variety of data-matching and other data-analytics services to all federal and many state agencies to support their efforts to prevent and detect improper payments. As part of the Do Not Pay Initiative, the Office of Management and Budget has designated the Department of the Treasury to host the Do Not Pay Working System, which is a centralized portal through which users can search multiple databases at one time to obtain information about potential payees and awardees. Data shared through the Do Not Pay Working System include the following:
    - SSA's Full File of Death Information

[4] For more information on SSA's data exchange services and to request access to death information, see https://www.ssa.gov/dataexchange/request_dmf.html.

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

- Treasury Offset Program Debt Check
- Department of Health and Human Services' List of Excluded Individuals and Entities
- General Services Administration's System for Award Management Exclusion Records

Appendix III: Additional Resources

This appendix contains 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. The resources provided below may also be useful in addressing risks related to implementing new or substantially changed programs, including emergency assistance programs. These additional resources are primarily intended for federal executive branch agencies; however, they may also be useful to federal entities outside the executive branch and to nonfederal entities, such as state, local, and quasi-governmental entities and nonprofit organizations.

Fraud and Improper Payments Resources

GAO Fraud and Improper Payments Topic Page

GAO's Fraud and Improper Payments website provides an issue summary, multimedia resources, and recent reports on fraud and improper payments. The topic page also includes GAO's most recent estimates of the amount of fraud in federal programs and agencies' most recent reported improper payments, including steps Congress and agencies can take to help reduce fraud and improper payments.[1]

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*.[2] 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 Framework

To provide management with an overall approach to managing improper payments, particularly for new emergency assistance programs or existing assistance programs that have received increased funding in response to public health or other national emergencies, GAO published *A Framework for Managing Improper Payments in Emergency Assistance*

[1] See GAO, Fraud and Improper Payments, https://www.gao.gov/fraud-improper-payments.

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

Programs (Improper Payments Framework) in July 2023.[3] This framework can also be useful for managing improper payments in non-emergency assistance programs or during normal program operations. It includes leading principles and practices for program managers and incorporates standards for internal control and fraud risk management; payment integrity requirements from the Payment Integrity Information Act of 2019 (PIIA), codified at 31 U.S.C. §§ 3351-58; and guidance on improper payments. It also highlights aspects of managing improper payments that occur during the provision of emergency assistance, which may require greater attention.

The steps within the framework include a control environment committed to addressing improper payments, including those resulting from fraud; assessing new risks, such as those stemming from the emergency; and implementing and monitoring control activities that address identified 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.

GAO Fraud Risk Framework

To help combat fraud in government entities and programs—both during normal operations and emergencies—GAO published *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).[4] Issued in 2015, the Fraud Risk Framework identifies leading practices for managing fraud risk and encompasses control activities for preventing, detecting, and responding to fraud, with an emphasis on prevention.

The Fraud Risk Framework provides comprehensive guidance for conducting fraud risk assessments and using the results as part of the development of a robust antifraud strategy. It also describes leading practices for establishing a control environment that is conducive to fraud risk management; designing and implementing controls to prevent and detect potential fraud; and monitoring and evaluating to provide

[3] GAO, *A Framework for Managing Improper Payments in Emergency Assistance Programs*, GAO-23-105876 (Washington, D.C.: July 2023).

[4] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

assurances to managers that they are effectively preventing, detecting, and responding to potential fraud.

GAO Antifraud Resource

GAO's Antifraud Resource website provides resources to help federal officials learn more about fraud schemes that affect the federal government, their underlying concepts, and how to combat such fraud.[5] The resource includes GAO's Conceptual Fraud Model, which was developed to determine the nature of known fraud, both financial and nonfinancial, that affects federal programs and operations.

OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*,[6] provides requirements for federal executive branch agencies to establish and implement a process to properly assess and improve internal control. The circular directs federal executive branch agencies to adhere to the leading practices identified in GAO's Fraud Risk Framework as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. This includes evaluating fraud risks and using a risk-based approach to design and implement control activities to mitigate identified fraud risks.

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*.[7] 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.

[5] GAO, Antifraud Resource, https://antifraud.gaoinnovations.gov.

[6] Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular A-123 (Washington, D.C.: July 15, 2016).

[7] 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).

Official PaymentAccuracy Website

The PaymentAccuracy.gov website provides information on agencies' progress in preventing and recovering improper payments, including resources for specific data, laws, and implementing guidance.[8]

Information Security Resources

National Institute of Standards and Technology Guidance

The National Institute of Standards and Technology (NIST) develops information security and cybersecurity standards for categorizing information and information technology systems, along with their security requirements, and guidelines for detection and handling of security incidents. NIST standards and guidelines include Federal Information Processing Standards (FIPS) and NIST Special Publications (SP) in the 800 series (NIST SP 800).[9] For example:

- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirement.[10]
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, addresses organizational requirements for managing risks in accordance with legal requirements for information security management for federal agencies.[11]
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, is a catalog of security and

[8] The website, https://www.paymentaccuracy.gov, is an OMB-managed official U.S. government website.

[9] NIST standards and guidelines may periodically be updated, and the current versions can be found at https://csrc.nist.gov/publications.

[10] National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems,* NIST FIPS 200 (Gaithersburg, Md.: March 2006). See https://csrc.nist.gov/pubs/fips/200/final.

[11] National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST SP 800-39 (Gaithersburg, Md.: March 2011). See https://csrc.nist.gov/pubs/sp/800/39/final.

privacy internal controls that can be implemented as part of an entity-wide process to manage risk.[12]

In addition, federal entities are required[13] to use NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) for managing their cybersecurity risks.[14] The Cybersecurity Framework is guidance, based on existing standards, guidelines, and practices, for organizations to better manage and reduce cybersecurity risk.

NIST also issues publications on emerging technologies. For example, NIST AI 100-1, *Artificial Intelligence Risk Management Framework*, offers a resource to the organizations designing, developing, deploying, or using artificial intelligence (AI) systems to help manage risks of AI and promote trustworthy and responsible development and use of AI systems.[15]

GAO Cybersecurity Topic Page

GAO's Cybersecurity website provides an overview, multimedia resources, and key reports on cybersecurity, including steps agencies can take to help address cybersecurity challenges.[16]

GAO Science & Technology Topic Page

GAO's Science & Technology website provides an overview of emerging technologies that may present both opportunities and risks to agencies, such as AI, automation, machine learning, and blockchain technology.

[12] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5 (Gaithersburg, Md.: December 2020). See https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[13] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017) (reprinted in 82 Fed. Reg. 22391), requires entities to use NIST's *Framework for Improving Critical Infrastructure Cybersecurity* to manage their cybersecurity risks. See https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[14] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (Gaithersburg, Md.: February 2024). See https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20.

[15] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Gaithersburg, Md.: January 2023). See https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10.

[16] See GAO, Cybersecurity, https://www.gao.gov/cybersecurity.

The topic page includes recent reports and other resources for responsible use of emerging technologies.[17]

OMB Circular A-130, Managing Information as a Strategic Resource

OMB Circular A-130, *Managing Information as a Strategic Resource*,[18] establishes minimum requirements for federal information security programs, assigns federal agency responsibilities for the security of information and information systems, and links agency information security programs and agency management control systems established in accordance with OMB Circular A-123.

[17] See GAO, Science & Technology, https://www.gao.gov/science-technology.

[18] Office of Management and Budget, *Managing Information as a Strategic Resource,* OMB Circular A-130 (Washington, D.C.: July 28, 2016).

Appendix IV: Acknowledgments

Comptroller General's Advisory Council on Standards for Internal Control in the Federal Government (2023-2025)

Dr. Audrey A. Gramling, Chair
Oklahoma State University

Dr. Brett M. Baker
National Archives and Records Administration, Office of Inspector General

Matthew Bohdan
Plante Moran, PLLC

Sheila Conley
U.S. Department of Health and Human Services (Retired)

Douglas Cotnoir
State of Maine, Office of the State Controller

Kayla Futch
KPMG LLP

MelaJo K. Kubacki
U.S. Department of Housing and Urban Development

Allison C. Lerner
National Science Foundation, Office of Inspector General (Retired)

Sonia Montano
City and County of Denver, Colorado, Office of the Auditor

Edward J. Murray
U.S. Department of Veterans Affairs

Sherrill F. Norman
State of Florida, Auditor General

Dr. Douglas F. Prawitt
Committee of Sponsoring Organizations of the Treadway Commission and Brigham Young University

Margaret Vo Schaus
National Aeronautics and Space Administration

Tammy Whitcomb Hull
U.S. Postal Service, Office of Inspector General

GAO Project Team

James R. Dalkin, Director

Carrie J. Morrison, Assistant Director
Estelle M. Tsay-Huang, Assistant Director
Lanie M. Carlson, Senior Auditor
Maria M. Morton, Senior Auditor
Heena R. Patel, Senior Auditor
Cherry Y. Vasquez, Senior Auditor

Kristen A. Kociolek, Managing Director, Financial Management and Assurance
Robert F. Dacey, Chief Accountant

Staff Acknowledgments

In addition to the project team named above, also contributing were Johana Ayers, Nicole Burkart, Alicia Cackley, Joseph Crays, Vijay D’Souza, Paulissa Earl, Lauren Stacy Fassler, Matthew M. Gardner, Jason M. Kelly, Jason Kirwan, Jonathon Oldmixon, Andrew Pauline, and Kimberly Y. Young.

Glossary

The following terms are provided to assist in clarifying the *Standards for Internal Control in the Federal Government*. The most relevant paragraph numbers are provided for reference.

application control activities: 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 input, processing, and output of data (paragraph 10.07)

attributes: Provide further explanation of the principles and may also contain minimum documentation requirements. Management considers attributes when designing, implementing, and operating the associated principles (paragraph OV2.08)

baseline: The current state of the internal control system compared against management’s design of the internal control system; it represents the difference between the criteria for the design of the internal control system and the condition of the internal control system at a specific point in time (paragraph 16.02)

business processes: Processes established across the entity to enable organizations to achieve their objectives and transform inputs into outputs through a series of transactions or activities (paragraph OV2.14)

competence: The capability to carry out assigned responsibilities (paragraph 4.02)

complementary user entity controls: Controls that a service organization identifies as being necessary for the entity to implement to achieve the control objectives specified by the service organization (paragraph OV4.04)

component: One of the five required elements of internal control; the internal control components are Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring (paragraph OV2.04)

configuration management: Control activities to develop and maintain the operating and security features of information technology and control changes to their configuration (paragraph 11.09)

contingency plans/planning: The processes defined to address an entity’s need to respond to sudden changes or unexpected events that could compromise the internal control system (paragraphs 4.06 and 11.17)

controls: Policies and procedures management establishes to effect relevant principles within each component of internal control (paragraph OV1.04)

control activities: Actions management establishes through policies and procedures as part of the control activities component to specifically mitigate risks to achieving the entity’s objectives to acceptable levels (paragraphs OV1.04 and 10.02)

control objective: The aim or purpose of specified controls to effect relevant principles within each component of internal control (paragraph OV3.05)

deficiency: When the design, implementation, or operation of a control does not allow management or other personnel, in the normal course of performing their assigned responsibilities, to achieve the entity’s objectives (paragraph OV3.07)

detective control activity: A control activity that is designed to discover and timely correct an unintended event or result after it occurs (paragraph 10.10)

entity objective: What an entity wants to achieve; entity objectives are intended to meet the entity’s mission, strategic plan, and goals; objectives are also set to meet requirements for the entity that are established in applicable laws and regulations (paragraph OV2.22)

entity-level control activities: Controls designed to mitigate risks that have a pervasive effect on an entity’s internal control system; entity-level control activities may include controls related to the entity’s risk assessment process, control environment, service organizations, management override, and performance or analytical reviews (paragraph 10.16)

fraud: Involves obtaining something of value through willful misrepresentation (paragraph 8.06)

general control activities: Actions established through policies and procedures that apply to all or a large segment of an entity’s information technology designed to mitigate information security risks; general control activities include security management, logical and physical access, configuration management, segregation of duties, and contingency planning (paragraphs 11.07 and 11.09)

Green Book: The commonly used name for *Standards for Internal Control in the Federal Government* (Overview: How to Use the Green Book)

improper payment: Any payment that should not have been made or that was made in an incorrect amount (e.g., overpayments and underpayments); payments are also considered improper when there is insufficient or lack of documentation (paragraph 8.11)

information security: The protection of information or information technology from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability (paragraph 11.02)

information system: 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 (paragraph 13.05)

information technology: The infrastructure, platforms, and software used to automate processes (paragraph 11.05)

information technology infrastructure: The physical information technology resources necessary to run software, including the hardware and devices used for information processing, data storage, and network communication (paragraph 11.05)

inherent risk: The risk to an entity in the absence of management's response to the risk (paragraph 7.03)

internal control: A process effected by an entity's oversight body, management, and other personnel, designed to provide reasonable assurance that the objectives of an entity will be achieved (paragraph OV1.01)

internal control system: Consists of integrated and continuous processes, effected by people, that are collectively designed to provide reasonable assurance, not absolute assurance, that an entity's objectives will be achieved (paragraph OV1.05)

key role: A position in an organizational structure that is assigned an overall responsibility of an entity (paragraph 3.06)

likelihood of occurrence: The level of possibility that an unintended event or result will occur (paragraph 7.08)

logical and physical access: Control activities that restrict access to information technology to authorized users (paragraph 11.09)

magnitude of impact: The likely magnitude of the effect of the risk on the entity’s ability to achieve its objectives; it is affected by factors such as the size, pace, and duration of the risk’s impact (paragraph 7.08)

management: Personnel who are directly responsible for all activities of an entity, including the design, implementation, and operating effectiveness of an entity’s internal control system (paragraph OV2.19)

monitoring activities: Activities that evaluate whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning or if change is needed (paragraph 16.02)

must: Denotes a requirement that management must comply with in all cases; these requirements are the components of internal control (paragraph OV2.04)

organizational structure: The overall entity, divisions, operating units, functions, and other structures management uses to achieve the objectives (paragraph OV2.14)

oversight body: Those responsible for overseeing management’s design, implementation, and operation of an internal control system (paragraph OV2.19)

performance measure: A means of evaluating the entity’s performance in achieving objectives (paragraph 6.07)

platforms: The logical information technology resources necessary to run application software, including operating systems and related computer programs, tools, and utilities (paragraph 11.05)

policies: Reflect management or oversight body statements of what is expected to be done to effect internal control (OV1.04)

preventive control activity: A control activity that is designed to avoid an unintended event or result before it occurs (paragraph 10.10)

principle: Fundamental concept that is integral to supporting the effective design, implementation, and operation of the associated components of internal control and represents requirements necessary to establish an effective internal control system (paragraph OV2.05)

procedures: Actions that implement policies (paragraph OV1.04)

qualitative objectives: Objectives where management may need to design performance measures that indicate a level or degree of performance, such as milestones (paragraph 6.07)

quality information: Information that supports the internal control system, using relevant data from reliable sources that are appropriate, current, complete, accurate, accessible, verifiable, retained as appropriate, and provided on a timely basis (paragraph 13.07)

quantitative objectives: Objectives where performance measures may be a targeted percentage or numerical value (paragraph 6.07)

reasonable assurance: A high degree of confidence, but not absolute confidence (paragraph OV1.05)

reporting lines: Communication lines, both internal and external, at all levels of the organization that provide methods of communication that can flow down, across, up, and around the organizational structure (paragraph 3.04)

residual risk: The risk that remains after management’s response to inherent risk (paragraph 7.03)

risk: The possibility that an event will occur and adversely affect the achievement of objectives (paragraph 7.02)

risk tolerance: The acceptable level of variation in performance relative to the achievement of objectives (paragraph 6.08)

security management: A separate process, addressing all components of internal control, for responding to risks related to information security (paragraph 11.09)

segregation of duties: The separation of responsibilities for performing control activities related to the authority, custody, and accounting of operations so that incompatible duties are segregated (paragraphs 10.21 and 10.22)

service organization: An external party that performs business processes or provides services in support of business processes for an entity (paragraph OV4.03)

should: Denotes a principle requirement management should comply with except in rare circumstances where the requirement is not relevant for the entity (paragraphs OV2.06 and OV2.07)

software: The application software, access control software, and other software used to perform specific functions of the entity's business processes (paragraph 11.05)

succession plans: The processes that address an entity's need to replace competent personnel over the long term (paragraph 4.06)

transaction control activities: Controls that directly mitigate information processing risks in the entity's business processes (paragraph 10.17)

user control activities: Partially automated control activities that individuals perform by using information technology or by relying on the information processed through technology (paragraph 10.07)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The printed version of the 2025 revision to *Standards for Internal Control in the Federal Government* can be ordered through the Government Publishing Office (GPO) online http://bookstore.gpo.gov/ or by calling 202-512-1800 or 1-866-512-1800 toll free.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us