United States Government Accountability Office



By the Comptroller General of the United States

September 2014

Standards for Internal Control in the Federal Government

GAO-14-704G

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?

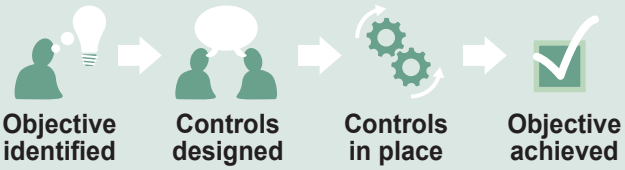
Internal control helps an entity

- 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?



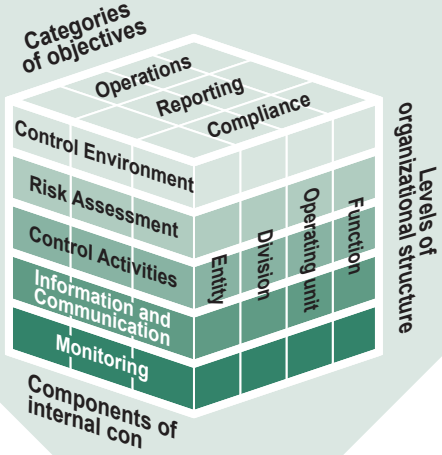
An entity uses the Green Book to design, implement, and operate internal controls to achieve its objectives related to operations, reporting, and compliance.

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

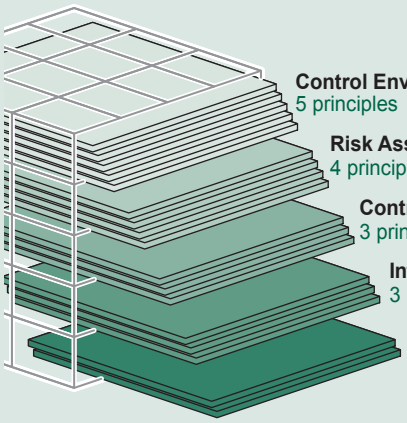
The cube

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

Each of the five components of internal control contains several principles. Principles are the requirements of each component.



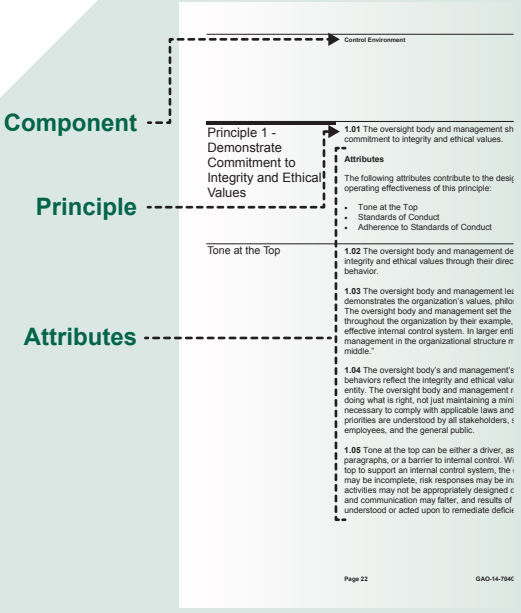
- **Control Environment** 5 principles
- **Risk Assessment** 4 principles
- **Control Activities** 3 principles
- **Information and Communication** 3 principles
- **Monitoring** 2 principles

Attributes

Each principle has important characteristics, called attributes, which explain principles in greater detail.

Page structure

Green Book pages show components, principles, and attributes.



Sources: GAO and COSO.

GAO.GOV/GREENBOOK

GAO-14-704G

Contents

Overview 1

Foreword 1
How to Use the Green Book 3
Section 1 - Fundamental Concepts of Internal Control 5
Definition of Internal Control 5
Definition of an Internal Control System 5
Section 2 - Establishing an Effective Internal Control System 6
Presentation of Standards 6
Components, Principles, and Attributes 7
Internal Control and the Entity 9
Roles in an Internal Control System 11
Objectives of an Entity 12
Section 3 - Evaluation of an Effective Internal Control System 14
Factors of Effective Internal Control 15
Evaluation of Internal Control 15
Section 4 - Additional Considerations 17
Service Organizations 17
Large versus Small Entities 18
Benefits and Costs of Internal Control 19
Documentation Requirements 19
Use by Other Entities 20

Control Environment 21

Principle 1 - Demonstrate Commitment to Integrity and Ethical Values 22
Tone at the Top 22
Standards of Conduct 23
Adherence to Standards of Conduct 23
Principle 2 - Exercise Oversight Responsibility 24
Oversight Structure 24
Oversight for the Internal Control System 26
Input for Remediation of Deficiencies 27
Principle 3 - Establish Structure, Responsibility, and Authority 27
Organizational Structure 27
Assignment of Responsibility and Delegation of Authority 28
Documentation of the Internal Control System 29
Principle 4 - Demonstrate Commitment to Competence 30
Expectations of Competence 30
Recruitment, Development, and Retention of Individuals 31
Succession and Contingency Plans and Preparation 31
Principle 5 - Enforce Accountability 32

Enforcement of Accountability 32
Consideration of Excessive Pressures 33

Risk Assessment 34

Principle 6 - Define Objectives and Risk Tolerances 35
Definitions of Objectives 35
Definitions of Risk Tolerances 36
Principle 7 - Identify, Analyze, and Respond to Risks 37
Identification of Risks 37
Analysis of Risks 38
Response to Risks 39
Principle 8 - Assess Fraud Risk 40
Types of Fraud 40
Fraud Risk Factors 41
Response to Fraud Risks 41
Principle 9 - Identify, Analyze, and Respond to Change 42
Identification of Change 42
Analysis of and Response to Change 43

Control Activities 44

Principle 10 - Design Control Activities 45
Response to Objectives and Risks 45
Design of Appropriate Types of Control Activities 45
Design of Control Activities at Various Levels 49
Segregation of Duties 50
Principle 11 - Design Activities for the Information System 51
Design of the Entity's Information System 51
Design of Appropriate Types of Control Activities 53
Design of Information Technology Infrastructure 53
Design of Security Management 54
Design of Information Technology Acquisition, Development, and Maintenance 55
Principle 12 - Implement Control Activities 56
Documentation of Responsibilities through Policies 56
Periodic Review of Control Activities 56

Information and Communication 58

Principle 13 - Use Quality Information 59
Identification of Information Requirements 59

	Relevant Data from Reliable Sources	59
	Data Processed into Quality Information	59
	Principle 14 - Communicate Internally	60
	Communication throughout the Entity	60
	Appropriate Methods of Communication	61
	Principle 15 - Communicate Externally	62
	Communication with External Parties	62
	Appropriate Methods of Communication	63
Monitoring		64
	Principle 16 - Perform Monitoring Activities	65
	Establishment of a Baseline	65
	Internal Control System Monitoring	65
	Evaluation of Results	66
	Principle 17 - Evaluate Issues and Remediate Deficiencies	67
	Reporting of Issues	67
	Evaluation of Issues	68
	Corrective Actions	68
Appendix I	Requirements	70
Appendix II	Acknowledgments	73
	Comptroller General's Advisory Council on Standards for Internal Control in the Federal Government (2013-2015)	73
	GAO Project Team	74
	Staff Acknowledgments	74
Glossary		75

Figures

Figure 1: Green Book Sample Page	4
Figure 2: Achieving Objectives through Internal Control	5
Figure 3: The Five Components and 17 Principles of Internal Control	9
Figure 4: The Components, Objectives, and Organizational Structure of Internal Control	10

Figure 5: The 17 Principles Supporting the Five Components of Internal Control 11
Figure 6: Examples of Common Categories of Control Activities 46

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

Overview

Foreword

Policymakers and program managers are continually seeking ways to improve accountability in achieving an entity's mission. A key factor in improving accountability in achieving an entity's mission is to implement an effective internal control system. An effective internal control system helps an entity adapt to shifting environments, evolving demands, changing risks, and new priorities. As programs change and entities strive to improve operational processes and implement new technology, management continually evaluates 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 (FMFIA)) requires the Comptroller General to issue standards for internal control in the federal government. *Standards for Internal Control in the Federal Government* (known as the Green Book), provide the overall framework for establishing and maintaining an effective internal control system. Office of Management and Budget (OMB) Circular No. A-123 provides specific requirements for assessing and reporting on controls in the federal government. The term internal control in this document covers all aspects of an entity's objectives (operations, reporting, and compliance).

The Green Book may also be adopted by state, local, and quasi-governmental entities, as well as not-for-profit 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 Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated its internal control guidance in 2013 with the issuance of a revised *Internal Control - Integrated Framework*.[1] COSO introduced the concept of principles related to the five components of internal control. The Green Book adapts these principles for a government environment.

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

The standards are effective beginning with fiscal year 2016 and the FMFIA reports covering that year. Management, at its discretion, may elect early adoption of the Green Book.

This revision of the standards 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 about 20 experts in financial and performance management drawn from federal, state, and local government; the private sector; and academia. The views of all parties were thoroughly considered in finalizing the standards.

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 throughout the entire process of developing and finalizing the standards.



Gene L. Dodaro
Comptroller General
of the United States

September 2014

How to Use the Green Book

The Green Book provides managers criteria for designing, implementing, and operating an effective internal control system. The Green Book defines the standards through components and principles and explains why they are integral to an entity's internal control system. The Green Book clarifies what processes management considers part of internal control. 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:

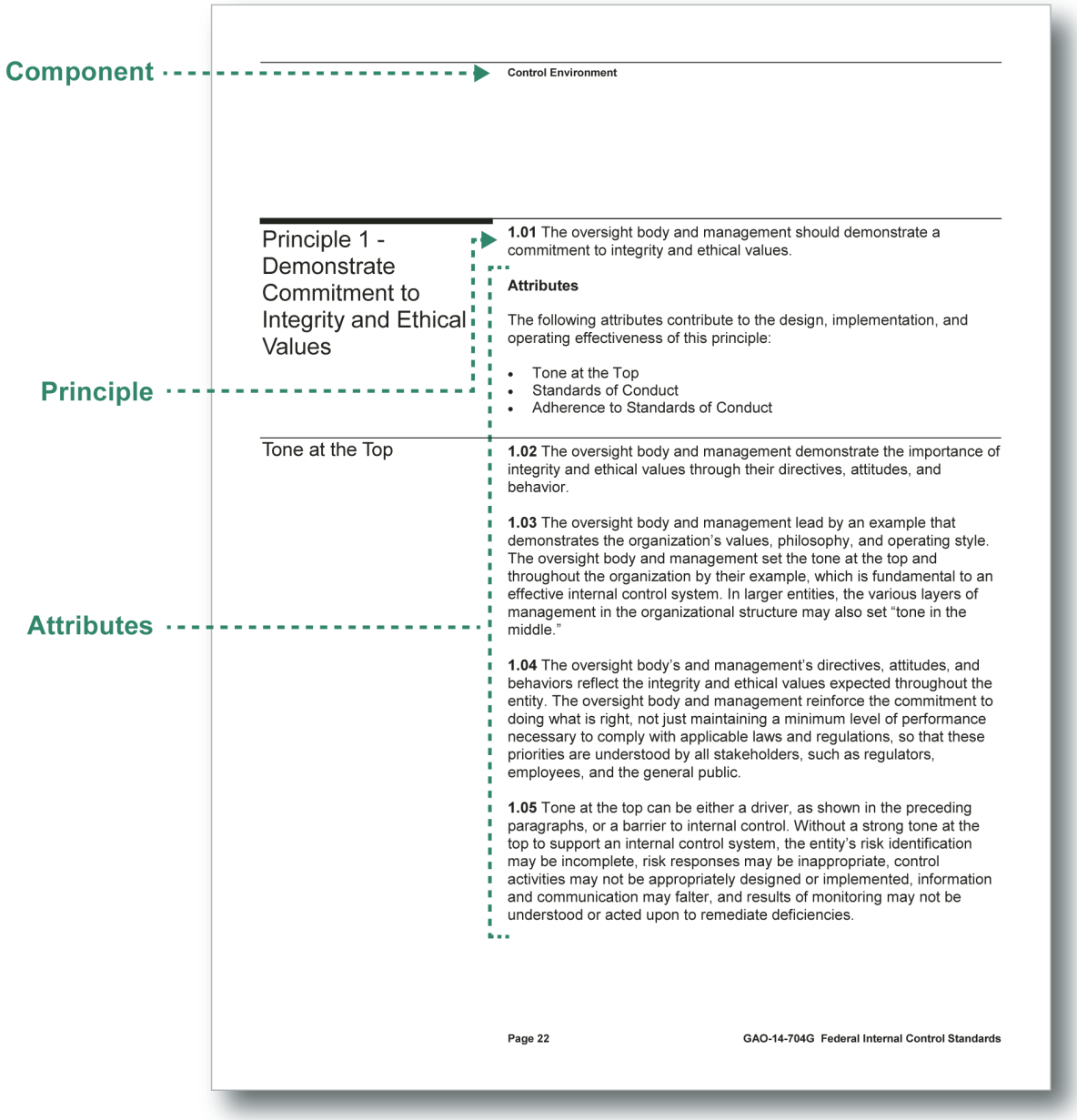
1. An Overview, which includes the following sections:
    - **Section 1:** an overview of the fundamental concepts of internal control
    - **Section 2:** a discussion of internal control components, principles, and attributes; how these relate to an entity's objectives; and the three categories of 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 the requirements for each of the five components and 17 principles as well as discussion of the related attributes, including documentation requirements.

The Green Book clearly indicates the component and principle requirements through the use of "must" and "should." Further discussion of these requirements is included in section 2 of the Overview. Documentation requirements are summarized in section 4 of the Overview.

Figure 1 depicts a sample page from the Green Book. This illustration identifies the components, principles, and attributes of the Green Book, which are further discussed in section 2 of the Overview.

Figure 1: Green Book Sample Page



Source: GAO. | GAO-14-704G

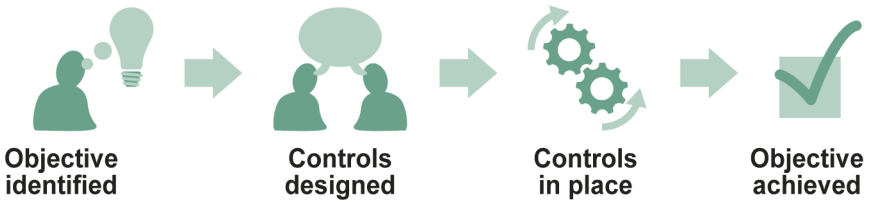
Section 1 - Fundamental Concepts of Internal Control

Definition of Internal Control

OV1.01 Internal control is a process effected by an entity's oversight body, management, and other personnel that provides 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-14-704G

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, and procedures 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. In short, internal control helps managers achieve desired results through effective stewardship of public resources.

Definition of an Internal Control System

OV1.04 An internal control system is a continuous built-in component of operations, effected by people, that provides reasonable assurance, not absolute assurance, that an entity's objectives will be achieved.

OV1.05 Internal control is not one event, but a series of actions that occur throughout an entity's operations. Internal control is recognized as an integral part of the operational processes management uses to guide its operations 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.

OV1.06 People are what make internal control work. Management 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, personnel throughout an entity play important roles in implementing and operating an effective internal control system.

OV1.07 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 all of an organization's objectives will be met. Factors outside the control or influence of management can affect the entity's ability to achieve all of its objectives. For example, a natural disaster can affect an organization's ability to achieve its objectives. Therefore, once in place, effective internal control provides reasonable, not absolute, assurance that an organization 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. 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 if an internal control system is 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 of an entity's objectives: operations, reporting, and compliance. However, these standards are not intended to limit or interfere with duly granted authority related to legislation, rulemaking, or other discretionary policy making in an organization. In implementing the Green Book, management is responsible for designing the policies and procedures to fit an entity's circumstances and building them 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 specific 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** - Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses.

[2]See para. OV4.10 for further discussion on use by other entities.

- **Control Activities** - The actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.
- **Information and Communication** - The quality information management and 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 address related risks. If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively. In addition to principle requirements, the Green Book contains documentation requirements.

OV2.07 The Green Book contains additional information in the form of attributes. These attributes are intended to help organize the application material management may consider when designing, implementing, and operating the associated principles. Attributes provide further explanation of the principle and documentation requirements and 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. Attributes may also provide background information on matters addressed in the Green Book.

OV2.08 Attributes are relevant to the proper implementation of the Green Book. Management has a responsibility to understand the attributes and exercise judgment in fulfilling the requirements of the standards. The Green Book, however, does not prescribe how management designs, implements, and operates an internal control system.

OV2.09 Figure 3 lists the five components of internal control and 17 related principles.

Figure 3: 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 the potential for fraud 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 achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies.

Information and Communication

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

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.

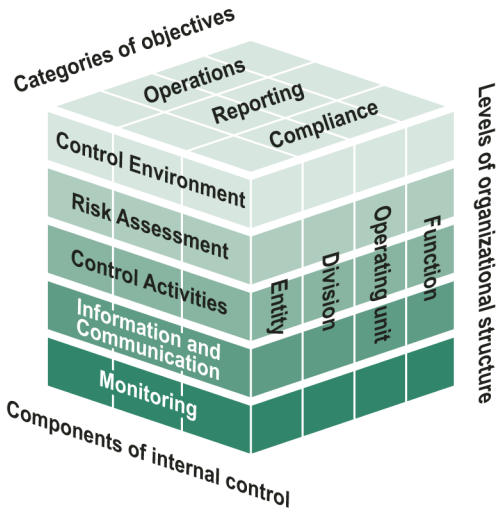
Source: GAO. | GAO-14-704G

Internal Control and the Entity

OV2.10 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. The five components of internal control are what are required of the entity to achieve the objectives. Organizational structure encompasses the operating units, operational processes, and other structures management

uses to achieve the objectives. This relationship is depicted in the form of a cube developed by COSO (see fig. 4).[3]

Figure 4: The Components, Objectives, and Organizational Structure of Internal Control



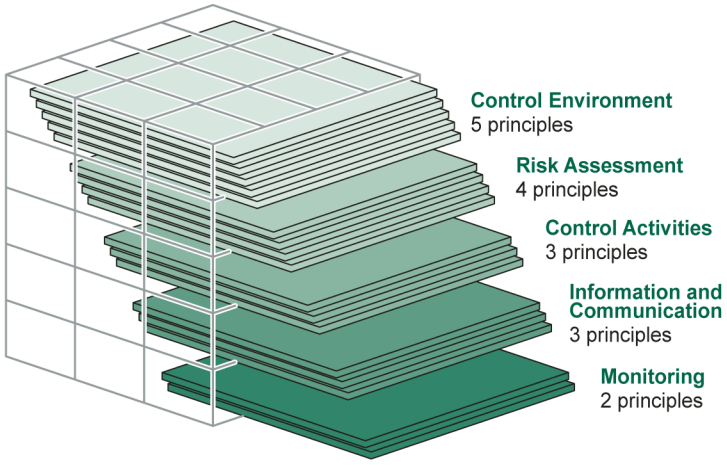
Sources: COSO and GAO. | GAO-14-704G

OV2.11 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.

OV2.12 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. 5).

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

Figure 5: The 17 Principles Supporting the Five Components of Internal Control



Source: GAO. | GAO-14-704G

OV2.13 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 factors such as mission, regulatory environment, strategic plan, entity size, risk tolerance, and information technology, and the judgment needed in responding to these differing factors.

Roles in an Internal Control System

OV2.14 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. For the purpose of the Green Book, oversight by an oversight body is implicit in each component and principle.

- **Management** - Management is directly responsible for all activities of an entity, including the design, implementation, and operating effectiveness of an entity's internal control system. Managers' responsibilities vary depending on their functions in the organizational structure.
- **Personnel** - Personnel help management design, implement, and operate an internal control system and are responsible for reporting issues noted in the entity's operations, reporting, or compliance objectives.[4]

OV2.15 External auditors and the office of the inspector general (OIG), if applicable, are not considered a part of an entity's internal control system. While management may evaluate and incorporate recommendations by external auditors and the OIG, responsibility for an entity's internal control system resides with management.

Objectives of an Entity

OV2.16 Management, with oversight by an oversight body, sets objectives to meet the entity's mission, strategic plan, and goals and requirements of applicable laws and regulations. Management sets objectives before designing an entity's internal control system. Management may include setting objectives as part of the strategic planning process.

OV2.17 Management, as part of designing an internal control system, defines the objectives in specific and measurable terms to enable management to identify, analyze, and respond to risks related to achieving those objectives.

Categories of Objectives

OV2.18 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

[4]See paras. 17.02 through 17.04 for further discussion on identifying issues.

Operations Objectives

OV2.19 Operations objectives relate to program operations that achieve an entity's mission. 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 from operational processes, while efficient operations do so in a manner that minimizes the waste of resources.

OV2.20 Management can set, 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 program operations in achieving the mission.

Reporting Objectives

OV2.21 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:

- **External financial reporting objectives** - Objectives related to the release of the entity's financial performance in accordance with professional standards, 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, 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 needed by management to support decision making and evaluation of the entity's performance.

Compliance Objectives

OV2.22 In the government sector, objectives related to compliance with applicable laws and regulations are very 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.

OV2.23 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 is able to exercise discretion relative to the performance of the entity.

Safeguarding of Assets

OV2.24 A subset of the three categories of objectives is the safeguarding of 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

OV2.25 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 to achieve these subobjectives. Both management and 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. For federal entities, OMB Circular No. A-123 provides specific requirements on how to perform evaluations and report on internal control in the federal government. Nonfederal entities 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 provides 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 if 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 the requirements of the act. 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 control are identified and the plans and schedule for correcting any such weakness are described. OMB issues guidance for evaluating these requirements in OMB Circular No. A-123. Nonfederal entities may refer to applicable laws and regulations for guidance in preparing statements regarding internal control.

Design and Implementation

OV3.05 When evaluating design of internal control, management determines if controls individually and in combination with other controls are capable of achieving an objective and addressing related risks. 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 meet 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 met. 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, and by whom or by what means they were applied. 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 by management's ongoing monitoring of the internal control system as well as any separate evaluations performed by both internal and external sources. A deficiency in internal control exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks.

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 level. Management evaluates the significance of a deficiency by considering the magnitude of impact, likelihood of occurrence, and nature of the deficiency. Magnitude of impact refers to 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 refers to the possibility of a deficiency impacting an entity's ability to achieve its objectives. The nature of the deficiency involves factors such as the degree of subjectivity involved with the deficiency and whether the deficiency arises from 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 as to whether the principle is designed, implemented, and operating effectively. Management considers the impact of deficiencies identified in achieving documentation requirements as part of this summary determination.[5] Management may consider the related attributes as part of this summary determination. If a principle is not designed, implemented, or operating effectively, then the respective component cannot be effective.

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 if the five components operate together effectively. If one or more of the five components are not effectively designed, implemented, or operating effectively 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

Service Organizations

OV4.01 Management may engage external parties to perform certain operational processes for the entity, such as accounting and payroll processing, security services, or health care claims processing. For the purpose of the Green Book, these external parties are referred to as service organizations. Management, however, retains responsibility for the performance of processes assigned to service organizations.

[5]See paras. OV4.08 through OV4.09 for further discussion of documentation requirements.

Therefore, management needs to understand the controls each service organization has designed, has implemented, and operates for the assigned operational process and how the service organization's internal control system impacts the entity's internal control system.

OV4.02 If controls performed by the service organization are necessary for the entity to achieve its objectives and address risks related to the assigned operational process, the entity's internal controls may include complementary user entity controls identified by the service organization or its auditors that are necessary to achieve the service organization's control objectives.

OV4.03 Management may consider the following when determining the extent of oversight for the operational processes assigned to the service organization:

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

Large versus Small Entities

OV4.04 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 operational processes and direct interaction with personnel. Smaller entities may find informal staff meetings effective for communicating quality information, whereas larger entities may need more formal mechanisms—such as written reports, intranet portals, or periodic formal meetings—to communicate with the organization.

OV4.05 A smaller entity, however, faces greater challenges in segregating duties because of its concentration of responsibilities and

authorities in the organizational structure.[6] Management, however, can respond to this increased risk through the design of the internal control system, such as by adding additional levels of review for key operational processes, reviewing randomly selected transactions and their supporting documentation, taking periodic asset counts, or checking supervisor reconciliations.

Benefits and Costs of Internal Control

OV4.06 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. The complexity of cost-benefit determination is compounded by the interrelationship of controls with operational processes. Where controls are integrated with operational processes, it is difficult to isolate either their costs or benefits.

OV4.07 Management may decide how an entity evaluates the costs versus benefits of various approaches to implementing an effective internal control system. However, cost alone is not an acceptable reason to avoid implementing internal controls. Management is responsible for meeting internal control objectives. The costs versus benefits considerations support management's ability to effectively design, implement, and operate an internal control system that balances the allocation of resources in relation to the areas of greatest risk, complexity, or other factors relevant to achieving the entity's objectives.

Documentation Requirements

OV4.08 Documentation is a necessary part of an effective internal control system. The level and nature of documentation vary based on the size of the entity and the complexity of the operational processes the entity performs. Management uses judgment in determining the extent of documentation that is needed. Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system. The Green Book includes minimum documentation requirements as follows:

[6]See paras. 10.12 through 10.14 for further discussion of segregation of duties.

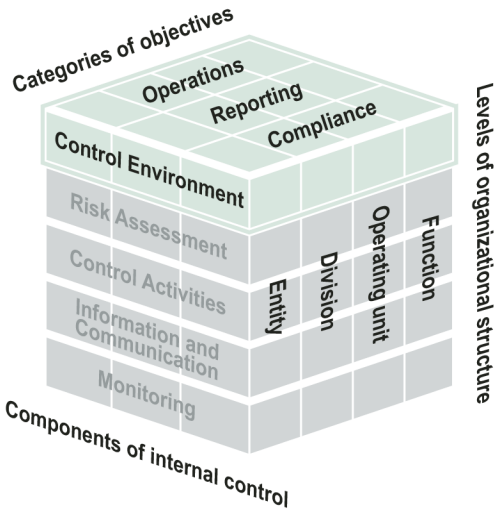
- If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively. (paragraph OV2.06)
- Management develops and maintains documentation of its internal control system. (paragraph 3.09)
- Management documents in policies the internal control responsibilities of the organization. (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 on a timely basis. (paragraph 17.05)
- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. (paragraph 17.06)

OV4.09 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 as to whether the related principle is designed, implemented, and operating effectively.

Use by Other Entities

OV4.10 The Green Book may be applied as a framework for an internal control system for state, local, and quasi-governmental entities, as well as not-for-profit organizations. If management elects to adopt the Green Book as criteria, management follows all relevant requirements presented in these standards.

Control Environment



Sources: COSO and GAO. | GAO-14-704G

Overview

The control environment is the foundation for an 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 "tone in the middle."

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, employees, and the general 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, employees, and the general public. The standards of conduct guide the directives, attitudes, and behaviors of the organization in achieving the entity's 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, or guidelines to communicate 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.[7] Individual personnel can also report issues through reporting lines, such as regular staff meetings, upward feedback processes, a whistle-blowing program, or an ethics hotline.[8] 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 the tolerance level for deviations. 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.

[7]See paras. 16.04 through 16.08 for further discussion of ongoing monitoring and separate evaluations.

[8]See para. 14.06 for further discussion of upward and separate reporting lines.

Management addresses deviations from expected standards of conduct timely and consistently. Depending on the severity of the deviation determined through the evaluation process, management, with oversight from the oversight body, takes appropriate actions and may also need to consider applicable laws and regulations. The standards of conduct to which management holds personnel, however, remain consistent.

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, 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 through the establishment of 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 the entity's integrity and ethical values.

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 needed by members 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 system of internal control)
- Programmatic expertise, including knowledge of the entity's mission, programs, and operational 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 systems and technology (e.g., understanding critical systems 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.[9]

[9]See GAO, *Government Auditing Standards: 2011 Revision*, GAO-12-331G (Washington, D.C.: December 2011), para. 3.03, for further discussion of independence.

Members of an oversight body scrutinize and question management's activities, present alternative views, and act when faced with obvious or suspected wrongdoing. Independent members with relevant expertise provide value through their 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, establish oversight structure, 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 the achievement of objectives, including the potential impact of significant changes, fraud, 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 management's evaluation and remediation of identified deficiencies.

2.10 These responsibilities are supported by the organizational structure that management establishes.[10] 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.

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

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, 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.[11]

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 discrete units to enable the organization to operate in

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

an efficient and effective manner, comply with applicable laws and regulations, and reliably report quality information.[12] Based on the nature of the assigned responsibility, management chooses the type and number of discrete units, such as divisions, offices, and related subunits.

3.04 As part of establishing an organizational structure, management considers how units interact in order to fulfill their overall responsibilities. Management establishes reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities.[13] 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.[14] Management also considers the entity's overall responsibilities to external stakeholders and establishes reporting lines that allow the entity to both communicate and receive information from external stakeholders.[15]

3.05 Management periodically evaluates the organizational structure so that it meets the entity's objectives and has adapted to any new objectives for the entity, such as a new law or regulation.

Assignment of Responsibility and Delegation of Authority

3.06 To achieve the entity's objectives, 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 to each unit, 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 retain ownership for fulfilling the overall responsibilities assigned to the unit.

[12]See paras. 13.05 through 13.06 for further discussion of quality information.

[13]See paras. 13.02 through 13.06 for further discussion of the use of quality information.

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

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

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 the delegation for proper segregation of duties within the unit and in 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.[16] As with assigning responsibility, those in key roles can 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.

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, as well as a means 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 cost benefit of documentation requirements 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.

[16]See paras. 10.12 through 10.14 for further discussion of segregation of duties.

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

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 qualification 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.[17]

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 individuals accountable to established policies by evaluating personnel's 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.

[17]See paras. 12.02 through 12.04 for further discussion of policies.

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 the 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 entity personnel accountable for performing their assigned internal control responsibilities. The oversight body, in turn, holds management accountable as well as the organization as a whole 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 the 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 the service organization to perform its internal control responsibilities.

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.[18]

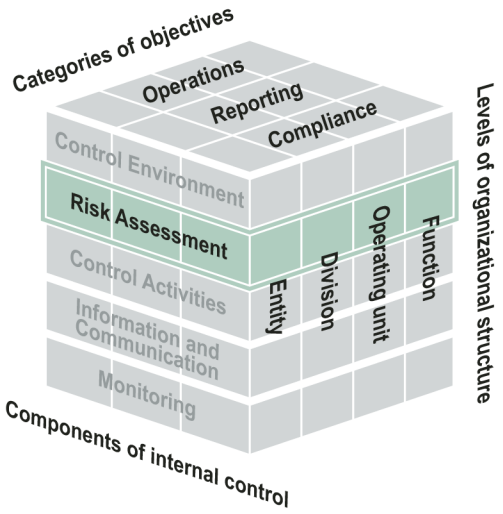
Consideration of Excessive Pressures

5.07 Management adjusts excessive pressures on personnel in the entity. Pressure can appear in an entity because of goals established by management to meet objectives or cyclical demands of various processes performed by the entity, 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.

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

Risk Assessment



Sources: COSO and GAO. | GAO-14-704G

Overview

Having established an effective control environment, management assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. Management assesses the risks the entity faces from both external and internal sources.

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 the potential for fraud 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 in specific and measurable terms to enable the design of internal control for related risks. 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 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 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,[19] oversight structure,[20] organizational structure,[21] and expectations of competence[22] as part of the control environment.

6.06 Management evaluates and, if necessary, revises defined objectives so that they are consistent with these requirements and 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 they are clearly stated and can be measured. Risk tolerance is often measured in the same terms as the performance measures for the defined objectives. Depending on the category of objectives, risk tolerances may be expressed as follows:

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

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

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

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

- **Operations objectives** - Level of variation in performance in relation to risk.
- **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 are made in light of 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** - Concept of risk tolerance does not apply. An entity is either compliant or not compliant.

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:

- Identification of Risks
- Analysis of Risks
- Response to Risks

Identification of Risks

7.02 Management identifies risks throughout the entity 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.

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. Management's lack of response to either risk could cause deficiencies in the internal control system.

7.04 Management considers all significant interactions within the entity and with external parties, changes within the entity's internal and external environment,[23] and other internal and external factors to identify risks throughout the entity. Internal risk factors may include the complex nature of an entity's programs, its organizational structure, or the use of new technology in operational processes. External risk factors may include new or amended laws, regulations, or professional standards; economic instability; or potential natural disasters. Management considers these factors at both the entity and transaction levels to comprehensively identify risks that affect defined objectives.[24] Risk identification methods may include qualitative and quantitative ranking activities, forecasting and strategic planning, and consideration of deficiencies identified through audits and other assessments.

Analysis of Risks

7.05 Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Significance refers to the effect on achieving a defined objective.

7.06 Management estimates the significance of the identified risks to assess their effect 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 deficiency that could result from the risk and 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 a risk 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

[23]See paras. 9.02 through 9.03 for further discussion of changes in the internal control system.

[24]See paras. 10.07 through 10.11 for further discussion of level of controls.

transactions. The oversight body may oversee management's estimates of significance so that risk tolerances have been properly defined.

7.07 Risks may be analyzed on an individual basis 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.

Response to Risks

7.08 Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective. Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance. These risk responses may include the following:

- **Acceptance** - No action is taken to respond to the risk based on the insignificance of the risk.
- **Avoidance** - Action is taken to stop the operational process or the part of the operational 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.

7.09 Based on the selected risk response, management designs the specific actions to respond to the analyzed risks. The nature and extent of risk response actions depend on the defined risk tolerance. Operating within the defined risk tolerance provides greater assurance that the entity will achieve its objectives. 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.

Principle 8 - Assess Fraud Risk

8.01 Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

Attributes

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

- Types of Fraud
- Fraud Risk Factors
- Response to Fraud Risks

Types of Fraud

8.02 Management considers the types of fraud that can occur within the entity to provide a basis for identifying fraud risks.[25] Types of fraud are as follows:

- **Fraudulent financial reporting** - Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. This could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles.
- **Misappropriation of assets** - Theft of an entity's assets. This could include theft of property, embezzlement of receipts, or fraudulent payments.
- **Corruption** - Bribery and other illegal acts.

8.03 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. This includes the misuse of authority or position for personal gain or for the benefit of another. Waste and abuse do not necessarily involve fraud or illegal acts.

[25]Fraud involves obtaining something of value through willful misrepresentation. Whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative system and is beyond management's professional responsibility for assessing risk.

However, they may be an indication of potential fraud or illegal acts and may still impact the achievement of defined objectives.

Fraud Risk Factors

8.04 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 include the following:

- **Incentive/pressure** - Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud.[26]
- **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 are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

8.05 Management uses the fraud risk factors to identify fraud risks. While fraud risk may be greatest when all three risk factors are present, one or more of these factors may indicate a fraud risk. Other information provided by internal and external parties can also be used to identify fraud risks. This may include allegations of fraud or suspected fraud reported by the office of the inspector general or internal auditors, personnel, or external parties that interact with the entity.

Response to Fraud Risks

8.06 Management analyzes and responds to identified fraud risks so that they are effectively mitigated. Fraud risks are analyzed through the same risk analysis process performed for all identified risks.[27] Management analyzes the identified fraud risks by estimating their significance, both individually and in the aggregate, to assess their effect on achieving the defined objectives. As part of analyzing fraud risk, management also assesses the risk of management override of controls.[28] The oversight

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

[27]See paras. 7.05 through 7.07 for further discussion of analyzing risks.

[28]See para. 10.13 for further discussion of management override.

body oversees management's assessments of fraud risk and the risk of management override of controls so that they are appropriate.

8.07 Management responds to fraud risks through the same risk response process performed for all analyzed risks.[29] Management designs an overall risk response and specific actions for responding to fraud risks. It may be possible to reduce or eliminate certain fraud risks by making changes to the entity's activities and processes. These changes may include stopping or reorganizing certain operations and reallocating roles among personnel to enhance segregation of duties. In addition to responding to fraud risks, management may need to develop further responses to address the risk of management override of controls. Further, when fraud has been detected, the risk assessment process may need to be revised.

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:

- Identification of Change
- Analysis of and Response to Change

Identification of Change

9.02 As part of risk assessment or a similar process, management identifies changes that could significantly impact the entity's internal control system. Identifying, analyzing, and responding to change is similar to, if not part of, the entity's regular risk assessment process. However, change is discussed separately because it is critical to an effective internal control system and can often be overlooked or inadequately addressed in the normal course of operations.

9.03 Conditions affecting the entity and its environment continually change. Management can anticipate and plan for significant changes by using a forward-looking process for identifying change. Management

[29]See paras. 7.08 through 7.09 for further discussion of responding to risks.

identifies, on a timely basis, significant changes to internal and external conditions that have already occurred or are expected to occur. Changes in internal conditions include changes to the entity's programs or activities, oversight structure, organizational structure, personnel, and technology. Changes in external conditions include changes in the governmental, economic, technological, legal, regulatory, and physical environments. Identified significant changes are communicated across the entity through established reporting lines to appropriate personnel.[30]

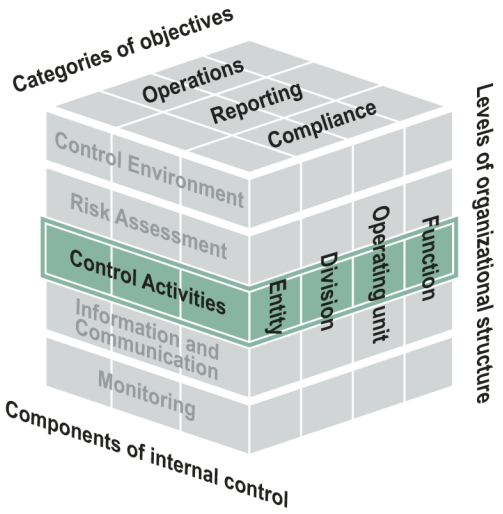
Analysis of and Response to Change

9.04 As part of risk assessment or a similar process, management analyzes and responds to identified changes and related risks in order to maintain an effective internal control system. 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. Management analyzes the effect of identified changes on the internal control system and responds by revising the internal control system on a timely basis, when necessary, to maintain its effectiveness.

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

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

Control Activities



Sources: COSO and GAO. | GAO-14-704G

Overview

Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system.

Principles

10. Management should design control activities to achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies.

Principle 10 - Design Control Activities

10.01 Management should design control activities to achieve objectives and respond to risks.

Attributes

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

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

Response to Objectives and Risks

10.02 Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies 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 to fulfill defined responsibilities and address identified risk responses.

Design of Appropriate Types of Control Activities

10.03 Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system. The common control activity categories listed in figure 6 are meant only to illustrate the range and variety of control activities that may be useful to management. The list is not all inclusive and may not include particular control activities that an entity may need.

Figure 6: Examples of Common Categories of Control Activities

- Top-level reviews of actual performance
- Reviews by management at the functional or activity level
- Management of human capital
- Controls over information processing
- Physical control over vulnerable assets
- Establishment and review of performance measures and indicators
- Segregation of duties
- Proper execution of transactions
- Accurate and timely recording of transactions
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control

Source: GAO. | GAO-14-704G

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.

Management of human capital

Effective management of an entity's workforce, its human capital, is essential to achieving results and an important part of internal control. Only when the right personnel for the job are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management continually assesses the knowledge, skills, and ability needs of the entity so that the entity is able to obtain a workforce that has the required knowledge, skills, and abilities to achieve organizational goals. 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 internal control 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.

Controls over information processing

A variety of control activities are used in information processing. Examples include edit checks of data entered; accounting for transactions in numerical sequences; comparing file totals with control accounts; and controlling access to data, files, and programs.[31]

Physical control over vulnerable assets

Management establishes physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment that might be vulnerable to risk of loss or unauthorized use. Management periodically counts and compares such assets to control records.

Establishment and review of performance measures and indicators

Management establishes activities to monitor performance measures and indicators. These may include comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Management designs controls aimed at validating the propriety and integrity of both entity and individual performance measures and indicators.

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.

[31]See paras. 11.02 through 11.17 for further discussion of controls over information processing.

Proper execution of transactions

Transactions are authorized and executed only by persons acting within the scope of their authority. 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.

Accurate and timely recording of transactions

Transactions are promptly recorded to maintain their 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. In addition, management designs control activities so that all transactions are completely and accurately recorded.

Access restrictions to and accountability for resources and records

Management limits access to resources and records to authorized individuals, and assigns and maintains accountability for their custody and use. Management may periodically compare resources with the recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Appropriate documentation of transactions and internal control

Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

An entity's internal control is flexible to allow management to tailor control activities to meet the entity's special needs. The specific control activities used by a given entity may be different from those used by others based on a number of factors. These factors could include specific threats the entity faces and risks it incurs; differences in objectives; managerial judgment; size and complexity of the entity; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

10.04 Control activities can be either preventive or detective. The main difference between preventive and detective control activities is the timing of a control activity within an entity's operations. A preventive control activity prevents an entity from failing to achieve an objective or address a risk. A detective control activity discovers when an entity is not achieving an objective or addressing a risk before the entity's operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk.

10.05 Management evaluates the purpose of the control activity as well as the effect a deficiency would have on the entity in achieving its objectives. If the control activity is for a significant purpose or the impact of a deficiency would be significant to achieving the entity's objectives, management may design both preventive and detective control activities.

10.06 Control activities can be implemented in either an automated or a manual manner. Automated control activities are either wholly or partially automated through the entity's information technology. Manual control activities are performed by individuals with minor use of 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.[32] If the entity relies on information technology in its operations, management designs control activities so that the information technology continues to operate properly.

Design of Control Activities at Various Levels

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

10.08 Management designs control activities for appropriate coverage of objectives and risks in the operations. Operational processes transform inputs into outputs to achieve the organization's objectives. Management designs entity-level control activities, transaction control activities, or both depending on the level of precision needed so that the entity meets its objectives and addresses related risks.

[32]See paras. 11.06 through 11.08 for further discussion of information system control activities.

10.09 Entity-level controls are controls that have a pervasive effect on an entity's internal control system and may pertain to multiple components. Entity-level controls may include controls related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring.

10.10 Transaction control activities are actions built directly into operational processes to support the entity in achieving its objectives and addressing related risks. "Transactions" tends to be associated with financial processes (e.g., payables transactions), while "activities" is more generally applied to operational or compliance processes. For the purposes of this standard, "transactions" covers both definitions. Management may design a variety of transaction control activities for operational processes, which may include verifications, reconciliations, authorizations and approvals, physical control activities, and supervisory control activities.

10.11 When choosing between entity-level and transaction control activities, management evaluates the level of precision needed for the operational processes to meet the entity's objectives and address related risks. In determining the necessary level of precision for a control activity, management evaluates the following:

- **Purpose of the control activity** - A control activity that functions to prevent or detect generally is more precise than a control activity that merely identifies and explains differences.
- **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 of performance** - A control activity that is performed routinely and consistently generally is more precise than one performed sporadically.
- **Correlation to relevant operational processes** - A control activity that is directly related to an operational process generally is more likely to prevent or detect than a control activity that is only indirectly related.

Segregation of Duties

10.12 Management considers segregation of duties in designing control activity responsibilities so that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk.

10.13 Segregation of duties helps prevent fraud, waste, and abuse in the internal control system.[33] Management considers the need to separate control activities related to authority, custody, and accounting of operations to achieve adequate segregation of duties. In particular, segregation of duties can address the risk of management override. Management override circumvents existing control activities and increases fraud risk. Management addresses 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.

10.14 If segregation of duties is not practical within an operational process because of limited personnel or other factors, management designs alternative control activities to address the risk of fraud, waste, or abuse in the operational process.

Principle 11 - Design Activities for the Information System

11.01 Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

Attributes

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

- Design of the Entity's Information System
- Design of Appropriate Types of Control Activities
- Design of Information Technology Infrastructure
- Design of Security Management
- Design of Information Technology Acquisition, Development, and Maintenance

Design of the Entity's Information System

11.02 Management designs the entity's information system to respond to the entity's objectives and risks.

11.03 Management designs the entity's information system to obtain and process information to meet each operational process's information requirements and to respond to the entity's objectives and risks. An information system is the people, processes, data, and technology that

[33]See paras. 8.02 through 8.03 for further discussion of fraud, waste, and abuse.

management organizes to obtain, communicate, or dispose of information. An information system represents the life cycle of information used for the entity's operational processes that enables the entity to obtain, store, and process quality information.[34] An information system includes both manual and technology-enabled information processes. Technology-enabled information processes are commonly referred to as information technology. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies 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 to fulfill defined responsibilities and address the identified risk responses for the entity's information system.

11.04 Management designs the entity's information system and the use of information technology by considering the defined information requirements for each of the entity's operational processes.[35] Information technology enables information related to operational processes to become available to the entity on a timelier basis. Additionally, information technology may enhance internal control over security and confidentiality of information by appropriately restricting access. 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 Management also evaluates information processing objectives to meet the defined information requirements. Information processing objectives may include the following:

- **Completeness** - Transactions that occur are recorded and not understated.
- **Accuracy** - Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing.

[34]See paras. 13.02 through 13.06 for further discussion of the use of quality information.

[35]See paras. 13.02 through 13.04 for further discussion of defined information requirements.

- **Validity** - Recorded transactions represent economic events that actually occurred and were executed according to prescribed procedures.

Design of Appropriate Types of Control Activities

11.06 Management designs appropriate types of control activities in the entity's information system for coverage of information processing objectives for operational processes. For information systems, there are two main types of control activities: general and application control activities.

11.07 Information system general controls (at the entity-wide, system, and application levels) are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls facilitate the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

11.08 Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to achieve validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interface, and data management system controls.

Design of Information Technology Infrastructure

11.09 Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Information technology requires an infrastructure in which to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be shared by different units within the entity or outsourced either to service organizations or to location-independent technology services. Management evaluates the objectives of the entity and related risks in designing control activities for the information technology infrastructure.

11.10 Management continues to evaluate changes in the use of information technology and designs new control activities when these changes are incorporated into the entity's information technology

infrastructure. Management also designs control activities needed to maintain the information technology infrastructure. Maintaining technology 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.

Design of Security Management

11.11 Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

11.12 Security management includes the information processes and control activities related to access rights in an entity's information technology, including who has the ability to execute transactions. Security management includes access rights across various levels of data, operating system (system software), network, application, and physical layers. Management designs control activities over access to protect an entity from inappropriate access and unauthorized use of the system. These control activities support appropriate segregation of duties. By preventing unauthorized use of and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism) or error.

11.13 Management evaluates security threats to information technology, which can be from both internal and external sources. External threats are particularly important for entities that depend on telecommunications networks and the Internet. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks. Internal threats may come from former or disgruntled employees. They pose unique risks because they 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 security management systems and processes.

11.14 Management designs control activities to limit user access to information technology through authorization control activities such as providing a unique user identification or token to authorized users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other control activities to promptly update access rights when employees change job functions or leave the entity. Management also designs control activities for access rights when different information technology elements are connected to each other.

Design of Information Technology Acquisition, Development, and Maintenance

11.15 Management designs control activities over the acquisition, development, and maintenance of information technology. Management may use a systems development life cycle (SDLC) framework in designing control activities. An SDLC provides a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the acquisition, development, and maintenance of technology. Through an SDLC, management designs control activities over changes to technology. 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, development of information technology and changes to the information technology may be included in one SDLC or two separate methodologies. Management evaluates the objectives and risks of the new technology in designing control activities over its SDLC.

11.16 Management may acquire information technology through packaged software from vendors. Management incorporates methodologies for the acquisition of vendor packages into its information technology development and designs control activities over their selection, ongoing development, and maintenance. Control activities for the development, maintenance, and change of application software prevent unauthorized programs or modifications to existing programs.

11.17 Another alternative is outsourcing the development of information technology to service organizations. As for an SDLC developed internally, management designs control activities to meet objectives and address related risks. Management also evaluates the unique risks that using a service organization presents for the completeness, accuracy, and validity of information submitted to and received from the service organization.

Principle 12 - Implement Control Activities

12.01 Management should implement control activities through policies.

Attributes

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

- Documentation of Responsibilities through Policies
- Periodic Review of Control Activities

Documentation of Responsibilities through Policies

12.02 Management documents in policies the internal control responsibilities of the organization.

12.03 Management documents in policies for each unit its responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness.[36] Each unit, with guidance from management, determines the policies necessary to operate the process based on the objectives and related risks for the operational process. Each unit also documents policies in the appropriate level of detail to allow management to effectively monitor the control activity.

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 operational 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.[37] Management communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities.

Periodic Review of Control Activities

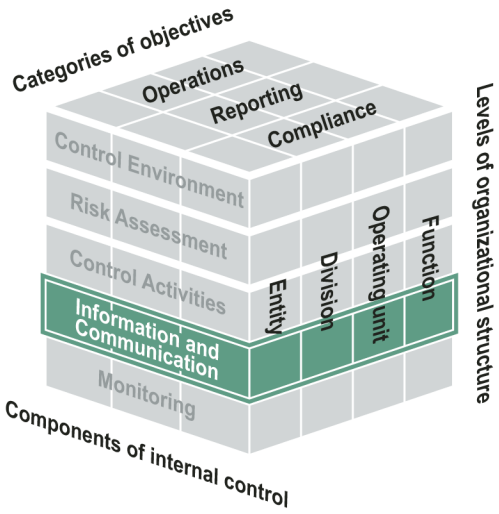
12.05 Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a

[36]See paras. 3.02 through 3.05 for further discussion of units.

[37]See para. 17.06 for further discussion of corrective actions.

timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology. Regulators; legislators; and in the federal environment, the Office of Management and Budget and the Department of the Treasury may also change either an entity's objectives or how an entity is to achieve an objective. Management considers these changes in its periodic review.

Information and Communication



Sources: COSO and GAO. | GAO-14-704G

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.

Principles

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

Principle 13 - Use Quality Information

13.01 Management should use quality information to achieve the entity's objectives.

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 achieve the objectives and address the risks. Information requirements consider the expectations 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 an effective internal control system. 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.

Relevant Data from Reliable Sources

13.04 Management obtains 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. Sources of data can be operational, financial, 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 the obtained data into quality information that supports the internal control system. This involves processing data into information and then evaluating the processed information so that 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, and provided on a timely basis. Management considers these characteristics as well as the information processing objectives in evaluating processed information and makes revisions when necessary so that the information is quality information.[38] Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.

13.06 Management processes relevant data from reliable sources into quality information within the entity's information system. An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information.[39]

Principle 14 - Communicate Internally

14.01 Management should internally communicate the necessary quality information to achieve the entity's objectives.

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 quality information throughout the entity using established reporting lines. Quality information is communicated down, across, up, and around reporting lines to all levels of the entity.

14.03 Management communicates quality information down and across reporting lines to enable personnel to 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.

[38]See paras. 11.02 through 11.05 for further discussion of information processing objectives.

[39]See paras. 11.02 through 11.05 for further discussion of information systems.

14.04 Management receives quality information about the entity's operational processes that flows up the reporting lines from personnel to help management achieve the entity's objectives.

14.05 The oversight body receives quality information that flows up the reporting lines from management and 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 to communicate 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, such as a written document—in hard copy or electronic format—or a face-to-face meeting. Management periodically evaluates the entity's methods of communication 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 externally communicate the necessary quality information to achieve the entity's objectives.

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 quality information from, external parties using established reporting lines. Open two-way external reporting lines allow for this communication. External parties include suppliers, contractors, service organizations, regulators, external auditors, government entities, and the general public.

15.03 Management communicates quality information externally through reporting lines so that external parties can help the entity achieve its objectives and address related risks. Management includes in these communications information relating to the entity's events and activities that impact the internal control system.

15.04 Management receives 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. This communication is necessary for the effective operation of internal control. Management evaluates external information received against the characteristics of quality information and information processing objectives and takes any necessary actions so that the information is quality information.[40]

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

[40]See paras. 11.02 through 11.05 for further discussion of information processing objectives.

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

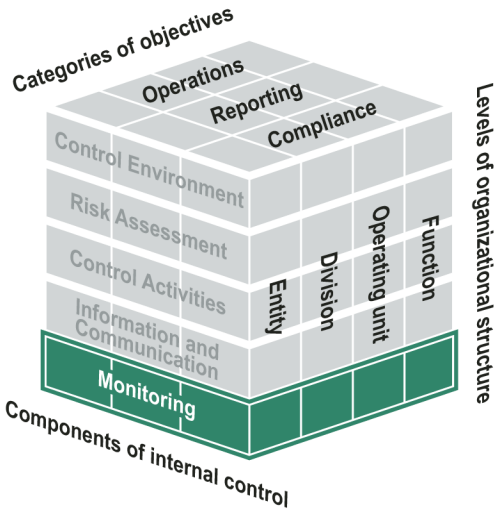
15.07 Management selects appropriate methods to communicate externally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider follow:

- **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, such as a written document—in hard copy or electronic format—or a face-to-face meeting. Management periodically evaluates the entity's methods of communication so 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 general public as well. In the federal government, entities not only report to the President and Congress but also to the general public. Entities consider appropriate methods when communicating with such a broad audience.

Monitoring



Sources: COSO and GAO. | GAO-14-704G

Overview

Finally, 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, environment, laws, resources, and risks. 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 control activities in order to achieve 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 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 of the design of the internal control system and 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. Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change. Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring.

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, and other routine actions. Ongoing monitoring may include automated tools,

which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions.

16.06 Management uses separate evaluations to monitor the design and operating effectiveness of the 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, effectiveness of ongoing monitoring, and rate of change within the entity and its environment. Separate evaluations may take the form of self-assessments, which include cross operating unit or cross functional evaluations.

16.07 Separate evaluations also include audits and other evaluations that may involve the review of control design and direct testing of internal control. These audits and other evaluations may be mandated by law and are performed by internal auditors, external auditors, the inspectors general, and other external reviewers. Separate evaluations provide greater objectivity when performed by reviewers who do not have responsibility for the activities being evaluated.

16.08 Management retains responsibility for monitoring the effectiveness of internal control over the assigned processes performed by service organizations. Management uses ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of the service organization's internal controls over the assigned process.[41] 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. 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.

[41]See paras. OV4.01 through OV4.03 for further discussion of service organizations.

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 general public and regulator comments may indicate areas in the internal control system that need improvement. Management considers whether current controls address the identified issues and modifies controls if necessary.

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.[42]

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. Such issues may include

- issues that cut across the organizational structure or extend outside the entity to service organizations, contractors, or suppliers and

[42]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.

- issues that may not be remediated because of the interests of management, such as sensitive information regarding fraud or other illegal acts.[43]

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 bodies that establish laws, rules, regulations, and 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 on a timely basis. Management evaluates issues identified through monitoring activities or reported by personnel to determine whether any of the issues rise to the level of an internal control deficiency. Internal control deficiencies require further evaluation and remediation by management. An internal control deficiency can be in the design, implementation, or operating effectiveness of the internal control and its related process.[44] Management determines from the type of internal control deficiency the appropriate corrective actions to remediate the internal control deficiency on a timely basis. Management assigns responsibility and delegates authority to remediate the internal control deficiency.

Corrective Actions

17.06 Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. These corrective actions include resolution of audit findings. 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. The audit resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies,

[43]See paras. 8.02 through 8.03 for further discussion of fraud.

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

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)

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 principle requirements of 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 the potential for fraud 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 achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies.

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

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 is a necessary part of an effective internal control system. The level and nature of documentation vary based on the size of the entity and the complexity of the operational processes the entity performs. Management uses judgment in determining the extent of documentation that is needed. Documentation is required to demonstrate the design, implementation, and operating effectiveness of an entity's internal control system. The Green Book includes minimum documentation requirements as follows:

- If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively. (paragraph OV2.06)
- Management develops and maintains documentation of its internal control system. (paragraph 3.09)
- Management documents in policies the internal control responsibilities of the organization. (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 on a timely basis. (paragraph 17.05)

- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. (paragraph 17.06)

Appendix II: Acknowledgments

Comptroller General's Advisory Council on Standards for Internal Control in the Federal Government (2013-2015)

The Honorable Jon Rymer, Chair
U.S. Department of Defense, Office of the Inspector General

Dr. Brett Baker
National Science Foundation, Office of the Inspector General

Lisa Casias
U.S. Department of Commerce

Carole Clay
U.S. Department of State

Melinda DeCorte
Crowe Horwath LLP

Stephen M. Eells
New Jersey Office of Legislative Services, Office of the State Auditor

Dr. Carol M. Eyermann
National Science Foundation

Bill Hughes
MorganFranklin Consulting LLC

Scot Janssen
KPMG LLP

John Kaschak
Pennsylvania Office of the Budget, Bureau of Audits

David L. Landsittel
Committee of Sponsoring Organizations of the Treadway Commission

The Honorable Samuel T. Mok
Condor International Advisors, LLC

Kenneth J. Mory
City of Austin, Texas

Dan Murrin
Ernst & Young

Dr. Annette K. Pridgen
Jackson State University

Dr. Sandra B. Richtermeyer
Xavier University

Neil Ryder
U.S. Department of Justice

Peggy Sherry
U.S. Department of the Treasury, Internal Revenue Service

F. Michael Taylor
Hanover County Government, Virginia

David A. Von Moll
Commonwealth of Virginia Office of the State Comptroller

David M. Zavada
Kearney & Company

GAO Project Team

Steven J. Sebastian, Managing Director
James R. Dalkin, Director
Robert F. Dacey, Chief Accountant
Jacquelyn N. Hamilton, Deputy Assistant General Counsel
Kristen A. Kociolek, Assistant Director
Grant L. Simmons, Senior Auditor
Christie A. Pugnetti, Senior Auditor

Staff Acknowledgments

In addition to the project team named above, also contributing were Francine M. DelVecchio, Lee Evans, Marci L. Goasdone, Peter B. Grinnell, Brian S. Harechmak, Debra L. Hoffman, Heather I. Keister, Jason M. Kelly, Judy Lee, William S. Lowrey, Alan S. MacMullin, Mary Arnold Mohiyuddin, Mary O. Osorno, Doris G. Yanger, 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 controls - Controls that are incorporated directly into computer applications for the purposes of validity, completeness, accuracy, and confidentiality of transactions and data during application processing; application controls include controls over input, processing, output, master file, interface, and data management system controls (paragraph 11.08)

Attributes - Additional information that provides further explanation of the principles and documentation requirements for effective internal control (paragraph OV2.07)

Baseline - The difference between the criteria of the design of the internal control system and condition of the internal control system at a specific point in time (paragraph 16.02)

Competence - The qualification to carry out assigned responsibilities (paragraph 4.02)

Complementary user entity controls - Controls that management of the service organization assumes, in the design of its service, will be implemented by user entities, and if necessary to achieve the control objectives stated in management's description of the service organization's system, are identified as such in that description (paragraph OV4.02)

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)

Contingency plans - The processes defined to address an entity's need to respond to sudden personnel changes that could compromise the internal control system (paragraph 4.06)

Control activities - The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks (paragraph 10.02)

Control objective - The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's objectives (paragraph OV3.05)

Deficiency - When the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks (paragraph OV3.07)

Detective control - An activity that is designed to discover when an entity is not achieving an objective or addressing a risk before the entity's operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk (paragraph 10.04)

Entity-level control - Controls that have a pervasive effect on an entity's internal control system; entity-level controls may include controls related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring (paragraph 10.09)

Fraud - Involves obtaining something of value through willful misrepresentation (paragraph 8.02)

General controls - The policies and procedures that apply to all or a large segment of an entity's information systems; general controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning (paragraph 11.07)

Green Book - The commonly used name for *Standards for Internal Control in the Federal Government* (Overview: Foreword)

Information system - The people, processes, data, and technology management organizes to obtain, communicate, or dispose of information (paragraph 11.03)

Information technology - Technology-enabled information processes (paragraph 11.03)

Inherent risk - The risk to an entity prior to considering management's response to the risk (paragraph 7.03)

Internal control - A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved (paragraph OV1.01)

Internal control system - A continuous built-in component of operations, effected by people, that provides reasonable assurance—not absolute assurance—that an entity's objectives will be achieved (paragraph OV1.04)

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 a risk will occur (paragraph 7.06)

Magnitude of impact - Severity of deficiency that could result from a risk and is affected by factors such as the size, pace, and duration of the risk's impact (paragraph 7.06)

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 OV2.14)

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 operating units, operational processes, and other structures management uses to achieve objectives (paragraph OV2.10)

Oversight body - Those responsible for overseeing management's design, implementation, and operation of an internal control system (paragraph OV2.14)

Performance measure - A means of evaluating the entity's performance in achieving objectives (paragraph 6.07)

Policies - Statements of responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness (paragraph 12.03)

Preventive control - An activity that is designed to prevent an entity from failing to achieve an objective or addressing a risk (paragraph 10.04)

Principle - Fundamental concept that is integral to the design, implementation, and operating effectiveness of the associated component (paragraph OV2.05)

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 from relevant and reliable data that is appropriate, current, complete, accurate, accessible, and provided on a timely basis, and meets identified information requirements (paragraph 13.05)

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 OV1.04)

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 - The information processes and control activities related to access rights in an entity's information technology (paragraph 11.12)

Segregation of duties - The separation of the authority, custody, and accounting of an operation (paragraph 10.13)

Service organization - An external party that performs operational process(es) for an entity (paragraph OV4.01)

Should - Denotes a principle requirement management must comply with except in rare circumstances where the requirement is not relevant for the entity (paragraph OV2.09)

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

Transaction - An event that may occur in operational, compliance, or financial processes (paragraph 10.10)

Transaction control activities - Actions built directly into operational processes to support the entity in achieving its objectives and addressing related risks (paragraph 10.10)

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 GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order Printed Copies	The printed version of the 2014 *Standards for Internal Control in the Federal Government* can be ordered through the Government Printing 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 Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper.