

Introduction to the COSO Framework

Christopher Goeman, CPA, CGFM



What is COSO?

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.



Thought Leaders In Accounting



American Institute of Certified Public Accountants



financial executives international

ima

The Association of Accountants and Financial Professionals in Business



The Institute of Internal Auditors

Why COSO?

- COSO is the most widely used internal control framework.
- The Green Book (Standards for Internal Control in the Federal Government) is built on COSO.
- Part 6 (Internal Control) of the Compliance Supplement and 2 CFR 200.303 indicates that internal controls should be in compliance with the Green Book or COSO.

3

What is internal control?

- Provides reasonable assurance that control objectives are met.



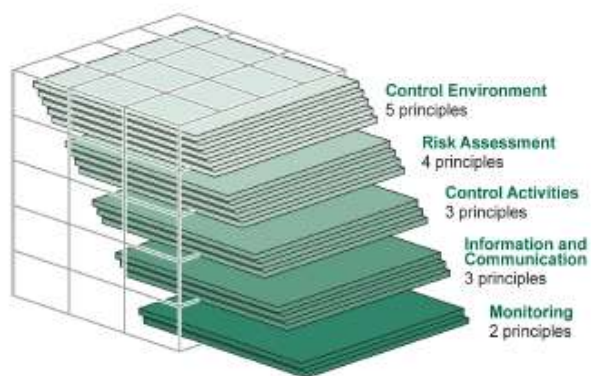
Source: GAO. | GAO-14-704G

4

COSO – Internal Control Framework



COSO – Internal Control Framework



Source: GAO. | GAO-14-704G

COSO Framework Definitions

- **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
- **Principle** - Fundamental concept that is integral to the design, implementation, and operating effectiveness of the associated component
- **Attributes** - Additional information that provides further explanation of the principles and documentation requirements for effective internal control

7

Summary of Green Book and COSO Components and Principles of Internal Control

Components of Internal Control	Principles
Control Environment	<ol style="list-style-type: none"> 1. Demonstrate Commitment to Integrity and Ethical Values 2. Exercise Oversight Responsibility 3. Establish Structure, Responsibility, and Authority 4. Demonstrate Commitment to Competence 5. Enforce Accountability
Risk Assessment	<ol style="list-style-type: none"> 6. Define Objectives and Risk Tolerances 7. Identify, Analyze, and Respond to Risks 8. Assess Fraud Risk 9. Identify, Analyze, and Respond to Change
Control Activities	<ol style="list-style-type: none"> 10. Design Control Activities 11. Design Activities for the Information System 12. Implement Control Activities
Information and Communication	<ol style="list-style-type: none"> 13. Use Quality Information 14. Communicate Internally 15. Communicate Externally
Monitoring	<ol style="list-style-type: none"> 16. Perform Monitoring Activities 17. Evaluate Issues and Remediate Deficiencies

8

Internal Control Definitions

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

9

Internal Control Definitions

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

10

Internal Control Definitions

- **Preventive control** - An activity that is designed to prevent an entity from failing to achieve an objective or addressing a risk
- **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
- **Segregation of duties** - The separation of the authority, custody, and accounting of an operation

11

Internal Control Definitions

- **Risk** - The possibility that an event will occur and adversely affect the achievement of objectives
- **Inherent risk** - The risk to an entity prior to considering management's response to the risk
- **Residual risk** - The risk that remains after management's response to inherent risk
- **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

12

Who Is Responsible for Internal Controls?

- Governing Board/Council
- Management
- Personnel

- Not auditors or oversight agencies

13

Which of the following is not a component of internal control?

- A. Control Environment
- B. Control Activities
- C. Monitoring
- D. Control Reconciliation

Where Does Management Start?

- Defining Objectives (Specific and Measureable)
 - Operating
 - Financial
 - Compliance

Who can provide examples of a financial reporting objective, operating objective, and compliance objective applicable to a governmental organization?

15

Operating Objective

- Achieving an entity's mission
 - i.e. providing an excellent education
 - i.e. providing safe and reliable water and wastewater service to customers
- Effective and efficient operations (avoiding waste)
- Safeguarding assets
 - Prevention, detection and correction

16

Reporting Objective

- External Reporting
 - Financial and non-financial – ACFR, single audit, adopted budget, water quality, crime statistics, continuing disclosures
- Internal Reporting
 - Financial and non-financial – Monitoring of budgets, student attendance, student performance, interim financial statements

17

Compliance Objective

- Conducts activities in accordance with laws and regulations
 - CFR, Statute, OMB, SEC, TEA

18

What makes a good Internal Control?

- The control is designed properly
 - Addresses a relevant control objective
 - Is effective in providing reasonable assurance
- The control is effectively implemented
 - Individuals have the competence and authority to implement the control.
- The costs of the control don't outweigh the benefits

19

What is internal control?

- A. Prevents all fraud
- B. Provides reasonable assurance that an objective is met.
- C. Serves to ensure compliance rather than financial reporting requirements.
- D. Provides absolute assurance that management's assertions are reliable.

Resources

- COSO Website
www.coso.org
- Green Book
<https://www.gao.gov/products/gao-14-704G>
- Part 6 of the Compliance Supplement
<https://www.whitehouse.gov/wp-content/uploads/2023/05/Part-6-Internal-Control.pdf>



21

Questions?

Christopher Goeman, CPA, CGFM
Email: christopher.goeman@hm.cpa
Cell: (928) 607-3354

