Effective implementation of COSO's new anti-fraud guidance

EY
Building a better working world

In September 2016, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a new Fraud Risk Management Guide (Anti-fraud Guide or Guide) in order to help organizations protect themselves and their stakeholders from acts of intentional deception, whether originating internally or externally. The Association of Certified Fraud Examiners (ACFE) is the Anti-Fraud Guide's co-author.

The Guide describes the critical importance of managing fraud risk as follows:

> "Large frauds have led to the downfall of entire organizations, massive asset and investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets, government, and not-for-profit entities."[1]

In this white paper, Ernst & Young LLP (EY or we) summarize the Anti-fraud Guide and its relationship to COSO's Internal Control – Integrated Framework. We describe COSO's definition of fraud, principles of fraud risk assessment and fraud risk management. We also provide practical guidance for implementation of the Anti-fraud Guide.

[1]The Guide, page 1.

Building on COSO's Internal Control – Integrated Framework

Beginning in 1992, with its publication of the original Internal Control – Integrated Framework, COSO has provided guidance for corporate governance and internal control that has been widely adopted as leading practice by numerous organizations. COSO now describes fraud risk management as "an integral component of corporate governance and the internal control environment,"[2] and emphasizes that fraud risk management is an issue for both the boards of directors and senior management.

Specifically, the Anti-fraud Guide builds on the COSO 2013 Internal Control – Integrated Framework (the 2013 Framework) that elevated the risk of fraud to the organization's "achievement of objectives."

The Anti-fraud Guide recommends comprehensive assessment of the risks of fraud, as distinguished from the risks of internal control errors.[3] The Anti-fraud Guide also recommends that each organization establish a comprehensive fraud risk management program.[4] In order to support this recommendation, the Anti-fraud Guide includes tools and resources for conducting a fraud risk assessment, writing an anti-fraud policy and establishing a comprehensive anti-fraud program.

Organizations should review the Anti-fraud Guide to assess their fraud exposures, to benchmark their capabilities against COSO's fraud risk management principles and to consider how to adapt the Anti-fraud Guide to their specific needs. Each organization will have choices to make, based on an understanding of its fraud risks and risk tolerance, along with consideration of the benefits and costs of specific anti-fraud controls.

Principle #8 of the 2013 Internal Control – Integrated Framework states that: "The organization considers the potential for fraud in assessing risks to the achievement of objectives."

The Anti-fraud Guide provides resources for fraud risk assessment and for fraud risk management.

[2] Ibid, page 8.
[3] Ibid, page 4.
[4] Ibid, page 3.

Defining fraud

COSO's definition of fraud is succinct: "Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain."[5] However, the scope of fraud is expansive. The Anti-fraud Guide uses the following categories:[6]

• Fraudulent financial reporting	• "Any intentional misstatement of accounting information represents fraudulent financial reporting."
• Fraudulent non-financial reporting	• "[F]raudulent non-financial reporting risks and schemes" that can lead to false environmental, safety, quality assurance reports or operational metrics.

• Misappropriation of assets	• "[B]y employees, customers, or vendors, [or] criminal organizations" affecting tangible and intangible assets and business opportunities.
	• Examples include:
	  • Employee theft
	  • Fictitious vendor invoices
	  • False customer claims
	  • External cyber-hacks

• Other illegal acts and corruption	• Illegal acts are: "violations of laws or governmental regulations that could have a material direct or indirect impact on the external financial reports." • Examples include bribery, abetting fraud, violating laws, illicit use of personal information, of trade secrets or of national security information and violations of labor, technology export or consumer protection laws. • Corruption is "the misuse of entrusted power for private gain," (e.g., violating the U.S. Foreign Corrupt Practices Act or similar laws of other countries.)

The Anti-fraud Guide sets out an approach to identify, assess and manage this broad range of risks.

[5] Ibid, page viii, emphasis added. This definition of fraud is key to a fraud risk assessment: "An organization that simply adds the fraud risk assessment to the existing internal control assessment may not thoroughly examine and identify possibilities for intentional acts designed to misstate, misappropriate or perpetrate." (Ibid, page xiii.)

[6] Ibid, pages 23-27. The Guide notes that the ACFE and COSO's 2013 Framework use somewhat different classifications. (Ibid, page 22.)

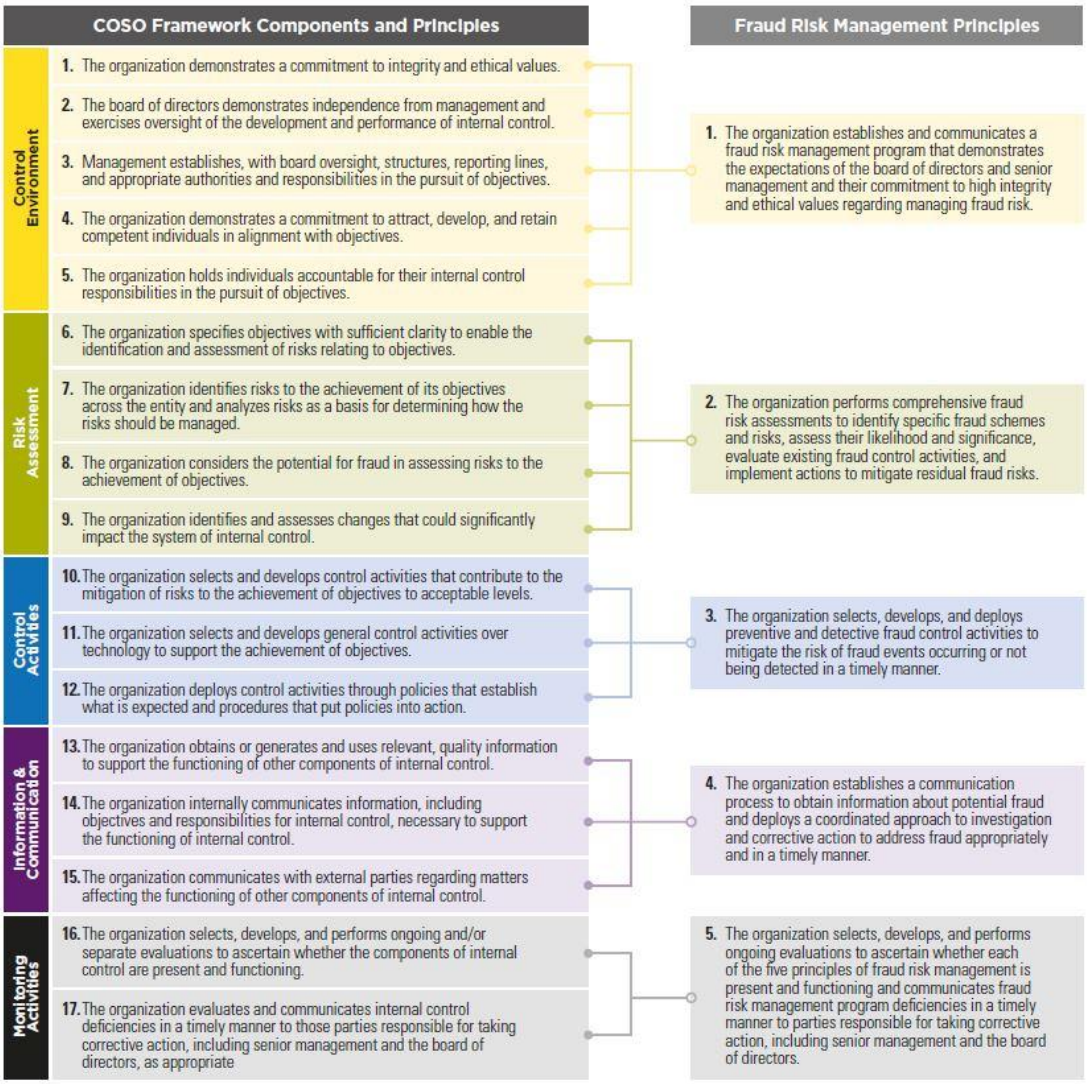
Strengthening the 2013 Framework's fraud risk assessment principle

COSO revised its Internal Control – Integrated Framework in 2013, defining 17 principles that guide the design and implementation of systems of internal control. For a system of internal control to be effective, each of the principles should be present, functioning and operating together in an integrated manner.

Principle 8 of the 2013 Framework brought specific focus to fraud, by requiring the organization to consider "the potential for fraud in assessing risks to the achievement of objectives" in support of a comprehensive risk assessment.[7]

The Anti-fraud Guide now goes beyond fraud risk assessment to distill five principles of fraud risk management. These five principles align with the 17 principles of integrated internal control:

Weaving fraud risk management into an integrated system of controls[8]



[7] The 2013 Framework states: "The actions being conducted as part of applying this principle [8] link closely to the preceding principle (identifies and analyzes risks), which assesses risks based on the presumption that the entity's expected standards of ethical conduct are adhered to by management, other personnel and outsourced service providers. This principle, Assesses Fraud Risk, assesses risk in a different context, when an individual's actions may not align with the expected standards of conduct." 2013 Framework, page 78, emphasis added.

[8] The Guide, page ix.

Fraud risk assessment and fraud risk management

To be clear, the five fraud risk management principles are not mandatory for compliance with the 2013 Framework. The Anti-fraud Guide "is intended to be supportive of and consistent with the 2013 COSO Framework." An organization "can use this guide's second fraud risk management principle … on a stand-alone basis to conduct a fraud risk assessment that is compliant with 2013 COSO Framework principle 8" or it "can implement this guide as a separate, compatible, and more comprehensive process for specifically assessing the organization's fraud risk as part of a broader fraud risk management program or process."[9]

The option that an organization chooses, however, should reflect a comprehensive understanding of its fraud risks and a frank assessment of its fraud risk management capabilities.

Fraud risk management principles

The Anti-fraud Guide provides detailed guidance and implementation resources for each of the fraud risk management principles:

Principle 1 addresses fraud risk governance by providing a foundation of ethical (not merely compliant) behavior and a "corporate governance program related specifically to fraud risk."[10] The Anti-fraud Guide states that [it] is "critical to the success of a fraud risk management program for one executive-level member of management to be assigned overall responsibility for fraud risk management and to report to the board periodically."[11]

Principle 2 addresses fraud risk assessment by identifying specific schemes, assessing their likelihood and potential impact and assessing the effectiveness of the organization's controls. As the Anti-fraud Guide recognizes, risk tolerance is an important consideration; an organization should invest in the management of its most critical risks.

Principle 3 addresses fraud control activities. Controls are specific to each fraud risk and are designed to prevent (and to deter) fraud incidents or to detect them promptly. An organization should use a mix of controls at different points in a business process. Preventive controls are broadly communicated; detective controls operate in the background. As we discuss below, the Anti-fraud Guide describes how data analytics can provide not only cost-efficient detective controls, but also a distinctive view of anomalies, trends and risk indicators.

The Anti-fraud Guide describes human resources' anti-fraud procedures, including background checks, incentive compensation reviews, segregation of duties and employee surveys, exit interviews and the confidential reporting or "whistleblower" system.[12] The Anti-fraud Guide also highlights the problem of management's override of controls, noting that "[i]n all but a very few cases, catastrophic frauds in the past were perpetrated by senior management officials."[13]

[9] Ibid, page 3.
[10] Ibid, page 9.
[11] Ibid, page 13.
[12] The Anti-fraud Guide categorizes confidential reporting as a Human Resources activity (see pages 44-47), but organizations that follow the Federal Sentencing Guidelines, U.S. Department of Justice and SEC anti-corruption program guidelines, or other regulatory compliance guidelines, typically assign responsibility for confidential reporting, incident response and communication of standards of conduct to a compliance and ethics program.
[13] The Guide, page 48. The Anti-fraud Guide refers to the AICPA's publication "Management Override of Internal Control: The Achilles' Heel of Fraud Prevention," an example of the application of the "Fraud Tree" factors of incentives/pressure, opportunity and rationalization factors to assess the likelihood of a significant fraud risk. (The Guide, page 48). The publication is available at https://www.aicpa.org/forthepublic/auditcommitteeeffectiveness/downloadabledocuments/achilles_heel.pdf.

Principle 4 addresses response to reports of fraud through "a system for prompt, competent, and confidential review, investigation, and resolution of instances of non-compliance and allegations involving fraud and misconduct."[14] An organization should have fraud investigation and response protocols, starting with a "'say-something-if-you-see-something' culture," and continuing through report triage, case management, the securing of evidence, the obtaining of legal and forensic accounting assistance, root-cause assessment and controls remediation.[1]

Principle 5 addresses monitoring of program activities to ensure that each of the five principles is present and functioning as designed, and to address deficiencies. Organizations should establish metrics of program operations and outcomes, e.g., year-over-year trends of fraud incidents. Organizations should also "consider known fraud schemes and new frauds discovered and reported in other industries and in other organizations in the same industry."[15]

The Anti-fraud Guide does not only apply to business organizations; its Appendix K has guidance for "Managing the Risk of Fraud, Waste, and Abuse in the Government Environment."

An emphasis on data analytics

COSO's 2016 Anti-fraud Guide updates the 2007 publication, Managing the Business Risk of Fraud: A Practical Guide.[16] Perhaps the biggest change is the focus on data analytics: The Anti-fraud Guide recommends that each organization have "a strategy for proactively using data analysis activities to assess areas of high fraud risk and to monitor fraud mitigation activities and controls."[17]

As compared to the 2007 Guidance, which mentions the word "analytics" only two times, the Anti-fraud Guide makes reference to analytics well over 100 times!

EY considers data analytics as important to fraud risk management. Regulators increasingly use data analytics to detect fraud;[18] professional guidance requires auditors to use analytics in fraud risk assessments.[19] The volume of data that organizations generate has exploded, and many analytics tools have become available.[20] As the Anti-fraud Guide states, "[D]ata analytics techniques can help isolate transactions or trends that represent potential fraud,"[21] can "trigger a follow-up investigation of anomalous trends rather than impose costly or intrusive controls designed to prevent every fraudulent transaction,"[22] and can support investigations and remediation of controls.[23]

[14] Ibid, page 54.
[15] Ibid, page 66.
[16] The authors were the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and the Association of Certified Fraud Examiners (ACFE).
[17] The Guide, page 14 (footnote omitted).
[18] "The Division of Economic and Risk Analysis (DERA) was created in September 2009 to integrate financial economics and rigorous data analytics into the core mission of the SEC. The Division is involved across the entire range of SEC activities, including policy-making, rule-making, enforcement, and examination." See https://www.sec.gov/dera/about
[19] The Guide, page 31.
[20] See EY "Global Forensic Data Analytics Survey 2016, Shifting into high gear: mitigating risks and demonstrating returns," available at http://www.ey.com/GL/en/Services/Assurance/Fraud-Investigation---Dispute-Services/EY-shifting-into-high-gear-mitigating-risks-and-demonstrating-returns
[21] The Guide, page 31.
[22] Ibid, page 44.
[23] Ibid, pages 58 and 60.

The Anti-fraud Guide provides practical examples for the application of leading data analytics techniques ranging from simple categorization to predictive and prescriptive models, including:

- Data stratification showing transactions in different business units or regions
- Risk scoring
- Trend analysis
- Data visualization
- Statistical and predictive modeling
- Big data and external information sources, including both structured and unstructured data sources

Appendix E of the Anti-fraud Guide describes how to implement a data analytics program in the context of a fraud risk program.

What should organizations do now?

The Anti-fraud Guide sets out a process for ongoing, comprehensive fraud management.[24]

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

[24]The Guide, page xiii.

EY recommends that each organization consider this process, and view the publication of the Anti-fraud Guide as an opportunity to review its fraud risks, to assess its risk mitigation activities across all the types of fraud that the Guide describes, and to develop an action plan.

As a first step, we recommend that the organization form a team consisting of representatives from different departments and business lines, having diverse perspectives about the organization's operations, fraud risks and anti-fraud controls. This team should:

- Review the Anti-fraud Guide as a benchmark document.
- Review the organization's recent fraud risk assessments to determine whether they provide a clear picture of the company's vulnerabilities and a solid basis for management decisions about deploying resources.
- Ask pointed questions to assess preparedness, for example:
  - Fraudulent financial reporting. What false statements might be made to management, and repeated in the organization's financial reports, regulatory filings or product descriptions?
  - Fraudulent nonfinancial reporting. Which of our reports do our regulators, customers or management consider critical?
  - Misappropriation of assets. What assets, personal data and intellectual property must the organization protect?
  - Illegal acts and corruption. What violations of law could have material impact on external financial reports?
  - Assessment. What fraud risk schemes are common to the organization's business lines and countries of operation? Is the organization leveraging its data for new insights about its fraud risks?
  - Prevention. Who might deceive the organization? Why and how? Are they inside the organization, outside the organization – or a combination of both?[25]
  - Detection. Is the organization investing in the right detective controls?
  - Response. If there is a report of fraud, can the organization respond quickly enough to protect critical assets, meet law enforcement expectations and protect the organization's reputation?
- Review the programs and departments in place to manage the types of fraud that COSO describes, e.g., the organization's financial controllership structure, its SEC disclosure committee, anti-bribery program and cybersecurity program.

[25]See EY's booklet, Managing insider threat A holistic approach to dealing with risk from within, available at http://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf

- Review the organization's fraud risk governance to determine if roles and responsibilities are clearly defined and if there are lines of defense (e.g., management, fraud risk owners and auditors) that would provide organizational checks and balances.
- Review the ethics and compliance program, including the organization's code of conduct, confidential reporting line and investigation protocols. Has the ethics and compliance program been adequately designed and resourced to support the elements of the Anti-fraud Guide? Do employees and contractors trust management and the confidential reporting line? Do they provide tips about frauds, crimes and security breaches?
- Consider whether senior management sets a strong ethical "tone at the top," and whether there is a culture of integrity in all of the organization's departments and regional operations.
- Consider whether senior management has the information it needs to make decisions about fraud risk management and allocation of resources.
- Consider whether the board of directors has the information it needs to provide oversight of anti-fraud risks for the organization, and more particularly, to guard against fraud by senior management.
- Prepare recommendations for implementation:
  - Choose one of the Anti-fraud Guide's two options: (i) a comprehensive fraud risk assessment in support of Principle 8 of the 2013 COSO Internal Control Framework, or (ii) a fraud risk management program that includes a comprehensive risk assessment and is based on COSO's five principles.
  - For a fraud risk assessment, consider whether the organization should update existing assessments or launch a new assessment. If the latter, then: Who will do conduct the assessment? What subject-matter resources will be required? What department will provide the budget? What assessment criteria will the organization use? How will the organization determine risk tolerance for specific types of fraud?
  - Or for a fraud risk management program, consider the organization's governance and design. How will a fraud risk management program align with existing programs and resources (i.e., anti-fraud, cyber-security, compliance and ethics or anti-corruption)?[26] Who should lead the program? How should the organization incorporate anti-fraud management into its existing corporate governance framework in order to facilitate board oversight and management actions?

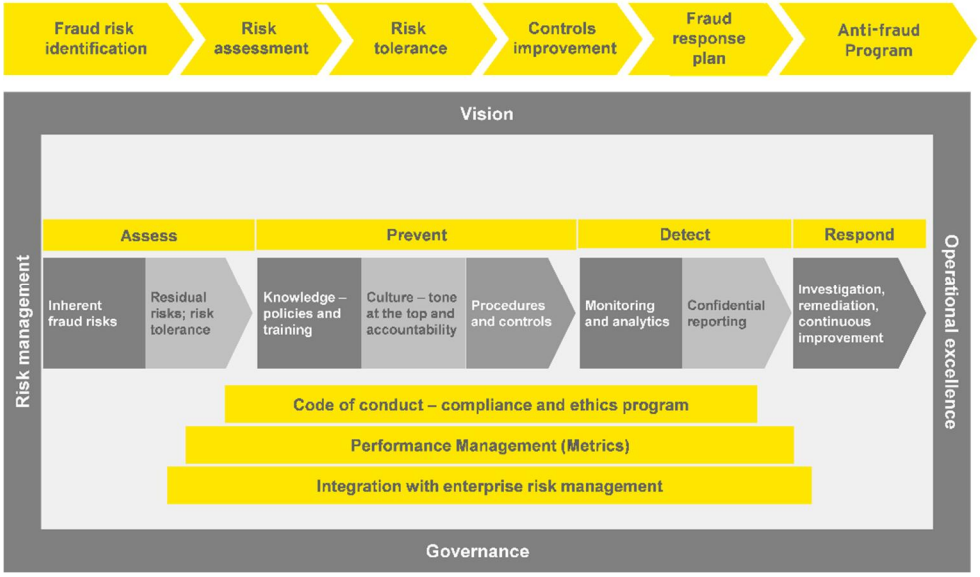
[26] The Anti-fraud Guide mentions compliance and ethics programs in passing. It also refers to governmental compliance guidelines that address criminal and regulatory fraud (see page 1 of the Guide). Chief Ethics and Compliance Officers and others responsible for fraud related programs (e.g., bribery or cyber security) might have direct reporting lines to the board of directors.
Organizations that create a fraud risk management program, with an executive-level anti-fraud program leader who reports to the board, should consider how to align the various fraud-related programs, leverage resources and processes across the programs and align roles, responsibilities and governance procedures. They should also consult with the board about program reporting relationships and sources of information that will facilitate oversight of such interrelated topics as corporate ethics, anti-fraud, legal compliance and cybersecurity.

How Ernst & Young LLP's Fraud Investigation & Dispute Services can help

When facing acts of fraud, government investigations, regulatory inquiries, major litigation or transactional disputes, clients turn to EY's Fraud Investigation & Dispute Services (FIDS) practice for timely and experienced assistance. FIDS' forensic accountants and other industry specialists work with our clients' legal counsel, internal audit teams and compliance departments to investigate and evaluate complex issues, and to develop practical solutions that address operational challenges.

Our multidisciplinary professionals are leaders in their field and have been drawn from both industry and the public sector, including national law enforcement, securities regulation and cyber intelligence agencies. We apply the collective knowledge and insight gleaned from working across industries and geographies to help our clients conduct fraud risk assessments, institute proactive anti-fraud and anti-corruption programs, utilize forensic data analytics and address complex business and financial challenges. Our framework provides a structured approach to fraud risk assessment and management, and we can help clients to design and implement effective anti-fraud programs.

From fraud risk assessment to fraud risk management



EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

Score no. 03095-161Gbl
1608-2037590

ED None

ey.com