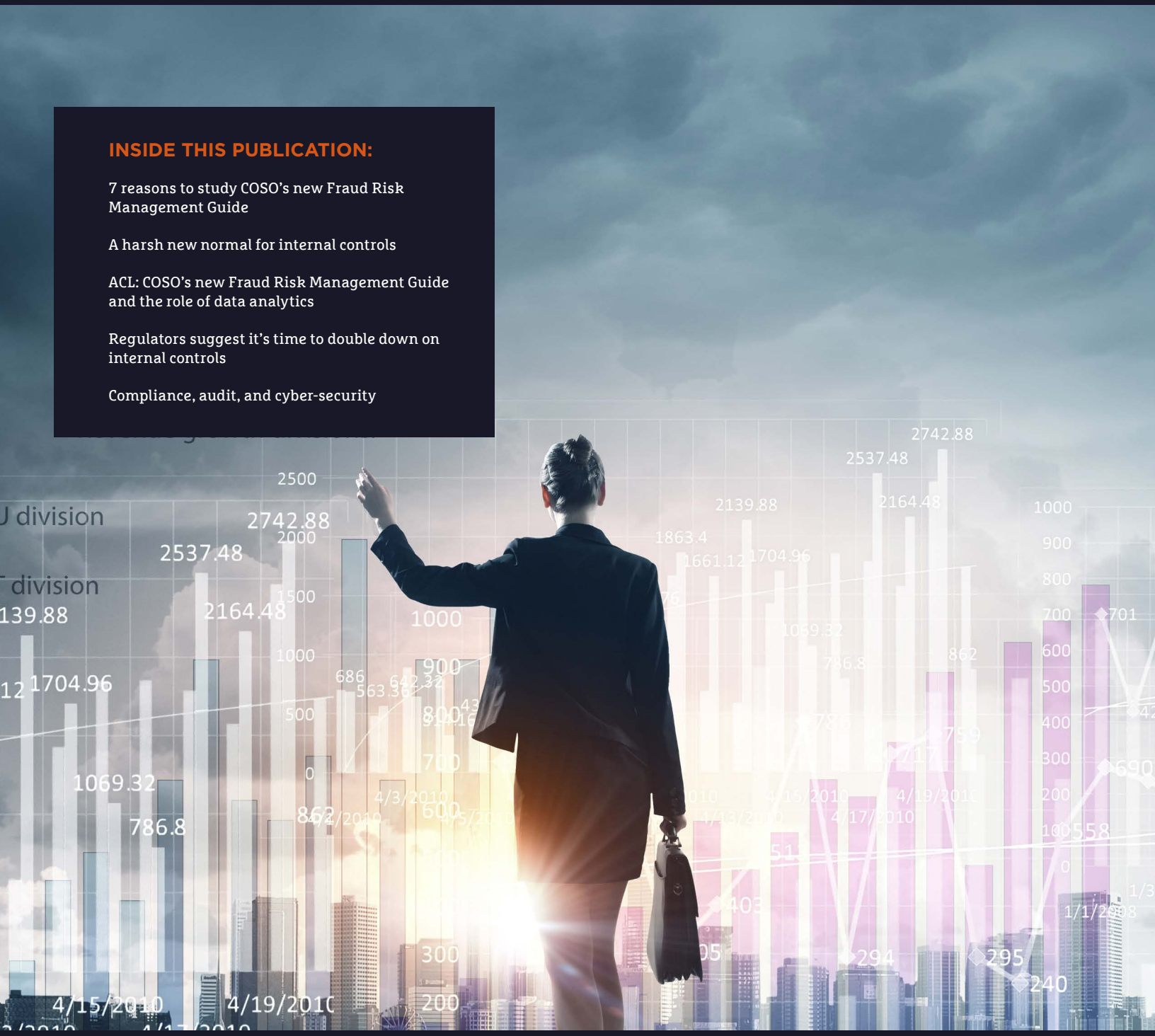
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

7 reasons to study COSO's new Fraud Risk Management Guide

A harsh new normal for internal controls

ACL: COSO's new Fraud Risk Management Guide and the role of data analytics

Regulators suggest it's time to double down on internal controls

Compliance, audit, and cyber-security

Technology's Emergence Into the

World of Internal Controls

An e-Book publication sponsored by acl™

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

ACL delivers technology solutions that are transforming audit, compliance, and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and compliance management professionals so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and compliance, and are used seamlessly at all levels of the organization, from the C-suite to front-line audit and compliance professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 30 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Visit us online at www.acl.com/compliance-management

Inside this e-Book

7 reasons to study COSO's new Fraud Risk Management Guide 4

A harsh new normal for internal controls 6

ACL: COSO's new Fraud Risk Management Guide and the role of data analytics 8

Regulators suggest it's time to double down on internal controls 10

Compliance, audit, and cyber-security 13

7 reasons to study COSO's new Fraud Risk Management Guide

Tammy Whitehouse says public companies would be wise to study COSO's new guide, because it could become a requirement.

No, COSO's recently published Fraud Risk Management Guide is not mandatory, but there are some compelling reasons audit committees and compliance officers should study and consider it—perhaps most importantly because it could eventually become a *de facto* requirement.

COSO, the same collaborative organization that authored the Internal Control—Integrated Framework that provides the most widely accepted path to Sarbanes-Oxley compliance, published the new fraud guide to elaborate on the 8th principle required under the IC framework. That's the principle that says the organization has considered the potential for fraud in assessing the risks to the achievement of objectives.

COSO updated its internal control framework in 2013, sending companies back into internal control documentation to assure they complied with the latest standards. It's a slippery slope, as the fraud guide is just published, to assert it could fall under the internal control umbrella and become part of Sarbanes-Oxley compliance, but experts say it's a possibility companies should not ignore.

So at the risk of creating a checklist, a tool that can raise eyebrows in audit circles these days, here is a list of seven reasons why companies should take a closer look at COSO's new Fraud Risk Management Guide.

7. Firms with anti-fraud controls suffer lower losses under faster detection. The Association of Certified Fraud Examiners says in its *2016 Report to the Nation* on occupational fraud and abuse that the presence of anti-fraud controls correlates with lower fraud losses and earlier detection of fraud schemes. Losses were 14 percent to 54 percent lower where organizations had specific anti-fraud controls in place, and frauds were detected 33 percent to 50 percent more quickly, the report says. An earlier 2015 global fraud report says as many as three-fourths of all companies fell victim to fraud in some fashion in the past year.

6. The guide represents the latest thinking and technology around how to combat fraud. COSO's new fraud guide is an update of the 2008 Managing the Business Risk of Fraud guide, providing a more modern approach to how to detect and prevent fraud, says Chuck Landes, vice president at the American Institute of Public Accountants. "It's been updated to reflect a lot of new anti-fraud techniques that fraud examiners are using these days," including fast-developing new technology such as data analytics, he says.

5. The new guide represents a united front, produced by several different organizations that approach the issue from different angles. COSO is sponsored by five different organizations, including the AICPA, the Institute of Internal Auditors, Financial Executives International, the Institute of Management Accountants, and the American Accounting Association. The ACFE participated heavily in producing the new guide with COSO, capturing the entire financial reporting chain, says COSO Chair Bob Hirth. "There's a lot of efficiency in having all those groups and all those functions involved in producing this one guide," he says. "We're all rowing in the same boat."

4. It's not just for big companies. The guide is nearly 150 pages in length, but that doesn't mean every page applies to every organization or every circumstance. "Tremendous efforts have been made to make the guidance scalable," says Toby Bishop, an independent forensic accountant with a Big 4 background, who was on the task force that helped with

the guide. "Even the smallest organizations can implement it, so they can take advantage of the sophistication of best practices, but without having to produce telephone-book-size documentation to support it."

3. The interactive tools and templates are pretty cool. Companies don't have to buy the complete guide to do the simplest, high-level assessment of their fraud risk to get a sense of where they may have weaknesses. Interactive scorecards assess existing components of a company's current fraud risk management approach to expose holes. An interactive tool summarizes and explains the various data analytics tests that can be integrated into a company's fraud approach. Ready-to-use spreadsheets help set up a risk assessment, a follow-up action plan, and documentation.

Sandra Johnigan, another independent forensic accountant with a Big 4 background, says she's encouraging skeptics to at least complete the initial scorecards to assess the current fraud program. "If you come up green all around, great," she says. "If you have a lot of yellow and red, maybe you need to step back and think about doing more of a program, than you thought you needed to do."

2. External audit of financial statements could be more efficient. Johnigan says it's possible auditors who dig into a firm's internal controls and see controls in place inspired by the fraud guide will consider that in planning their audits and selecting test controls. "Obviously, the stronger the control environment you have, the more identifiable your prevention and detection controls are that you can assess, and the more you can rely on them if they are effective," she says. "That's the way risk assessments work, both from the audit perspective and the company perspective."

1. Auditors might even regard the guide as an extension of the COSO IC framework. Here's where the slope to a possible *de facto* rule starts to get slick. Those that adopted COSO's internal control framework as updated in 2013 may have hit some rough patches with auditors in asserting compliance with the 8th principle that explicitly addresses the risk of fraud.

It became clear during implementation, says Bishop, that firms and auditors need specific guidance on how to address fraud risk under the updated approach to internal control. "Fraud specialists were seeing what is politely called a wide diversity of practice," he says. "Other people might consider it a scary nightmare if you believe in preventing fraud. Bringing greater consistency and quality to the implementation of fraud deterrence and detection was a huge need."

Bruce Dorris, vice president and program director at ACFE, says he not only believes it's possible auditors will expect companies to follow the new guidance, but he expects it. The guide is designed to expand on the fraud aspect of the internal control framework, he says. That's the same framework companies are widely expected to follow to comply with Sarbanes-Oxley.

"It certainly opens the door to what best practices are" in terms of companies asserting they have controls in place to address fraud risk, says Dorris. "It's going to open up a dialogue between audit, compliance, and management."

Timothy Hedley, a partner in fraud risk management services at KPMG, says it's too soon to say whether auditors will expect companies to incorporate the guidance into their internal controls for SOX reporting purposes. "We like to see companies do as much as possible with respect to mitigating the risk of fraud and other types of misconduct, but the way we conduct audits is driven by professional standards and the expectations of the Public Company Accounting Oversight Board," he says. ■

"There's a lot of efficiency in having all those groups and all those functions involved in producing this one guide. We're all rowing in the same boat."

Bob Hirth, Chair, COSO

A harsh new normal for internal controls

As auditors require more information and firms push back against what they feel are excessive demands, a consensus that works for everybody remains elusive. **Tammy Whitehouse** has more.

Signals are mixed on whether companies have made any head way in meeting auditors' requests for documentation in a way that will satisfy regulators, most notably the Public Company Accounting Oversight Board. Auditors say enhanced dialogue is producing greater understanding of what has to be done; though, preparers say it's too soon to suggest any kind of consensus has formed.

In 2015, after a few years of blistering audit inspection findings, companies began buckling under increased audit demands for documentation, especially around internal control over financial reporting. Some started getting more vocal and pushing back. That produced some high-level dialogue toward the latter half of the year bringing together the PCAOB, the Securities and Exchange Commission, representatives of the U.S. Chamber of Commerce and Financial Executives International, and the major audit firms.

"I do think we've made progress," says Trent Gazzaway of Grant Thornton. "Everyone involved has been talking a lot. We've been learning. The regulators have been learning. Now we're starting to get to a little bit of equilibrium or status quo."

Early on, the focus was on assuring the right controls were in the scope of internal control assessments and auditing. Now the focus is on assuring assessment and testing are occurring at the right level of precision to address misstatement risk. "As we get better in certain areas, the questions get harder," says Sara Lord, RSM national director of assurance services. "So we continue to move forward and continue refining."

Tom Quaadman, senior VP at the Chamber's Center for Capital Markets Competitiveness, called it "uneven progress." By the time talks got under way in 2015, audit planning for 2015 year-end audits was already well in hand. "Different firms may be in different places," he says, "but it's a matter of continuing this dialogue to get it on an even keel. We've seen progress, but it has been at an uneven level."

That's similar to what the FEI found when it conducted an internal poll of its Committee on Corporate Reporting. More than 70 percent of CCR members said they saw yet another increase in the latest audit cycle in audit demands for evidence and documentation, says Erik Bradbury, professional accounting fellow at the FEI. Likewise, 70 percent said they believed auditors were asking for audit documentation that exceeded what management believed was necessary for them to produce to comply with SEC management guidance on internal controls.

But that suggests roughly 30 percent of members are not experiencing what they consider to be excessive audit demands. "There's still a lot of tension in the system right, but it's mixed," says Bradbury. "It speaks to how individual some of the audits can be. There are still quite a lot of judgment calls being made by audit partners and audit staff, and that means every single audit is truly different and unique."

The SEC and PCAOB have suggested companies having challenges with their auditors over documentation or evidence demands should elevate the discussion to the engagement partner and perhaps even the national office. That's a great idea, but not easily done, says Laura Phillips, a member of the FEI's CCR who has led an ad hoc working group on internal controls.

Some might sense conflict across dozens of controls, so the preparer community is wrestling with exactly what questions to elevate through the audit firm. "I would suggest if you think you're in that position, pick just a couple that you think are representative and spend time focused on just those couple," says Phillips. "That might be enough to break the log jam."

One of the big challenges for firms, according to Bradbury, is the time it takes for information to flow from PCAOB inspection results through the information supply chain to the internal control owners who have to adapt to new demands. "Unfortunately, they're at the end of the compliance funnel," says Bradbury.

The FEI and the Chamber have asked the PCAOB and SEC to consider forming some kind of task force, bringing together all the relevant parties to formalize and hasten the information exchange. Neither the SEC nor the PCAOB have said directly whether they like that idea. The PCAOB said through a spokesman that they've met with CCR members and others and consider the dialogue helpful. "We will continue to welcome these meetings and consider insights obtained in light of our investor protection mission," said spokesman Colleen Brennan in a statement.

In a speech from Wesley Bricker, a deputy chief accountant at the SEC, he said the staff has heard some indications that the situation is improving, but that there's still more work to do. He acknowledged the dialogue in late 2015 likely followed the audit planning and documentation that had already occurred for year-end reporting purposes.

Bricker encouraged auditors to dialogue early and often. He also issued a strong reminder that internal control is management's responsibility. "The ICFR auditing issues identified by the PCAOB may not be just a problem of audit execution but rather, at least in part, indicative of deficiencies in management's controls and assessments," he said.

Pat Voll, vice president at RoseRyan, says she sees more discussion occurring and more push back. "Companies are requesting more dialogue," she says. They're saying, 'we understand your regulator is asking you to do this, but what does it mean to me? We believe we are already giving you enough'."

Protiviti EVP Brian Christensen says the survey results suggest firms are acknowledging improvements in ICFR. "Auditors and companies are conforming to these expectations and realizing this is the new reality," he says. "If anybody was hoping they were going to see something that would offer them a lesser or less rigorous response, that's not on the drawing board. It's not something we're going to see in the future." ■

IMPORTANCE OF ICFR

Below is an excerpt of a speech by SEC Deputy Chief Accountant Wesley Bricker on the importance of internal control over financial reporting.

ICFR remains a significant area of focus not only for OCA but also for our colleagues in the Divisions of Corporation Finance and Enforcement. A recent enforcement action against an issuer and several individuals, including company management, the company's auditors, and a company consultant, for deficient evaluation of the company's ICFR, demonstrates our coordinated efforts related to ICFR as well as some of the challenges that remain in this area. From my perspective, there are three important takeaways from that case:

- The first is that management has the responsibility to carefully evaluate the severity of identified control deficiencies and to report, on a timely basis, all identified material weaknesses in ICFR. Any required disclosure should allow investors to understand the cause of the control deficiency and to assess the potential impact of each for disclosure as a material weakness.
- The second is the importance of maintaining, or augmenting with, competent and adequate accounting staff resources to keep books, records, and accounts that accurately reflect the company's transactions and to maintain internal accounting controls designed to ensure that company transactions are recorded in accordance with management's authorization and in conformity with GAAP. Qualified accounting resources will be of vital importance in connection with the adoption of the new accounting standards that I mentioned earlier.
- And finally, management has to take responsibility for its assessment of ICFR. That responsibility cannot be outsourced to third party consultants. At the same time, third party consultants have obligations to uphold when assisting management in its evaluation of ICFR.

Source: Securities and Exchange Commission

COSO's new Fraud Risk Management Guide and the role of data analytics

COSO's most recent publication on managing fraud risk is a very welcome document. One of several reasons for its usefulness is its specific mention of the role of data analytics. The new COSO Fraud Risk Management Guide establishes five principles for managing the risks of fraud and links them to the five components of the 2013 Framework for Internal Controls, as well as the 17 Internal Control Principles.

The five elements of guidance on establishing a fraud risk management program include:

1. Establishing fraud risk governance policies
2. Performing a fraud risk assessment
3. Designing and deploying fraud preventive and detective control activities
4. Conducting investigations
5. Monitoring and evaluating the total fraud risk management program

The role of data analytics in fraud risk management

It seems to me that data analytics have a valuable role to play within each of the middle three elements. Companies vary considerably in terms of how and where they use data analytics in risk management overall. Some are quite advanced, while the majority are in the early stages of use. The following are some of the ways I have seen organizations, both large and small, use data analytics in some aspect of managing fraud risks.

Risk assessment: Data analysis can be used to examine massive volumes of data and activities within entire business processes in order to assess fraud risk and provide indicators of where the most likely risks of fraud exist. Current analytic technologies can profile data in multiple ways and provide powerful visual indicators of financial and operational business activities that are anomalous and likely to be a problem. They can detect potential fraud at a detailed level around specific transactions, or in terms of general trends relating to, say, a regional office or business unit manager—raising red flags about something does not make sense and warrants closer attention.

Testing controls: Data analytics can be used to detect instances in which fraud prevention controls have been bypassed or failed, as well as instances in which fraud has occurred and for which no controls were in place.

Controls may be designed, for example, to ensure that every new vendor set up in a purchase-to-pay system is legitimate and that every purchase and payment is approved by an appropriate individual. But no control system is perfect. There may be flaws in the design that allow fraudulent workarounds to occur. Data analysis can quickly determine if, despite the controls that are meant to be in place, controls are ineffective. What if a new vendor is established and approved without proper segregation of duties—and is actually a phantom vendor controlled by an employee? What if a manager approved a whole series of purchase orders and payments just under their approval limit, so that in total a very large fraud took place? Suites of analytic tests can be implemented that regularly test all types of transactions—in multiple ways—to test control effectiveness.

Preventive measures: Data analytics can help to prevent fraud from occurring in the first place—primarily when analytics are run at the time of transaction entry and initial processing. When red flags are raised, suspect transactions can be put on hold for further investigation. At the same time, the existence of control and transaction monitoring can itself play a role in fraud prevention if management and employees are aware of it and so think twice before acting in a fraudulent way. Tone-at-the-top and zero tolerance programs can certainly help to establish an anti-fraud culture. Letting everyone in an organization know that fraud prevention policies are backed up by constant monitoring of activities can do much to discourage all but the most determined fraudsters.

Fraud investigation: Data analysis can also be used very effectively in the investigation process in order to determine the circumstances of fraud and provide documentary evidence of the full nature and extent. While traditional techniques, such as whistleblower hotlines, may uncover specific

instances of fraud, analytics can rapidly expand an investigation to look for all related instances in a way that is not practically achievable through manual techniques. Smart analytics can find links and patterns in seemingly unrelated activities.

Corrective actions: Management can spend considerable effort in fixing and improving weak controls after fraud has been uncovered. The challenge is to determine whether the corrective actions have been successful. Again, analytics can be used to point out problems that indicate that corrective actions are still not effective.

Continuous monitoring: All of the data analytic techniques for examining and testing financial and other activities can be performed on an as-needed one-off basis. However, the use of data analytics in fraud risk management delivers the greatest benefit as part of an ongoing continuous monitoring and risk assessment process. Using traditional audit and fraud prevention techniques, instances of fraud are often uncovered years after they commenced. There are clear advantages when analytics uncover instances of fraud soon after they first occur, before they have been allowed to grow—preventing any further escalation.

Auditors have been doing this for some time...

It is apparent, when looking at these roles of analytics in COSO's five elements of fraud risk management, that they are actually very similar to the role of data analytics in various different stages of the internal audit process. In this context, analytics can be used to assess risks to support decisions as to what audits to perform. When planning a specific audit, analytics provide direction on where to focus audit activities. They can be used to test controls and perform substantive audit procedures, as well as to investigate initial findings and to support and quantify audit reports that are provided to management. They can also be used to determine the effectiveness of management's response to audit findings.

Who is responsible for fraud risk management analytics—which line of defense?

Clearly there is considerable overlap between the use of data analytics in fraud risk management and in internal audit. Of course, this is not surprising, as it really all comes down to the issue of who is performing the activities and with which responsibility. Direct responsibility for fraud prevention and detection controls presumably lies primarily with business and financial management—the first line of defense in the Institute of Internal Auditor's model. In some organizations, specific responsibility for fraud detection and compliance with fraud controls lies within specialist groups within the second line of defense. In others, it falls to internal audit.

Internal audit has been using data analytics to support multiple aspects of the audit process for many years. In many ways, they have been leaders in the use of data analysis for anti-fraud control testing, and have been advocates for extending the use of analytics into the first two lines of defense where, arguably, it makes most sense to perform ongoing monitoring and control testing. The most important thing—from an analytics perspective—is that someone is making use of data analytics and monitoring to address the risks and damaging effects of fraud

Why is it taking so long?

COSO, and its component professional bodies, have been doing great work over the years in producing their risk management and control frameworks. Personally, for many years I have been surprised—and disappointed—that there has been so little specific mention to date of the role that data analytics and related technologies can play in relation to these frameworks. So I can only be positive about the importance of COSO's specific inclusion of the role of data analytics in their new Fraud Risk Management Guide.

Within the past few years data analytics have done much to transform many critical aspects of business, from product design and management, through marketing and sales, to customer service. It is well past time that data analytics should be applied comprehensively to help transform fraud risk management processes.

JOHN VERVER, CPA, CA, CISA, CMC, ADVISOR TO ACL

John Verver, CPA CA, CISA, CMC is an acknowledged thought leader, writer and speaker on the application of data analysis technology in audit, fraud detection, risk management and compliance. He is recognized internationally as a leading innovator in continuous controls monitoring and continuous auditing and as a contributor to professional publications. He is currently a strategic advisor to ACL, where he has also held vice president responsibilities for product strategy, as well as ACL's professional services organization. Previously, John was a principal with Deloitte in Canada.

Regulators suggest it's time to double down on internal controls

The SEC and PCAOB are telling companies to get tougher on their auditors, reports **Tammy Whitehouse**.

After nearly a year of moderating corporate gripes of excessive auditing driven by regulatory inspections, regulators say the answer is for companies to double down on their controls and use a little more muscle with their auditors.

Representatives of the Securities and Exchange Commission and the Public Company Accounting Oversight Board say they have met with preparers to hear their detailed accounts of where they believe auditors made demands that didn't make sense. The U.S Chamber of Commerce initiated the sessions with particular concerns around the audit of internal control over financial reporting.

For at least the last few annual inspection cycles, the PCAOB has taken a hard line on auditors over their compliance with Auditing Standard No. 5, which governs the audit of internal control, as well as a group of newer auditing standards that give auditors some specific marching orders around responding to risks. Both are areas of concern at the PCAOB, where board members and inspection staff say some firms are making limited improvements, but compliance is still falling short.

Jim Schnurr, chief accountant at the SEC, said his monitoring of the outreach suggests the issues being identified by the PCAOB may not be entirely audit problems. "Rather, they may, at least in part, be indicative of deficiencies in management's controls and assessments," he said during prepared remarks at a recent national accounting conference, where an entire panel of regulators, preparers, and auditors explored how to work through the tension. He urged companies to take a closer look at their controls and initiate more dialogue with auditors to get to core issues.

The push by the PCAOB is prompting auditors to demand more audit evidence and more documentation, especially around management review controls, in ways that has left preparers scratching their heads. "Preparers are on the back end of the compliance funnel," said conference attendee Kevin McBride, global accounting and financial services controller at Intel. "We can't just wake up one day and find that everything is different. It's very difficult to evolve the control environment on a timely basis."

Susan Insley, vice president of internal audit at VMware, says she's seen a "drift" away from the top-down, risk-based approach to the audit of internal controls that is mandated under AS5. "We're moving away from reliance on management review controls and wanting an inclusion of a broader set of control activities rather than relying on the management review controls that are really important to the running of the business," she said.

Preparers still aren't entirely sure what they need to do to satisfy auditors, said McBride. "There is a lack of clarity on what exactly is sufficient in management review controls and their precision," he said.

That suggests some lack of understanding of why such controls are even in place or what they're intended to do, said Brian Croteau, deputy chief accountant at the SEC. "On a basic, fundamental level, it is important to understand the fundamental risks that any control is meant to address," he said. "In assessing internal control over financial reporting, management needs to understand and address the specific controls it has in place to address financial reporting risks. Not all management review controls

are created equal."

The same goes for auditors, said Jeanette Franzel, a board member at the PCAOB. "If management doesn't understand it, auditors' problems are compounded," she said. "The auditor needs this understanding of the flow of transactions, and the understanding of how controls fit into the flow of transactions, in order to properly apply the top-down, risk-based approach of AS5."

The auditor uses this approach to identify the entity-level controls based on risks of misstatement and then to select the controls to test, Franzel said. If auditors don't understand the flow of transactions and the controls to address risk, they won't get the evidence they need to properly support an audit opinion. "Auditors then compound their problems by relying on that as if it were effective and effectively tested to reduce their substantive testing."

This is where auditors get dinged by inspectors for not assuring controls are operating at the right level of precision. In response, auditors have placed less reliance on entity-level controls and tested controls at lower levels. The key question, said Helen Munter, director of inspections for the PCAOB, is to focus on whether the control can mitigate risk of misstatement by itself. "Is the entity-level control you selected sufficient to operate and be tested on its own and in isolation? Or does it in fact depend on the operation of another control?"

PwC Partner Mike Gallagher said the firm responded with more training and examples for auditors and tools to help guide their thinking around documentation and evaluation. Others have taken similar measures. "Having that consistency of performance, we've found, is a game changer, which has shown up positively in our inspection results," said Gallagher.

Croteau said AS5 and the SEC's interpretive guidance to management on internal controls are fully aligned on the issue of control precision. Representatives of neither the SEC nor the PCAOB suggested any change in regulatory approach is expected to address the ongoing tension.

Rather, the SEC and PCAOB are encouraging preparers who are still stumped by auditor demands to assure plenty of dialogue, as early in the process as possible, and to push back on why auditors need the evidence or documentation they request. "In all of our outreach, this is one of the most important things that has come out of the tension," said Franzel. "It's a lack of understanding between auditors and management. If an auditor says we have to, think about why. Does the auditor not understand your controls? Is the auditor taking the lazy way out? That's not an acceptable response."

Insley said she is encouraged by the dialogue she's seen so far, though she is wary about auditor use of templates and whether some auditors may follow them blindly like checklists. Gallagher urged preparers to press auditors if their actions don't make sense in the context of the company's control environment. "I worry about any professional who can't articulate the why," he said. "If that's the answer you're getting from the auditor, talk to someone in the organization who can give you an answer that makes sense." ■

"We're moving away from reliance on management review controls and wanting an inclusion of a broader set of control activities rather than relying on the management review controls that are really important to the running of the business."

Susan Insley, VP of Internal Audit, VMware

Reduce the Cost & Burden of SOX/ICFR Compliance

SOX isn't going away, you won't be getting more staff, and regulators are getting tougher with expectations—technology is the one lever you can use to alleviate your SOX compliance burden.

ACL's comprehensive compliance platform reduces the burden of compliance with a data-driven approach to managing end-to-end-processes. Manage your 404 and 302 certification obligations and ensure proper governance of internal controls over financial reporting with data analytic and workflow management software.

ACL's Compliance Management Solution helps you:

- Map regulatory requirements to your control framework
- Validate internal controls effectiveness
- Streamline policy attestation
- Identify, remediate and track issues
- Create comprehensive actionable reporting
- Continuously monitor the vast amount of data flowing through your organization
- Lower external audit fees

acl™

Visit acl.com/compliance-management to learn more about taking a centralized approach to compliance management.

Compliance, audit, and cyber-security

Matt Kelly explores three ideas for merging cyber-security into your compliance and audit programs.

Cyber-security has become a paramount issue for all CCOs these days. The good news is there is already plenty of strong theory and practice surrounding the issue. Let's take a look at some best practices.

First, worry more about the process of how information is governed at your business than about the tools you use to protect it. Tools address one specific risk, and they may do that quite well—but they may also be useless for every other risk. And if your process for governing information is sloppy overall, those other risks will hit you eventually.

I always favor analogies from the real world, so try this one: At some point in life you might suffer a heart attack. You can go through life equipped with tools to reduce that risk, such as a defibrillator, and it will indeed help when the time comes. Or you can improve your process of being healthy: eating right and exercising. Neither one of those procedures will assure that you never have a heart attack—but they will help you stay alive should a heart attack come to pass.

Good tools without good process is the equivalent of carrying around a defibrillator while you overdose on salty foods. Does that sound like a good strategy for preventing heart attacks to you?

Second, define the roles for managing cyber-security risk. The Three Lines of Defense Model is my default for any conversation about who oversees what part of a risk. Internal auditors have things a bit easy: You're in the third line as usual, testing the security procedures and controls like you would any other.

The first and second lines of defense get more complicated. Clearly IT (or the IT security function, if you have a separate one) belongs in the second line. Compliance does too. But each one supports the business units, bravely holding down the first line of defense in different ways. My first point above, to worry more about process than tools, still holds true—but you do need both tools and process to have effective cyber-security: IT supporting the tools to fight cyber-security risks, compliance supporting the processes.

For business units to follow effective processes, compliance needs to do its job in the second line defining those processes. They might be policies to have third parties certify data security, or procedures for data breach disclosure. But the business units can't follow a good process unless compliance does its job spelling out the policies that govern that process.

The third point, and perhaps the most heartening, is that Corporate America has faced a mess of poor controls and poor understanding of risk before—and we solved the problem. Think Sarbanes-Oxley.

Several times I've heard management worry about weak processes, but then add, "unless it's a SOX process, because our SOX processes are generally strong."

Study the parallels between SOX compliance and cyber-security, because they're vital. A huge amount of cyber-security risk hinges on access: ensuring that only authorized users can access certain data. That is the same worry compliance and internal auditors have about access control to financials—and you've been testing your access controls for financial data for the better part of a decade. Drop the word "financial" from my last sentence, and you have your marching orders for cyber-security risk. That's the goal.

You can even make an intellectual leap from SOX compliance back to the importance of a strong process. When you read through the 17 guiding principles of the updated COSO framework, those principles are all about strengthening your process. COSO intended the framework to be a roadmap for internal control over many risks, cyber-security included.

So as scary as cyber-security might be right now, it can be conquered. If the compliance and audit community tamed SOX, you're in prime fighting shape for this threat too. ■