WINNING THE RISK GAME

COSO AND THE ACFE RELEASE NEW GUIDE ON MANAGING FRAUD RISK

Organizations can prevent massive, paralyzing frauds. And they can detect small frauds before they become massive frauds. Practical anti-fraud support is available in the new COSO/ACFE *Fraud Risk Management Guide*.

"Fraud can't happen to us."

Tell that to the C-suite of Wells Fargo. Or the devastated Madoff investors. Or the managers at Lehman Brothers. Or the more than 20,000 former employees of defunct Enron. Or the millions of fraud victims around the world.

In spite of evidence that fraud can occur in organizations when individuals are motivated in that direction, many organizations sometimes underemphasize the importance of fraud deterrence, prevention and detection.

Fraud is almost always devastating to an organization. It's not just the monetary and reputational damage; the sense of betrayal and loss of trust in employees and leaders can have long-lasting impacts.

Organizations *can* prevent massive, paralyzing frauds. And they can detect small frauds before they become massive frauds. Fraud risk management guidance is available for well-run organizations that commit to protecting stakeholder assets. Managing fraud risk is a systematic process that has benefits beyond protecting assets and reputations.

Now, many of you work for organizations that have been intensely looking for ways to prevent fraud for years. But just as many of you (possibly more) have been trying to persuade management

By David L. Cotton, CFE, CPA, CGFM; Sandra Johnigan, CFE, CPA/CFF; and Leslye Givarz, CPA

to learn the techniques of fraud examination and construct realistic measures to fend off fraud in its many forms. This article is for both groups — and all those in between.

Here's renewed hope for organizations of all sizes: the new COSO/ACFE *Fraud Risk Management Guide*. (Visit ACFE.com/fraudrisktools and read the sidebar on page 53.)

The new guide is built on the foundation of the efforts of many since the 1980s. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has been tackling fraud-fighting issues since it released its first report in 1987. (See the sidebar on page 54.) The COSO's 2013 *Internal Control – Integrated Framework* — a revision and update of COSO's 1992 version — contains a specific focus on fraud risk management, which became an explicit requirement for COSO followers.

The 2013 framework includes (along with its three internal control objectives and five internal control components) 17 internal control principles. These principles represent the "fundamental concepts associated with each component."

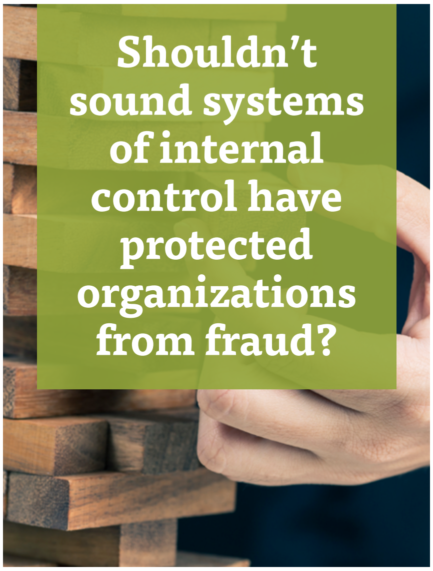
Taken aback by principle 8

Principle 8 of COSO's 2013 *Internal Control – Integrated Framework* is: *The organization considers the potential for fraud in assessing risks to the achievement of objectives.*

In response to the 2013 COSO framework, organizations began trying to implement its new principles and seeking guidance on how to comply with principle 8.

Many organizations — even those that had been conforming to the 1992 framework for 21 years — were taken aback by this new *fraud* addition. Since COSO's roots were fraud-focused (the Treadway Commission Report was titled *The National Report on Fraudulent Financial Reporting*, after all), shouldn't fraud risk have always been the central focus of the framework? Shouldn't sound systems of internal control have protected organizations from fraud? Perhaps. It depended on how organizations viewed and implemented the framework.

It's one thing to design a system of baseline controls to guard against *unintentional* errors and misstatements, such as installing checks and balances, using computer programs to ensure accuracy, requiring management approvals, segregating duties and pre-approving vendors. It's a different matter, however, to design a system that protects against *intentional* misstatements and fraudulent transactions.



Shouldn't sound systems of internal control have protected organizations from fraud?

When organizations consider *intent*, controls designed to guard against *unintentional* errors or misstatements might no longer do the job. For example, it's possible to deliberately circumvent checks and balances, surreptitiously alter computer programs, forge or evade managerial approvals, override the segregation of duties and add bogus vendors to an approved vendor list.

It's likely that many organizations following the 1992 COSO framework hadn't specifically and explicitly considered fraud risk as part of their internal controls and that many of them assumed that baseline controls were more than sufficient.

However, COSO principle 8 warrants that *all* organizations pause and reconsider the adequacy of their controls by asking a simple extra question with respect to every control: *Is this control adequate if someone tries to intentionally override or circumvent it?* Another — more important — consideration regarding the establishment of principle 8 is to prompt all well-run and forward-thinking organizations to address fraud risk in a more comprehensive and proactive manner.

Task force yields new COSO/ACFE guide

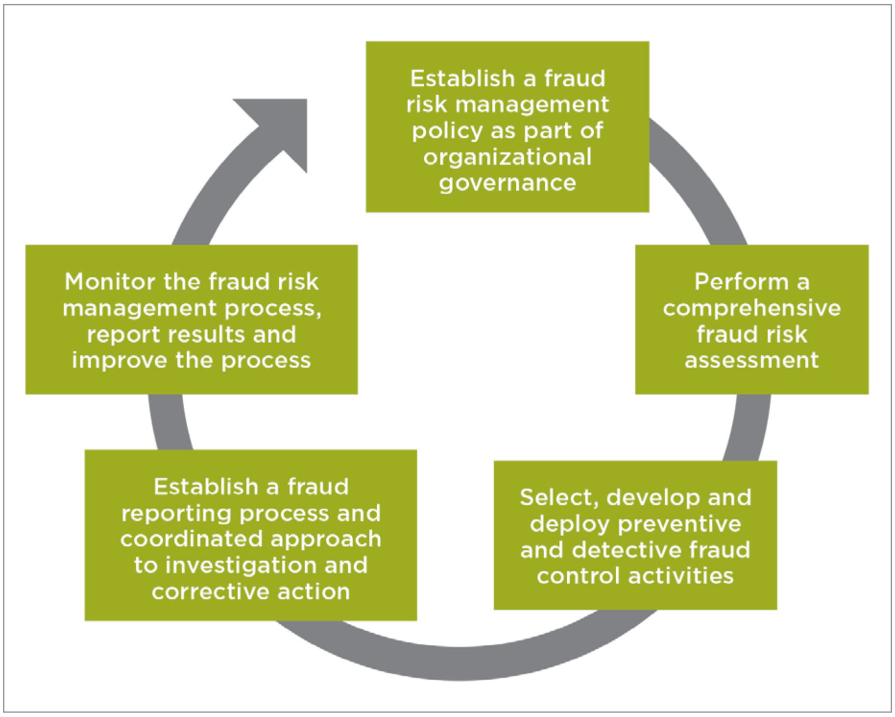
To meet the demand for more comprehensive guidance on fraud risk management, COSO and the ACFE formed a task force in January 2015. This 31-member task force's mission was to update the 2008 publication *Managing the Business Risk of Fraud — A Practical Guide* (MBRF) to make it consistent with and supportive of the 2013 COSO Framework. (In that earlier guide, the ACFE, Institute of Internal Auditors and the American Institute of CPAs explained how to establish a comprehensive fraud risk management program consisting of fraud risk governance, fraud risk assessments, fraud prevention and detection controls, and an investigation and reporting process.)

The task force completed its efforts by the end of 2015, and the *Fraud Risk Management Guide* was published in September 2016.

In addition to aligning with the 2013 COSO Framework's internal control components, the *Fraud Risk Management Guide* supports its five principles with numerous *points of focus* that also are consistent with those in the 2013 COSO Framework.

Five essential processes

The *Fraud Risk Management Guide* describes implementation of the five principles through five essential processes (see Figure



Establish a fraud risk management policy as part of organizational governance
Perform a comprehensive fraud risk 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

Figure 1: Ongoing, comprehensive fraud risk management process (from the *Fraud Risk Management Guide*)

1 above) to protect stakeholder assets and interests from fraud risks.

1. Establish fraud risk governance policy

The commitment to implement the fraud risk management process will come from the highest organizational level — ideally, the governing board. It's usually not difficult to convince a governing board to embrace and promote comprehensive fraud risk management; when an organization falls victim to fraud, board members almost always absorb much or most of the blame because of their governance responsibilities.

Implementing the fraud risk management commitment then entails appointment of a "champion" to oversee the process. That person needs to be at a high enough organizational level to ensure that employees take the process seriously, have adequate resources and see it through to completion.

The fraud risk governance policy establishes and documents the commitment to managing fraud risk; summarizes fraud control strategies; outlines the fraud risk management program; defines procedures for reporting fraud; establishes employment conditions; defines conflict of interest policies; establishes procedures for fraud investigation; sets forth an internal audit strategy; and explains the review, monitoring and feedback process.

Good news here: An organization doesn't need to develop a fraud risk governance policy from scratch. The *Fraud Risk Management Guide* contains a "Sample Fraud Control Policy Framework" and a "Sample Fraud Risk Management Policy" that can be adapted to any organization.

2. Assess fraud risk

This step is the most important fraud risk management step, because it establishes the baseline for succeeding steps. Assembling a fraud risk assessment team comprising employees from all parts of the organization — not just financial management and accounting personnel but also operations personnel — is important. The fraud risk assessment team then meets to carry out a comprehensive *brainstorming* process. (Merriam-Webster defines brainstorming as "A group problem-solving technique that involves the spontaneous contribution of ideas from all members of the group; *also*: the mulling over of ideas by one or more individuals in an attempt to devise or find a solution to a problem.")

The goal is to think of every potential way that fraud could happen to or within the organization. Effective brainstorming requires energy, imagination and creativity. Numerous meetings held over several weeks enable participants to maintain high levels of these characteristics, which will promote comprehensive results.

The fraud risk assessment documentation chart, Figure 2 on page 50, can help you organize the results of your brainstorming sessions.

The goal is to fill that first column with a thorough, comprehensive list of potential fraud vulnerabilities and schemes. Keep brainstorming until that list is complete. (During this process, participants inevitably will discuss fraud cases at other organizations, and you'll ask, "Could that happen to us?" Check to see if you've addressed those same frauds in your initial fraud risk assessment.)

More good news here. The new guide contains a comprehensive list of the most common fraud schemes as good starting points for the risk assessment process.

After the team members complete the first column in the fraud risk assessment documentation chart (page 50), they assess each potential fraud scheme from the perspectives of *likelihood* (What are the chances this might happen?) and *significance* (If this happens, how much damage would it cause?). In assessing *significance*, don't think just in monetary terms. Reputational damage is often a greater consideration — especially for tax-exempt, academic and governmental organizations.

The team then creates a "heat map" (Figure 3, page 52) that plots the likelihood of occurrence and significance of specific frauds. The numbers represent identified fraud risks in an organization. Organizations often use employee surveys, facilitated sessions and other data-gathering techniques to gain a more reflective perspective on fraud risks.

Every organization has its own "tolerance for risk." One organization might decide that it can ignore low-likelihood, low-significance potential frauds (and thus not put preventive controls in place), while another might want controls for *every* possible fraud.

Completing the fraud risk assessment documentation then entails:

- Identifying who might be involved in each possible fraud scheme or exposure.
- Identifying any *existing* fraud control procedures already in place with respect to each fraud scheme or exposure.
- Assessing the effectiveness of each existing fraud control procedure.
- Determining the residual risk after considering the effectiveness of existing controls.
- Deciding on the fraud risk response where residual risk exists.

The fraud risk responses column in the fraud risk assessment documentation chart (below) is the trigger for the next steps in the process. Wherever the team finds residual risks, it considers additional prevention and detection controls.

3. Design and implement fraud control activities

Fraud prevention control activities are designed to stop a fraud before it happens. These activities can include such elements as segregating duties, requiring higher-level approvals and incorporating better physical security over assets. Prevention control activities don't need to be complex or expensive to be effective.

The key in designing prevention control activities is to work from the fraud risk assessment documentation and to carefully and methodically devise the most cost-effective controls that should prevent each type of fraud. Internal auditors can be effective at designing these controls. And if the organization is too small to have an internal audit staff, it can retain an accountability professional such as a Certified Fraud Examiner to help in that part of the process.

Fraud detection control activities are designed to identify any frauds that happen *as soon as possible after they happen*. If an organization detects frauds quickly, the crimes are unlikely to grow to become catastrophic. (As a colleague of ours always says, "There are no such things as small frauds, just frauds that haven't matured yet.")

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Financial Reporting • • •							
Non-Financial Reporting • • •							
Asset Misappropriation • • •							
Illegal Acts and Corruption • • •							

Figure 2: Fraud risk assessment documentation (from the *Fraud Risk Management Guide*)

If an organization does a great job designing *prevention* controls, does it need *detection* controls? Good question. There are two reasons for *detection* control activities.

First, it's simply impossible to think of *every* fraud scenario that might occur; fraud perpetrators are clever, resourceful and sometimes desperate enough to take foolish chances. Second, and perhaps more importantly, prevention controls can come with a cost — not just the cost of the procedures themselves but also the cost of operational disruption.

For example, consider a retail clothing business. Because shoplifting can erode profits, the company *could* design prevention controls and put them in place to stop all shoplifting. The business *could* require all shoppers to check their shopping bags and purses at the door when they enter the store. And it could install closed-circuit TV cameras in all the dressing rooms. While these controls probably will stop shoplifting, the business is likely to quickly lose all its customers.

So, organizations need to allow that reasonable prevention controls won't stop every fraud scheme. Therefore, it's important for organizations to install detection controls to *detect* each possible fraud scheme if it happens.

While most prevention controls are in the open and visible for employees and stakeholders to see, the most effective *detection* control procedures are usually covert; they operate quietly in the background, and only a small group knows about them.

Because almost every organization now has electronic records, *data analytic control procedures* can be the least costly and most effective detection controls to implement. For example, if one of the fraud concerns is that an employee might set up a phony vendor and process payments to that vendor, the organization can easily set up a data analytic process that periodically compares the employee database and vendor database to identify any matching names, addresses, phone numbers, bank routing numbers, etc. That process should identify any bogus vendors as soon as they're set up. (This example demonstrates why it's important that such control procedures are covert.)

4. Establish reporting and investigation processes

According to the 2016 *ACFE Report to the Nations on Occupational Fraud and Abuse* (ACFE.com/RTTN), the No. 1 source of discovered frauds is tips, usually from employees of the victim organization. In smaller organizations (100 employees or

less), 29.6 percent of discovered frauds come from this source; in larger organizations, 43.5 percent of discovered frauds come from this source (Figure 22, page 22). And, according to the report, organizations with fraud hotlines experienced frauds that were 50 percent less costly and detected frauds 50 percent more quickly (Figures 59 and 60, page 44).

Given those statistics, an organization that's fully committed to managing fraud risk will set up a hotline reporting mechanism. But aren't hotlines expensive? Not any more. Organizations can subscribe to an independent, external, web- or telephone-based reporting system for a few hundred dollars per year. (A caution: Perform due diligence when selecting an external hotline vendor. Make sure the vendor has sound information security controls to protect the sensitive information it possesses.)

Although the risk assessment team designs and implements preventive and detective control activities for all fraud schemes, your organization will need more fraud risk management work. The next step is to anticipate what can happen if a fraud perpetrator succeeds despite fraud risk management efforts.

A common mistake many organizations make is waiting until they're victims to decide what to do. It's far better to have a well-thought-out plan that you can implement immediately rather than having to make hasty and ill-advised decisions in the chaotic and emotional environment immediately following the discovery of a fraud. Your organization must be committed to taking swift, decisive and appropriate actions against the fraud perpetrator once you've discovered and proven the fraud.

Your organization might be tempted to settle the unpleasant fraud matter quietly and quickly by letting the perpetrator simply resign and disappear. While that *might* minimize the reputational impact to the organization, it allows the perpetrator — now a smarter criminal — to victimize another organization. Further, and perhaps more importantly, despite any efforts to keep the matter quiet, other employees will almost undoubtedly know what has happened. The organization should be prepared for more fraud if it sends the message that the only consequences of committing fraud are collecting a severance payment and finding a new job.

And, of course, it's also important to make sure that you fix the control breakdown that allowed the fraud.

5. Monitor the entire fraud risk management process

After your organization has established fraud risk governance, performed a fraud risk assessment, implemented control activities, and established reporting and investigation processes, the fraud management work still isn't complete.

Just as internal control documentation doesn't necessarily mean that controls are being carried out as documented, designing a fraud risk management process doesn't mean that the process will continue to work as designed. *Monitoring* the overall process, and each component, ensures that everything operates as planned.

All organizations are dynamic and always changing. They grow, merge, combine, and develop new products and lines of business. Personnel change. Managerial structures change. Industries, markets and operating environments change. Consequently, implementing a fraud risk management program is not a one-and-done exercise. Any changes will trigger the need to reassess fraud risk.

Even if your organization doesn't face that many changes, it's important that you conduct a new fraud risk assessment

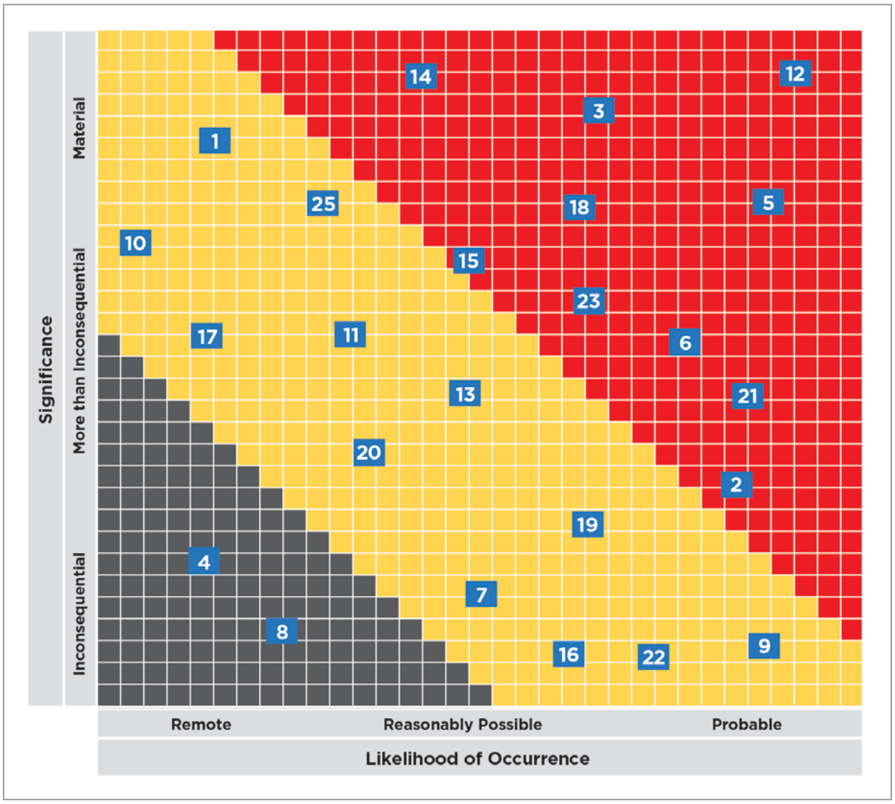


Figure 3: Fraud risk assessment heat map (from the *Fraud Risk Management Guide*)

at least annually. The good news is that reassessments now should be much less time-consuming because they build on previous COSO and ACFE work. Consider using a new risk assessment team to engender fresh perspectives.

Finally, keep your governing board informed about fraud risk management efforts and results. The board will want to know the assessment's rigorousness and effectiveness of the process and controls. And, of course, the board will want to know of any hotline reports, fraud examination results and remediation efforts.

Deterring fraud

Investigating and remediating frauds is expensive. Designing and maintaining preventive and detective controls also comes with a cost. Deterring fraud — establishing an atmosphere and perception that the likelihood of getting caught is so high that it scares potential fraud perpetrators away — is by far the best way to manage fraud risk, and it's cheaper.

An organization can *deter fraud* when it a) establishes a rigorous fraud governance process and ensures that employees are aware of that process, b) conducts a periodic, aggressive fraud risk assessment, c) designs, implements and maintains effective fraud prevention and detection control processes and procedures, and d) takes swift actions against those who attempt to commit fraud.

According to the 2016 *ACFE Report to the Nations*, the presence of anti-fraud controls in the study was correlated with both lower fraud losses and quicker detection. Where controls were present, fraud losses were 14.3 percent to 54 percent lower and frauds were detected 33.3 percent to 50 percent more quickly. (See page 5 of the report or the Executive Summary at http://tinyurl.com/j6bketx.)

The 2016 COSO/ACFE *Fraud Risk Management Guide* contains an executive summary and five chapters — each explaining one of the five fraud risk management principles. The guide also contains valuable appendices and links to additional interactive tools that will facilitate the entire process.

Are the costs worth the benefits?

At this point, your organization's executives might think this whole fraud risk management thing is expensive and time-consuming because it will take time away from other more important activities.

Visit website for *Fraud Risk Management Guide* and other tools

Visit ACFE.com/fraudrisktools to purchase the new COSO/ACFE *Fraud Risk Management Guide* and download its executive summary. You can also access frameworks and reports, and magazine articles plus these free tools:

Interactive scorecards

Use the scorecards to access the five principles for determining the comprehensiveness and effectiveness of your organization's fraud risk management program. (For more information about the principles, see the *Fraud Risk Management Guide*.)

Library of anti-fraud data analytic tests

Explore an interactive tool that details, by fraud risk type, how to integrate data analytics tests into your fraud risk assessment or investigative work plans. The library of test examples displays a variety of tests to consider and is organized by categories of occupational fraud risks.

Risk assessment and follow-up action templates

This Excel spreadsheet provides a risk assessment matrix — which you can use with the foundational matrix in the *Fraud Risk Management Guide* — to document your organization's fraud risks and controls.

The template automatically creates a heat map that shows the significance and likelihood of each identified fraud exposure, a fraud risk ranking page that displays each fraud risk exposure from most to least severe and a control-activities matrix that shows the identification and evaluation of existing control activities related to each fraud risk exposure.

The template also provides space to identify additional control activities and to record your organization's response plan for each exposure. In addition, the template contains pages to record allegations of suspected fraud plus document investigations, outcomes plus fraud risk management monitoring plans.

Points of focus documentation templates

Use these Excel templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud examination and follow up, and fraud risk management monitoring.

However, here are some additional benefits of implementing a fraud risk management program beyond "just" minimizing fraud risk. The risk assessment gives your organization a much better understanding of how it operates. Strong controls protect honest employees. And, the best, most trusted and most respected organizations take proactive measures like fraud risk management. Sending the signal to stakeholders that the organization is committed to the strongest fraud risk management processes conveys an important message: *your money, your time and effort, and your trust are safe with us*.

That message will attract more investments, more business, more donations, more volunteer efforts, more trust and more respect. We can't think of a better way to persuade your C-suite.

Still not sure?

Fortunately, we have an easy way for your executives to find out if making the investment in fraud risk management is the right thing for your organization. Download and give them the guide's five "scorecards." See ACFE.com/coso-scorecard.

These scorecards can help them assess your organization's existing fraud risk management process. They provide key attributes of strong fraud risk governance, risk assessments, control activities, reporting and investigations, and monitoring. Each attribute can be scored as: red ("we have a problem"), yellow ("we are making progress but have room for improvement"), or green ("we have fully implemented this attribute"). Completing each scorecard should only take about 30 minutes (perhaps longer for larger organizations). You should be worried if the results include a lot of reds because the organization probably is vulnerable to fraud.

We probably don't have to convince you that your organization should have a dynamic fraud risk management program. Now we've given you some tools to help persuade your C-suite. These plans will benefit your community and your organization's employees, reputation and shareholders.

If we were to ask the devastated Madoff investors, the managers at Lehman Brothers, the more than 20,000 former employees of defunct Enron or the millions of fraud victims around the world if they believe a small investment in fraud risk management would have been worthwhile, what do you suppose they might say? ■ FM

COSO began anti-fraud mission in 1985

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), an independent private-sector initiative, began in 1985 to study the causal factors that can lead to fraudulent financial reporting.

The COSO member organizations are the American Accounting Association, American Institute of Certified Public Accountants (AICPA), Financial Executives International, The Association of Accountants and Financial Professionals in Business, and The Institute of Internal Auditors (IIA). According to its website, COSO "is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence."

The Treadway Commission issued its *Report of the National Commission on Fraudulent Financial Reporting* in 1987. (James C. Treadway Jr. was a former commissioner of the U.S. Securities and Exchange Commission.)

COSO continued to operate and focused its efforts on improving internal controls and managing enterprise risk. In 1992, COSO issued its initial *Internal Control—Integrated Framework.*

The 1992 framework quickly became the best-practice roadmap for designing, implementing and maintaining a system of internal control. *All* publicly traded companies in the U.S. and most forward-thinking non-public companies, not-for-profit organizations and academic institutions also adhered to that framework.

David L. Cotton, CFE, CPA, CGFM, is chairman of Cotton & Company, LLP, in Alexandria, Virginia. His email address is: dcotton@cottoncpa.com.

Sandra Johnigan, CFE, CPA/CFF, is the owner of Johnigan, P.C., in Dallas, Texas. Her email address is: skj@johniganpc.com

Leslye Givarz, CPA, was a technical editor for both the AICPA and the Public Company Accounting Oversight Board. Her email address is: lgivarz@gmail.com.

The authors were key task force members and principal authors of the COSO/ACFE "Fraud Risk Management Guide." — ed.

Fraud Risk Management Task Force

Barbara Andrews
AICPA

Michael Birdsall
Comcast Corporation

Toby Bishop
Formerly ACFE, Deloitte

Margot Cella
Center for Audit Quality

David Coderre
CAATS

David L. Cotton, chair
Cotton & Company LLP

James Dalkin
GAO

Ron Durkin
Durkin Forensic, Inc.

Bert Edwards
Formerly State Department

Frank Faist
Charter Communications

Eric Feldman
Affiliated Monitors, Inc.

Dan George
USAC

John D. Gill
ACFE

Leslye Givarz
Formerly AICPA, PCAOB

Cindi Hook
Comcast Corporation

Sandra K. Johnigan
Johnigan, PC

Bill Leone
Norton Rose Fulbright

Andi McNeal
ACFE

Linda Miller
GAO

Kemi Olateju
General Electric

Chris Pembroke
Crawford & Associates, PC

J. Michael Peppers
University of Texas

Kelly Richmond Pope
DePaul University

Carolyn Devine Saint
University of Virginia

Jeffrey Steinhoff
KPMG

William Titera
Formerly EY

Michael Ueltzen
Ueltzen & Company

Pamela Verick
Protiviti

Vincent Walden
EY

Bill Warren
PwC

Richard Woodford
U.S. Coast Guard Investigative Service

Fraud Risk Management Advisory Panel

Dan Amiram
Columbia University Business School

Zahn Bozanic
The Ohio State University

Greg Brush
Tennessee Comptroller of Treasury

Tamia Buckingham
Massachusetts School Building Authority

Ashley L. Comer
James Madison University

Molly Dawson
Cotton & Company LLP

Eric Eisenstein
Cotton & Company LLP

Michael Justus
University of Nebraska

Theresa Nellis-Matson
New York Office of the State Comptroller

Jennifer Paperman
New York Office of the State Comptroller

Daniel Rossi
New York Office of the State Comptroller

Lynda Harbold Schwartz
Upland Advisory LLC

Rosie Tomforde
Regional Government

The COSO Board gratefully acknowledges David L. Cotton, chair of the Fraud Risk Management Task Force, for his outstanding leadership and efforts toward the completion of the *Fraud Risk Management Guide*.