COSO Fraud Risk Management Guide

NSAC TFACC 2017
August 7, 2017
Salt Lake City, UT
Instructors

- Phil Miller
- NSAC Asst. Education Director
- pwm01@comcast.net

- Bill Erlenbush
- NSAC Education Director
- nsacdired@gmail.com
Discussion Topics

- COSO History
- COSO Integrated Framework
- COSO Fraud Risk Management Guide
- Fraud Risk Management Principles 1-5
- Users of the Guide
- Resource Information
COSO Mission

- Develop comprehensive guidance on:
  - Enterprise risk management
  - Internal Control
  - Fraud Deterrence
  - Improving Organizational Performance
  - Improving Governance
  - Reducing the Extent of Fraud
COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
The National Commission was sponsored jointly by five major professional association headquartered in the United States:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives Institute (FEI)
- Institute of Internal Auditors (IIA)
- National Association of Accountants – now the Institute of Management Accountants (IMA)
The first chairman of the National Commission was James C. Treadway, Jr., Executive Vice President and General Counsel, Paine Webber Incorporated and a former Commissioner of the U.S. Securities and Exchange Commission. Hence, the popular name "Treadway Commission." Currently, the COSO Chairman is Robert Hirth.
COSO History

- Operating Policies:

- COSO is a committee of five sponsoring organizations whose representatives come together periodically to work on specific projects. COSO’s projects are undertaken, reviewed and finalized in accordance with policies agreed to by the sponsoring organizations.
COSO History

- Key COSO Publications:
  - 1996 – Internal Control Issues in Derivatives Usage
  - 2006 – Internal Control over Financial Reporting
    - Guidance for Smaller Public Companies
  - 2009 – Guidance on Monitoring Internal Control Systems
  - 2013 – Framework revised and reissued
  - 2016 – Fraud Risk Management Guide

NSAC
National Society of Accountants for Cooperatives
First Published in 1992

Gained wide acceptance with financial control failures in the early 2000’s

Recognized for designing, implementing, and conducting internal control
Revised Framework

- Published in 2013

- Added 17 additional principles to add clarity in designing, implementing, and understanding requirements for an effective internal control system

- These 17 principles align with the 5 internal control components in the original
COSO 17 Principles – The Control Environment

1. A commitment to integrity and ethical values
2. Board independence from management
3. Management structures, reporting lines, and appropriate authorities and responsibilities
4. A commitment to hire competent employees
5. Individuals held accountable for internal control responsibilities.
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks.

7. The organization identifies risks and analyzes risks as a basis for determining how risks should be managed.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.
COSO 17 Principles – Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
This publication, *Fraud Risk Management Guide* (Guide) is intended to be supportive of and consistent with the 2013 Framework and can serve as best practices guidance for organizations to follow.

This guide is designed to be familiar to COSO Framework users. It contains principles and points of focus. This guide’s five principles are consistent with the five COSO Internal Control Components and the 17 COSO principles.
Definition of Fraud

Fraud is defined as:

“Any intentional act or omission to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.”
Deterrence is achieved when an organization implements a fraud risk management process that:

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture
- Includes a thorough fraud risk assessment periodically
- Designs, implements, and maintains preventative and detective fraud control processes and procedures
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in the wrongdoing
For organizations desiring to establish a comprehensive approach to managing fraud risk, this guide includes guidance on establishing an overall Fraud Risk Management Program including:

- Establishing fraud risk governance policies
- Performing a fraud risk assessment
- Designing and deploying fraud preventive and detective control activities
- Conducting investigations, and
- Monitoring and evaluating the total fraud risk management program
Ongoing Comprehensive Fraud Risk Management Process

- Establish a fraud risk management policy as part of organizational governance
- Perform a comprehensive fraud assessment
- Select, develop, and deploy preventive and detective fraud control activities
- Establish a fraud reporting process and coordinated approach to investigation and corrective action
- Monitor the fraud risk management process, report results, and improve the process

NSAC
National Society of Accountants for Cooperatives
Fraud Risk Management Principles

- **Principle No.# 1 – Fraud Risk Governance:**

  - The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing Control fraud risk.
Fraud Risk Management Principles

- **Principle No.# 1 – Fraud Risk Governance – the Importance of Ethics:**

- Effective boards and organizations address issues of ethics and the effects of ethical behavior on business strategy, operations, and long-term survival. The level of board and organizational commitment to these objectives varies widely and directly effects the fraud risk tolerance of an organization.
Fraud Risk Management Principles

• Principle No.# 1 – Fraud Risk Governance – the Tone at the Top:

  One of the most important elements of effective fraud risk management is the “Tone at the Top” of the organization. Organization leadership has a responsibility to lead by example to ensure that all personnel and all business partners understand that the organization is serious about promoting ethical behavior and is committed to deterring, preventing, and detecting fraud.
• Principle No.# 2 – Fraud Risk Assessment:

• The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.
Fraud Risk Management Principles

• **Principle No.# 2 – Fraud Risk Assessment – Involve Appropriate Levels of Management:**
  
  • Before conducting a risk assessment, senior management identifies a risk management team. The team should include individuals from throughout the organization with different knowledge, skills, and perspectives. In addition, the risk assessment relies on a combination of internal and external resources.
Fraud Risk Management Principles

• **Principle No.# 2 – Fraud Risk Assessment – Considers Various Types of Fraud:**

  • To ensure a comprehensive assessment of potential fraud risks impeding an organization based on its identified objectives, management considers various types of fraud that can be committed against or by the organization.
Fraud Risk Management Principles

- Principle No.# 3 – Fraud Control Activity:
  
  The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
Fraud Risk Management Principles

- **Principle No.# 3 – Fraud Control Activity – the Importance of Documentation:**

  - Fraud control activities are documented with descriptions of the identified fraud risk and scheme, the fraud control activity that is designed to mitigate the fraud risk, and the identification of those responsible for the fraud control activity.
Principle No.# 3 – Fraud Control Activity – Fraud Preventive Controls:

A fraud preventive control is a control activity designed to avoid a fraudulent event or transaction at the time of initial occurrence. Such control activities are specific processes and procedures designed to help eliminate the causes of fraud from occurring.
Fraud Risk Management Principles

- **Principle No.# 3 – Fraud Control Activity – Fraud Detective Controls:**

- A fraud **detective** control is a control activity designed to discover a fraudulent event or transaction after the initial processing has occurred. Such control activities are specific processes and procedures designed to identify attempted or existing frauds in a timely manner, thereby limiting the effects of any fraud that circumvents the organization’s preventive controls.
Fraud Risk Management Principles

• Principle No. # 4 – Fraud Investigation and Corrective Action:

  • The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.
Fraud Risk Management Principles

- Principle No.# 4 – Fraud Investigation and Corrective Action – “Say Something if You See Something”:
  
  It is essential that any reasonably suspected or known violation, deviation, or other breach of the code of conduct, fraud, or corruption be communicated internally and dealt with in a timely and effective manner, regardless of where in the organization these occur or by whom these are committed.
Fraud Risk Management Principles

- Principle No.# 4 – Fraud Investigation and Corrective Action – Conduct Investigations:
  
  An investigation team establishes the investigation tasks as outlined in an investigation work plan and assigns each task to the appropriate team members. The plan prioritizes the performance of tasks to provide reports of findings. The investigation team considers legal issues and constraints in dealing with employees and third parties, obtains relevant information, and develops related documentation.
Fraud Risk Management Principles

**Principle No.# 4 – Fraud Investigation and Corrective Action – Communicate Results:**

- Reports of investigations are delivered to the individuals overseeing the investigation (e.g., legal counsel, CEO, board chair, directors, senior management) who ultimately will decide on the specific disciplinary or other actions to be taken. The investigation report has to be accurate, clear, and impartial. It presents only relevant facts and is timely in its preparation and delivery.
Fraud Risk Management Principles

- **Principle No. 5 – Fraud Risk Management Monitoring Activities:**

  - The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.
Principle No.# 5 – Fraud Risk Management


Ongoing evaluations are generally routine processes that monitor a control activity on a real-time basis. A plan that targets the organization’s areas of highest fraud risk assists the organization in managing an ongoing evaluation of the five principles of fraud risk management.
Users of the Guide

• **Board of Directors:**
  • Provides oversight
  • Defines expectations
  • Challenges Management / asks tough questions
  • Seeks input from internal auditors, independent auditors, external reviewers, and legal counsel and utilizes these resources as needed to investigate any issues.
Users of the Guide

• **Senior Management:**

  • Assesses the entity’s Fraud Risk Management Program in relation to this Fraud Risk Management Guide, focusing on how the organization applies the five principles in support of its Fraud Risk Management Program. Further, they assess the entity’s fraud risk in compliance with principles of the 2013 COSO Framework.
Users of the Guide

• **Other Management and Personnel:**
  
  • Consider how they are conducting their responsibilities in light of this guide and discuss with more senior personnel ideas for strengthening fraud risk controls. More specifically, they consider how existing controls affect the relevant principles within the five components of fraud risk management, as well as principles of the COSO Framework.
Users of the Guide

- **Internal Audit:**

  - Review their internal audit plans and how the plans are applied to the entity’s Fraud Risk Management Programs in connection with implementation of this guidance. Internal auditors will review this guide and consider possible implications of changes to the entity’s fraud risk program on audit plans, evaluations, and any reporting on the entity’s fraud risk management and system of internal control.
Users of the Guide

- **Independent Auditors:**
  
  In many situations, an independent auditor is engaged to audit or examine the effectiveness of the client’s internal control over financial reporting in addition to auditing the entity’s financial statements. The 2013 COSO Framework introduced principle 8: the organization considers the potential for fraud in assessing risks to the achievement of objectives. Auditors can assess the entity’s implementation of that principle using this guide.
Users of the Guide

- **Other Professional Organizations:**
  - Providing guidance on fraud risk as it relates to operations, reporting, and compliance may consider their standards and guidance in comparison to the guide. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
Users of the Guide

• **Educators:**
  
  • With the presumption that the guide attains broad acceptance, its concepts and terms will find their way into university curricula.
The Guide contains some 60 pages of appendices. These appendices contain valuable templates, samples, examples, and tools to assist users in implementing the guide’s best practices. Included are: glossary of terms, sample fraud control policy frameworks, listings of fraud risk exposures, sample surveys, reference materials, and sample scorecards for risk governance, risk assessment, fraud control activities, fraud investigations, risk management monitoring, and fraud corrective actions.
To buy a copy of the Guide, go to The Institute of Internal Auditors website Bookstore: $ 55.20 for members, $ 69.00 for non-members: at www.theiia.org.
Resources

- Committee of Sponsoring Organizations (COSO): www.coso.org
- Institute of Internal Auditors (IIA): www.theiia.org
- Association of Certified Fraud Examiners (ACFE): www.acfe.com
COSO Fraud Risk Management Guide

Questions???