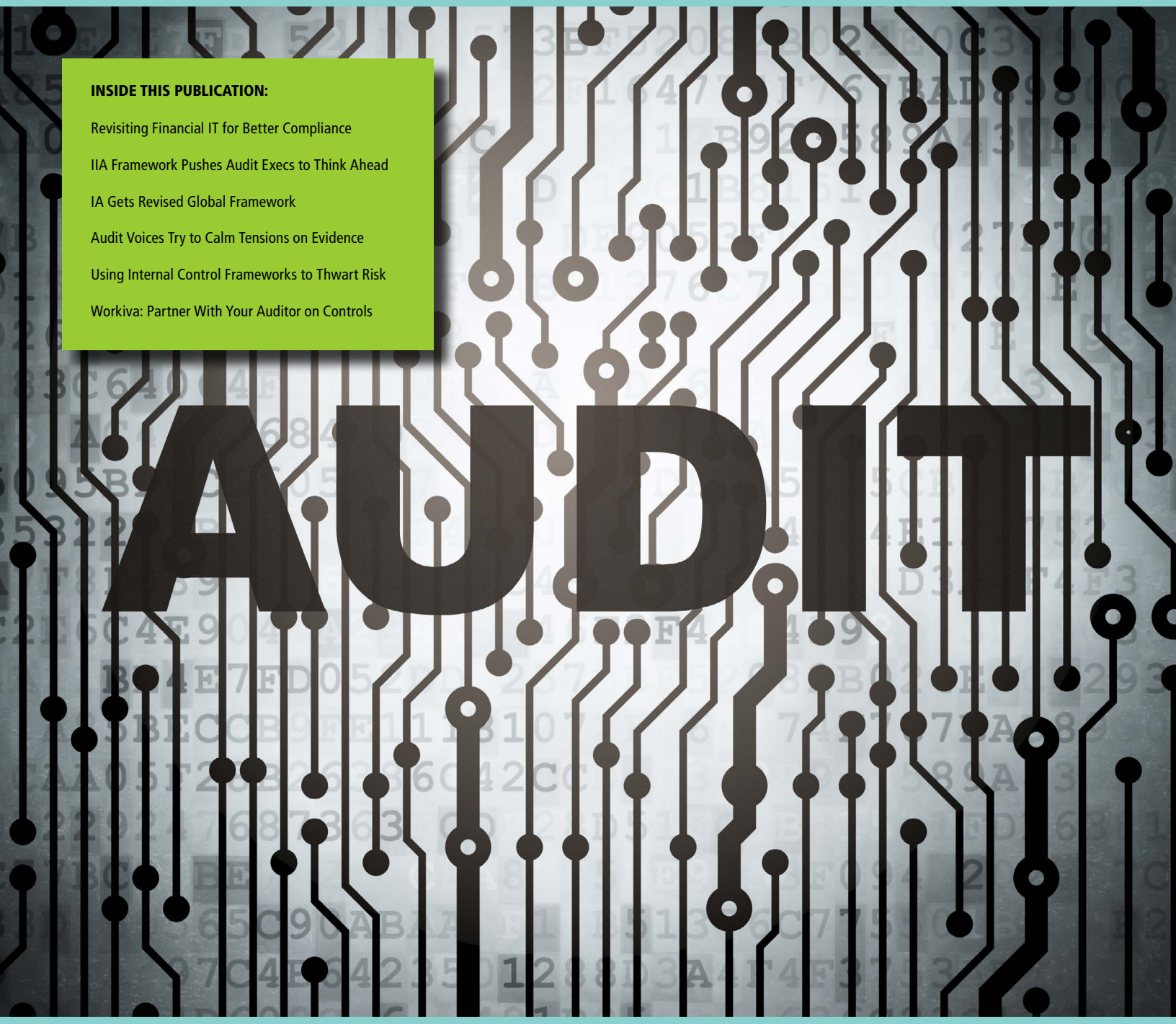
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Modern Technology: Changing

The Face of Audit

An e-Book publication sponsored by Workiva Wdesk

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.

Workiva (NYSE:WK) created Wdesk, a cloud-based productivity platform for enterprises to collect, link, report, and analyze business data with control and accountability. Thousands of organizations, including over 65% of the 500 largest U.S. corporations by total revenue, use Wdesk. The platform's proprietary word processing, spreadsheet, and presentation applications are integrated and built upon a data management engine, offering synchronized data, controlled collaboration, granular permissions, and a full audit trail. Wdesk helps mitigate enterprise risk, improve productivity, and gives users confidence to make decisions with real-time data. Workiva employs more than 1,200 people with offices in 16 cities. The company is headquartered in Ames, Iowa. For more information, visit workiva.com.

Inside this e-Book:

Revisiting Financial IT for Better Compliance

Advanced IT to improve monitoring and testing exists, but integrating those solutions into corporate data warehouses and business operations is harder than first thought

by Tammy Whitehouse

With a steady rise in risk and volatility in the modern global economy, companies are dialing up their adoption of technology solutions to manage their monitoring and testing in risk, compliance, and control activities—or at least, they are trying to.

"We are seeing more companies moving to integrated controls," says Joe Howell, executive vice president at Workiva. Companies with only partially deployed ERP systems are starting to take a fresh look at what they can do with the software they have, he says.

"People love IT, but it may have been expensive, complicated, or required a lot of IT involvement to fully implement," he says. "It took a lot of discipline to get them up and running. Now there's pressure to rethink that. Even though it's expensive and complicated, people are drawn back to use them."

Interest in advanced or automated monitoring and testing solutions is accelerating, says Jerry Stone, a partner with PwC and leader of the firm's compliance services. A recent PwC survey showed roughly 60 percent of CEOs saw more business opportunity on the horizon in the next three years—and the same percentage also said they saw more risk. "That balance is what companies are looking at," he says. "How do I pursue opportunities in a world that is changing at a greater pace? How do I grow but have the right balance of infrastructure, and therefore monitoring and proactive feedback?"

That same PwC survey said roughly two-third of chief executives expect significant regulatory change over the next five years. "Organizations are responding to the environment, and that environment includes an increase in regulatory complexity," Stone says. Monitoring and testing solutions give compliance and risk officers more timely feedback on their processes, and more sustainability to that feedback. "So they can move more nimbly into some of the growth areas that are presented by advances in technology and globalization."

> "That balance is what companies are looking at. How do I pursue opportunities in a world that is changing at a greater pace? How do I grow but have the right balance of infrastructure, and therefore monitoring and proactive feedback?"
>
> Jerry Stone, Partner, PwC

Dan Kinsella, third-party assurance solutions leader for Deloitte Advisory, says many compliance operations are outfitted with modern monitoring and testing solutions, but haven't found them to be the cure-all people expected. "There was this view that this would be panacea of the future, that this was going to do all of this automagically," he says.

Not so much magic has arrived yet. Companies have implemented lots of systems, and systems technology is improving, but the idea of "master data management" is still somewhat elusive for many companies.

"Ten or 15 years ago, you may not have had the right data to make decisions," Kinsella says. "Now you have too much data to make the right decisions." Now companies are starting to make more use of automated controls and automated analytics to meet varied reporting requirements and achieve some efficiency, he says, especially in the more heavily regulated sectors like financial services, health sciences, and energy.

Getting to a Good ROI

The technology has developed to a point where it tends to provide a good return on investment, says Gary Sturisky, national consulting leader for McGladrey. "We've seen a significant migration toward automation to get efficient and drive down the compliance cost," he says. "Compliance for the most part has become somewhat mature. When you look at the repetitive, known aspects of it, companies are looking for ways they can draw down the costs."

The bad news: Those bucks will still be a significant investment, says Warren Stippich, partner and national GRC leader for Grant Thornton. He warns that organizational challenges will still flummox lots of companies. "It's where we need to get as a profession focused on risk, compliance, and controls," he says. More advanced technology is the "poster child" for optimizing the compliance function.

MONITORING TRENDS

Below, the IIA examines to what extent companies are automating, monitoring, and testing solutions.

The Institute of Internal Auditors' Global Internal Audit Common Body of Knowledge (CBOK) Practitioners Survey says 44 percent of respondents globally — more than 14,500 — report moderate or extensive activity for continuous/real-time auditing. It is not clear how many combine this with continuous/automating monitoring.

The IIA's GAIN survey, which includes information from internal audit functions at 479 organizations including 315 in the United States, found 62 percent of respondents use computer-assisted audit techniques, while 33 percent report performing continuous auditing.

Source: The Institute of Internal Auditors

"How do you look at the risk and compliance environment and test it with a lot more efficiency?"

Miklos Vasarhelyi, professor of accounting information systems at Rutgers University, has been studying the development and use of continuous auditing and continuous monitoring solutions for more than 20 years. "I used to tell students: Everyone uses computers, so everyone will use this information technology to audit in five years," he says. "All these years later, never underestimate the time it takes for companies to adopt modern technologies."

Research shows that firms still have cultural constraints to consider in how to move professionals into modern methods, he says, but companies are gradually making the move. "The whole idea of manual audit has become very close to preposterous," he says. "The idea of sampling on huge populations is very procedural. It is an old-fashioned view of the world."

It's been a long haul for a variety of reasons, says Sandra Richtermeyer, accounting professor at Xavier University who studies accounting systems. Many companies have invested in a significant IT infrastructure and robust control processes, but they struggle with integration, she says. "What about an enterprise system that only utilizes 20 percent of its capability?" she says. "That's what I hear a lot. They may have all these really cool islands of technology, but they don't speak to each other."

Richtermeyer also sees companies with ERP systems that have the capability for customized monitoring, but they haven't found the time or staffing expertise to deploy those capabilities well. Companies also struggle to some extent with having controls around monitoring systems. "As some companies become more complex in their business model or they are expanding, their comfort in using something automated may go down," she says. "It's monitoring the monitoring, or putting processes around processes."

Companies are working through some of those adoption challenges by taking a pilot approach, Stone says. "There isn't a lot of resistance to the need to have more sustainable monitoring in place," he says. "So companies are looking at the practical aspects of piloting and how to implement in a way that makes sense." Companies typically turn to their risk assessments to determine where to prioritize their adoption of new technology, he says. "Organizations need to measure that business priority like any other business priority and put it on a scale around everything else they're doing." ■

QUESTIONS TO ASK

Below is a sample of questions that PwC says companies should ask themselves:

1.What is your strategic posture—for now and the future?
- » Do you operate in global markets or plan to?
- » Do you operate in emerging markets or plan to?
- » Are you expanding the diverse markets in which you operate?

2. What are your needs, strengths, and weaknesses around controls monitoring? Is there a desire to get to the next level?
- » Is your company required to have controls monitoring activities?
- » Do you currently have recurring controls monitoring activities in place? If not, is there a need or desire to establish those activities?
- » Are there opportunities to enhance risk coverage through better coordination of your controls monitoring?
- » Do you effectively leverage your data (both structured and unstructured) to maximize automated monitoring?
- » Is the organization open to evaluating outsourcing approaches and improvement strategies?

3. What is your level of risk maturity?Are you an early-stage organization that still needs to put the basic elements of risk management in place?
- » Are you a developing organization looking to better link your business and risk strategies?
- » Are you an organization with mature risk management and corporate compliance systems but with a need for improvements around monitoring and testing of processes and controls?
- » Are your needs broad based or tightly focused? Are you seeking to alleviate stress points in your infrastructure by redistributing specific responsibilities?
- » Are you seeking to better utilize technology to more effectively automate your risk processes?

4. Could a restructured approach offer opportunities to optimize your controls monitoring?
- » Is there an opportunity to centralize controls monitoring activities to drive quality, maximize the use of data, control costs, and achieve greater economies of scale?
- » Could enhanced coordination and consistency in testing approaches provide opportunities for greater efficiency and effectiveness and drive more-reliable testing results?
- » Is there a desire to leverage a long-term, sustainable solution rather than a one-time controls monitoring project?

5. Are you looking for opportunities to reduce the cost of compliance?
- » Are there opportunities to better centralize and standardize your monitoring and testing activities to save costs while improving quality?
- » Are your resources stretched or at capacity—without the flexibility to handle changes to your risk and controls environment?
- » Are there issues with turnover in the controls monitoring functions?

Source: PwC

IIA Framework Pushes Audit Execs to Think Ahead

The Institute of Internal Auditors has unveiled its new professional practices framework, guidance intended to drive auditors to think critically about risk management and organizational improvement

by Tammy Whitehouse

For internal auditors who haven't yet seen the writing on the wall calling them to a more modern approach to practice, leaders in the profession have taken measures to make the writing more explicit.

At its recent annual global conference, the Institute of Internal Auditors layered over its entire professional practices framework a new mission and 10 core principles that are meant to point internal auditors in that new direction. The new International Professional Practices Framework emerged at the same time as a five-year IIA study of the profession that suggests many internal auditors already understand the need to steer themselves in that way, lest they be left behind.


Harrington

"The world is changing at light speed," says Larry Harrington, chairman of the IIA global board of directors and head of internal audit at Raytheon. "Risks are changing on a daily basis. Stakeholder expectations at the board and regulator level are raising the bar. They want us to be an integral part of understanding risk."

The IIA's revised professional practice framework is not a regulatory requirement, simply an urging from the profession's leaders calling internal auditors to a higher level of practice. It states the mission of internal audit as enhancing and protecting organization value by providing risk-based and objective assurance, advice, and insight. It tells internal auditors to embrace core principles that in some cases are already contained in existing standards, but in others are not so clearly articulated.

Core principles focused on integrity, competence, communication, positioning, resources, and due professional care, for example, might already be standard-issue for many internal auditors today. "When you look at the core principles, certainly the first eight, in my mind, are very much what many good internal audit functions do today," says Hal Garyn, vice president at the IIA.

A handful, however, may stretch the typical internal auditor beyond his or her comfort zone. For example, internal auditors should be "insightful, proactive, and future-focused," and should "promote organizational improvement," according to two of the principles.

"That's an area where some internal audit functions may have to say, 'I need some guidance on what that might mean,' " Garyn says. "That's not necessarily where every internal audit function is today."

The IIA's latest "Global Pulse" study seems to suggest such guidance won't come as a shock to internal auditors globally. The report says internal auditors around the world recognize that they need to develop more forward-looking risk-management practices and that they need to anticipate the needs of stakeholders.

That clearly ties back to the new framework guidance, Harrington says. "It's about making sure we understand the changes taking place in business and technology and learning to use those to our advantage," he says. "We must learn to invest in ourselves with the world changing so quickly."

Sridhar Ramamoorti, associate accounting professor at Kennesaw University, says the enhanced framework directs internal auditors to get more in tune with "leading" indicators of risk rather than focusing on "lagging" indicators. "The leading indicators are extremely important signals of risks that may be coming down the pike," he says. "Lagging indicators only tell you about risks that have already materialized and hit the financial statements."

Putting the Practice Framework Into Practice

Tom O'Reilly, director of internal audit at technology company Analog Devices, says he was a bit skeptical at first as he learned about the newly enhanced framework, but changed his mind upon closer examination. Some of the principles can serve as easy benchmarks for how his internal audit department is functioning, he says. "It's another source to help me tactically verify whether the work my department does is best positioned to enable positive change for our company," he says.

O'Reilly pointed to the principle saying internal auditors should be insightful, proactive, and forward-looking as a challenge to the way many internal audit departments function. "If internal auditors are performing more management roles such as Sarbanes-Oxley testing, it's going to be hard to be future-focused," he says.


O'Reilly

Other exercises often performed by internal audit that ideally should be performed by management, O'Reilly says, include verifying inventory or having responsibilities for risk management, security, or monitoring a company's whistleblower hotline. "The more we do that, reacting to events that have happened, we won't be future focused," he says.

Mark Kultgen, national leader of the internal audit and SOX practice at McGladrey, says audit executives should first use the framework as an educational tool internally. He suggests pointing out that the guidance is consistent with the direction of the 2013 COSO Internal Control—Integrated Framework, which provides a heightened focus on entity-level controls and IT controls.

"Personally, I'd perform a self-assessment around the principles and use it as a discussion point with the audit committee and management," he says. "Get their sense. Do they see internal audit as having that degree of independence? Are we aligned with strategies and objectives?"

Andy Dahle, a risk assurance partner with PwC, says chief audit executives should react to the new guidance by taking a serious look at what they're doing and how they could move internal audit further into a leadership role. He suggests using the new guidance as a trigger for new discussion with audit stakeholders about where internal audit can do more, while also using it to ignite the internal audit staff. "Use this as a motivator to drive change within the department," he says. "Help them buy into the mission that internal audit has to be more than it was yesterday."

> "Risks are changing on a daily basis. Stakeholder expectations at the board and regulator level are raising the bar. They want us to be an integral part of understanding risk."
>
> Larry Harrington, Chairman, IIA

Pundmann

It might be a tough sell either within the department or with audit stakeholders, depending on how bogged down the internal audit staff is with SOX control testing, for example, or how stretched it might be for resources. Sandy Pundmann, a partner in internal audit and strategic risk for Deloitte, advises chief audit executives to use the framework update as leverage in discussions about resources.

"You have to be transparent with senior executives, boards, and audit committees," she says. "Here are all the risks of the organization. With my current funding and resources, if all I'm doing is Sarbanes-Oxley, all I'm covering are financial risks. I'm not focusing on operational or strategic or compliance risks. That's a huge white space that isn't being covered."

If that's still a tough sell—after all, the guidance isn't mandated by any regulatory body with authority to enforce it; it is simply provided by a professional body trying to raise the bar on its practice—then the progressive chief audit executive has a bigger issue to consider, says Warren Stippich, a partner and national GRC leader at Grant Thornton. "Professionalism is at hand here," he says. "If they say, 'We don't care about this because there's no law,' that begs higher-level questions for me; then you have to ask: Would I want to work for an organization like that?" ■

IA GETS REVISED GLOBAL FRAMEWORK

Below, CW's Tammy Whitehouse highlights some of the key changes to the Institute of Internal Auditors' International Professional Practies Framework.

The International Professional Practices Framework has been updated to try to strengthen the position of internal audit as a key player in the organizational structure, says Larry Harrington, Instiute of Internal Auditors global board chairman. "As we traverse an increasingly complex business environment, we must be clear what internal audit's mission is and underscore the basic tenets and principles that will continue to propel our profession forward," he said in a statement. The framework was last updated in 2007.

The Framework is a blueprint for how the body of knowledge and guidance for internal auditors fits together to support the professional practice of internal audit. It encompasses all the authoritative standards and guidance written by the IIA, which is a professional association that sets the standards for the profession.

A key update to the IPPF is the establishment of a mission for internal audit and the outlining of 10 core principles that should underpin the professional practice of internal audit. The mission of internal auditors under the new framework is "to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight."

A key update to the IPPF is the establishment of a mission for internal audit and the outlining of 10 core principles that should underpin the professional practice of internal audit. The mission of internal auditors under the new framework is "to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight."

The new core principles of the framework are meant to highlight what effective internal auditing looks like in practice, says the IIA, focusing on the individual auditor, the internal audit function, and the internal audit outcomes. The framework says internal auditors must demonstrate integrity, objectivity, competence, and due professional care, and must be proactive, insightful, and focused on the future.

The new framework also specifies that "practice advisories" will become a more comprehensive suite of "implementation guidance," and practice guides and global technology audit guides will be grouped as "supplemental guidance."

The IIA says the changes to the framework do not affect other key mandatory elements of the framework, such as the definition of internal audit, the code of ethics, or other professional practice standards, but standards will be evaluated and may need to be revised over time to support the recent revisions to the framework.

— Tammy Whitehouse

Audit Voices Try to Calm Tensions on Evidence

Leaders of the auditing world are calling for a truce in arguments between internal and external auditors over how much evidence external auditors should collect

by Tammy Whitehouse

Leaders of the auditing world are calling for a truce in the arguments between internal and external auditors over how much evidence external auditors should collect themselves while scrutinizing corporate finances and internal controls—and are calling on audit committees to intervene earlier as referees of those disputes.

That issue of how much external auditors can rely on the work of internal auditors was a running theme at the Institute of Internal Auditors' national conference, prompting the IIA and the Center for Audit Quality to urge that corporate audit committees get more involved in planning how internal audit and external audit can cooperate and avoid unnecessary duplication of audit effort.

"As often happens, when the regulator speaks, perhaps in some cases there can be an overreaction," Richard Chambers, president and CEO of the IIA, said.

The regulator in question is the Public Company Accounting Oversight Board. It spoke back in October 2013 through its Audit Practice Alert No. 11, which warned external auditors that their work on audits of internal control over financial reporting needed marked improvement. The PCAOB summarized inspection findings to call out numerous areas where inspectors found too many departures from professional standards, including reliance on the work of internal auditors.

The 25-page alert includes a few pages reminding auditors of their duty to consider risk when using the work of internal audit and to evaluate the competence and objectivity of internal auditors who performed any work that external auditors might rely on. "When using the work of others that provide direct assistance, the auditor should supervise that work, including reviewing the work, as well as testing and evaluating it," the PCAOB wrote.

Internal auditors say they have most definitely felt the consequences of that pronouncement. In an IIA survey to assess a variety of issues across the internal audit profession, 65 percent of internal auditors at public companies said they have experienced increased scrutiny from external audit as a result of the PCAOB's guidance, and 55 percent said they are increasing the number of hours they devote to provide direct assistance to external auditors—essentially acting under external auditors' orders.

Jeanette Franzel, a member of the Public Company Accounting Oversight Board, said at the IIA conference that the over-reliance problem was not nearly as pervasive in inspection findings as external auditors' apparent response to Practice Alert 11 would suggest.

"Overall, our inspection results regarding the external auditor's use of internal auditors' work are relatively positive," she said. "For the U.S.-based member audit firms of the six largest global networks, the number of audit deficiencies involving the external auditors' use of internal auditors' work is low overall. And it is low on a relative basis as well, when compared to other frequently cited deficiencies and to the total number of deficiencies identified through our inspections."


Franzel

Franzel said she is disappointed to hear anecdotal accounts of external auditors reducing or avoiding reliance on internal audit work to avoid an inspection finding. "Letting the pendulum swing too far is not a solution audit firms should be using to respond to PCAOB findings in this area," she said. "Essential value will be lost if external auditors simply avoid the use of internal auditors' work or turn this process into a massive duplication effort and check-the-box documentation exercise."

Calming the Mood

The CAQ and IIA conducted roundtable discussions to try to air out the tension, says Cindy Fornelli, executive director of the CAQ. "The alert was not meant to be a new standard, but to clarify the PCAOB's expectations of external auditor reliance on the use of internal audit's work," she says. "It became clear it may have inadvertently created tension between internal audit and external audit."

A joint report from the IIA and CAQ says auditors vented at roundtable discussions that the PCAOB is looking for granularity, that the guidance has strained the relationship between internal and external auditors, and that management is irked over the "audit fatigue" of having its staff subjected to duplicative audit demands, not to mention the cost consequences. More than 60 percent of internal auditors in the IIA survey said their external audit fees are rising.

"It's clear there are still some cases where external auditors are being particularly cautious, and perhaps just not relying on the work of internal audit at all, or asking for a lot of additional documentation to reperform the work of internal audit, essentially," Chambers says. "All of that creates tension between internal and external audit, and external audit fees going up creates angst with the audit committee and management in general."

The solution that emerged from roundtable discussions, says the CAQ and IIA, is for audit committees to get more involved and for audit planning to be more coordinated and better communicated upfront. The audit committee, internal audit, and external audit should plan together how the work will be allocated, what templates will be used, and

how walkthroughs will be performed to reduce duplication of efforts. "The audit committee can help coordinate internal audit's time and resources and how those are going to be used by external auditors," Fornelli says.

> "It's clear there are still some cases where external auditors are being particularly cautious, and perhaps just not relying on the work of internal audit at all, or asking for a lot of additional documentation to reperform the work of internal audit, essentially."
>
> Richard Chambers, President & CEO, IIA

External auditors would welcome that conversation, says Sara Lord, a partner with McGladrey. "Everything can benefit from more communication," says Lord, who has seen the tension on both sides through the firm's external audit services as well as outsourced internal audit services. "Reach out sooner, and plan this together. What are your audit plans? Are you using sample sizes that are sufficient? Do you have enough coverage coordinated with our audit methodology? This can only benefit the risk structure of the company and assure effective use of resources."

Peter Bible, a partner with audit firm EisnerAmper, says the tension represents a "pothole" in the continued evolution of auditing as a regulated profession. He worries the tension could harm the strides internal audit has made in recent years in becoming more elevated in corporate structures.

"I would hate to see this become a step backward for them," he says. "If firms are less likely to rely on the work of internal audit and do the work themselves, that has a couple of outcomes—all bad. The audit fees go up, and management will start questioning why internal audit needs a large budget."

Chambers

Chambers doesn't believe that's an immediate concern. "There's probably a healthy appreciation among management and audit committees that perhaps this has been an overreaction on the part of external auditors to the PCAOB's guidance," he says.

McGladrey's Lord says auditors are responding to the totality of standards and guidance, not any one piece of guidance. "As CPA firms, we're responding to guidance issued by the PCAOB in the form of official standards as well as guidance given through the course of inspection," she says. "It's difficult to point to just one of those sources of guidance and say you overreacted to a certain piece without looking at it in total." ■

STRATEGIC CONSIDERATIONS FOR INTERNAL AUDIT

Below is a list of statistics and starter questions put together by the IIA and Audit Executive Center for CAEs to pursue with their key stakeholders.

- 95 percent of respondents from publicly traded companies report assisting management to some degree with its documentation of ICFR, with 51 percent being either very or extremely involved.
- 65 percent of respondents from publicly traded companies experiencing increased scrutiny from external audit since 2013 expect an increase in external audit fees as a direct consequence of PA 11.
- 55 percent of respondents from publicly traded companies experiencing increased scrutiny expect an increase in the hours devoted by internal audit to providing direct assistance to external audit. (When providing direct assistance, internal auditors function as part of the external audit team and are directly supervised by the external auditors.)

Clearly, internal audit, external audit, and the audit committee will need to continue to collaborate going forward to strike the most appropriate balance for the company, taking into account three key factors—reliance, external audit fees, and the highest and best use of internal audit resources.

Addressing the fallout from PA 11 and its impact on audit planning and risk assessment will require an effective collaboration among internal and external audit functions, senior management, and the audit committee. Here is a starter list of questions for CAEs to pursue with their key stakeholders:

- When collaborating on annual planning activities, do external audit and internal audit have a common understanding of what areas are deemed most risky from an ICFR standpoint? Is there clear agreement on an acceptable level of external audit's reliance on the work of internal audit for these risky areas?
- Does the audit committee have an understanding of where external audit is, and is not, placing reliance on the work of internal audit, and the rationale behind the reliance parameters?
- Do internal audit and the audit committee clearly understand how external audit evaluates the competence and objectivity of internal audit?
- If there are opportunities to enhance the competence of internal audit, are those opportunities being pursued?
- If there are opportunities to enhance the perceived objectivity of internal audit, are those opportunities discussed?
- Does the external auditor have competence- and objectivity-related discussions with the audit committee? If not, does the audit committee know to initiate the conversation?
- To lay the groundwork for an informed cost/benefit decision about a potential increase in reliance work, is it clear how increased reliance on the work of internal audit might affect not only external audit fees, but also other internal audit priorities?

Sources: IIA; Audit Executive Center

Using Internal Control Frameworks to Thwart Risk

by Tammy Whitehouse

With the year-end audit approaching, now is the time for companies to look closely at one relatively new pain point in corporate audits—IT and cyber-security controls—to assure that the conversation is appropriately targeted toward risk.

External auditors no doubt will be scrutinizing IT controls that are important to financial statements, as the Public Company Accounting Oversight Board continues to give auditors poor marks in that area. Johnny Lee, a managing director at Grant Thornton who focuses on forensic accounting, says the interactions between external audit and IT staff will go much faster and easier if everyone can stay focused on risk.

"The conversation is difficult if you start straying too far from a risk-based discussion," he says. "What are the core risks you're trying to have us speak to in the control environment?"

Cyber-security has become major focus in corporate IT circles in recent years, but that does not mean auditors and IT folks are focused on the same priorities or even working from the same standards or frameworks. That's where the chief compliance officer needs to step into the discussion, says Worth MacMurray, senior vice president at compliance services provider GAN Integrity.

Auditors almost always follow the COSO Internal Control-Integrated Framework in their audit of financial statements and internal controls important to financial reporting, because that's the framework almost all companies follow to satisfy their Sarbanes-Oxley reporting requirements. IT staff, however, might be following any number of frameworks that have different objectives, because the IT needs of any given company encompass much more than just financial reporting.

"The chief compliance officer can play a significant role in aligning those various parties because of their skill set," MacMurray says. "They are used to dealing with a complex, multijurisdictional environment. It's quite analogous to dealing with anti-corruption."

It's a common point of confusion, especially with audit committees, says Sandy Herrygers, a partner and IT specialist at Deloitte. "If you're looking at a cyber-security program broadly, that's going to cover all facets of the business: operational, processes, systems, and financial reporting," she says. "If you're looking at information systems controls that are tested as part of an integrated audit, you're looking at a narrow slice of controls related to systems that are relevant to financial reporting."

David Roath, a partner in risk assurance for PwC who focuses on cyber-security and other IT risks, says the COSO framework looks at controls from a higher level compared with many of the IT frameworks used today. "Other IT frameworks are more security- and privacy-oriented," he says.

He's thinking of the NIST framework, for example, produced by the National Institute of Standards and Technology and intended foremost for critical infrastructure industries such as public utilities. Others are published by the International Organization for Standardization, or ISACA and its Control Objectives for Information and Related Technology framework (better known as CoBIT).


Roath

"The interesting thing is that these are just frameworks," Roath says. "It's guidance. It doesn't mean it's how it has to be. When we do assessments, we're looking broadly at security, privacy, maturity. We will incorporate different pieces of any of those frameworks. No one framework is right for any company. It has to be supplemented with broader knowledge, skills, expertise, to really elevate the risk in that environment."

Adventures in Mapping

Brian Palazini, a systems architect at sensor-maker Analog Devices, has been involved in mapping exercises to reconcile the requirements of different frameworks for different purposes. He's seeing some demands from different constituencies to make more use of the NIST framework, which experts say is becoming more common for U.S.-based companies as cyber-security attacks have become more routine. "It's pretty painful to try to do those matrices, mapping it back to a specific source document," he says. "It's a lot of manual work."

Mapping across frameworks is an "unfortunate reality" for anyone working with an external auditor who answers to the PCAOB, says David Brand, managing director in the IT audit practice at consulting firm Protiviti.

"The PCAOB is swinging a big stick in the IT space," he says. "It consumes so much time and effort to comply with COSO and external audit expectations; it pushes some of the other things out to the edge. Some IT departments don't have time to do other things because they are so focused on getting all of this stuff right for one individual regulatory requirement."


Hirth

Bob Hirth, chairman of COSO, says he doesn't see any conflict between COSO and other IT frameworks. "NIST and other frameworks are more granular and appropriately more detailed than COSO," he says. "If you follow those, you can tick off many things in the COSO framework." And much of what the IT frameworks cover is not relevant to financial reporting, he says. "For example, if you have a retailer with credit card information, that may not fall with SOX, because SOX is focused on a limited subset of internal controls."

Cyrus Amir-Mokri, a partner at law firm Skadden, Arps, Slate, Meagher & Flom, says the situation is not unlike others where companies face multiple regulators pushing different regulatory requirements. "We are prob-

ably making more of the differences between standards than actually exists," he says. Companies choose different IT frameworks based on their particular needs, and some companies are further along in addressing IT security than others, he says.

With so many frameworks and standards in play, that's one of the reasons chief compliance officers need to help make sense of it, says Pamela Passman, president and CEO for consulting firm CREATe.org, formerly corporate vice president in charge of global regulatory affairs for Microsoft. "This is where the new normal is headed," she says. "The first movers are trying to have a comprehensive approach in this cyber-security area, but these are the early days. The chief compliance officer and general counsel can really play a role here."

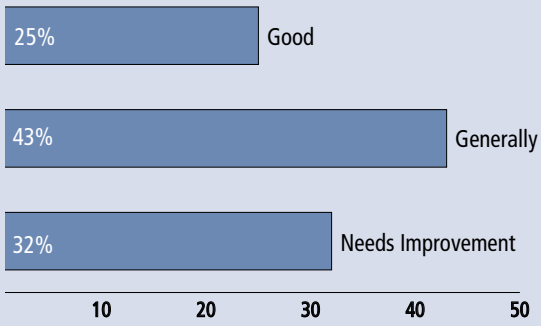
Grant Thornton's Lee agrees organizations need to be careful not to get lost in the details. "I don't think the adoption of one framework over another changes the dialogue one bit," he says. "If you can get away from which framework is important and talk about which control objectives are important, you're going to have a far more productive dialogue. If we have to marry your checklist of 237 points to my checklist of 182 points, that's going to be a long day." ■

CYBER-RISK FOCUS FOR AUDIT COMMITTEES

Below, KPMG outlines four key areas of focus to determine whether "management has its arms around cyber-risk."

Periodically review management's cyber security risk assessment. Every company should be conducting cyber security risk assessments as a matter of course. What are the company's highest value digital assets, and what are the greatest threats and risks to those assets? How quickly will the company know if a security breach occurs? In a robust cyber security risk assessment, key areas of focus will include: cyber-security leadership and governance, human factors or "people risks," legal and regulatory compliance, business continuity, operations and technology, and information risk. If the company has the right internal resources, the cyber security risk assessment can be conducted internally; however, as the cyber threat becomes more sophisticated, the company may need to call on recognized security specialists for support.

How would you rate the quality of information you receive on cyber-security and the potential impact on the company?



Source: 2014 KPMG Global Audit Committee Survey

Understand the company's cyber-security strategy and governance structure and how it fits into the company's ERM program. Once viewed as a stand-alone program, cyber-security is increasingly a multi-disciplinary process that is integrated into the company's ERM processes and overall governance structure. Does the cyber-security strategy and governance structure reflect an understanding of the company's data security priorities and security gaps? How are we deploying our financial and human capital to protect these assets against the greatest threats? Management needs to demonstrate that it is "skating to where the puck is going"—i.e., our cyber-security efforts must continuously improve to protect the company as our businesses and technologies evolve and cyber-threats become more sophisticated. Does leadership understand our cyber-security priorities and risks?

Insist on a cyber-security scorecard. As a matter of routine at each meeting, many audit committees and boards review with management a cyber-security scorecard, which typically shows (for the most recent period): the volume of identified cyber-incidents; the materiality and nature of cyber-incidents and how they are being managed; key trends and what is happening in the external environment (e.g., in the private and public sector and on the legislative front). A good cyber-security scorecard—which develops and evolves over time—helps to improve both the quality of cyber-information and the quality of director dialogue regarding cyber-security.

Understand the company's cyber-incident response plan. As one leading CIO recently told us, it's challenging to define a precise process or a set of concrete steps for managing a cyber-incident because cyber-incidents don't all have the same attributes and implications for the company or its customers. That said, incident management is a critical component of an overall cyber-risk program, and the effectiveness of the incident response plan will depend on several factors. First, scenario planning is critical, and all the key players—including the communications, legal, and policy teams—need to be involved. Second, it's important to establish clear accountability—if you have a breach, who is responsible for doing what? The final piece involves decision making—particularly if an incident has external implications, as most do. When third parties or customers might need to be notified, it's important to have a framework for making those decisions—sometimes very quickly.

Source: KPMG

WHITE PAPER

workiva

Partner With Your Auditor on Controls

How management can help its auditors address PCAOB inspections findings on internal control

Written by Thomas Ray, Distinguished Lecturer at Baruch College

Introduction

At the August 2015 meeting of the American Accounting Association, Public Company Accounting Oversight Board (PCAOB) member Jeanette Franzel voiced her concern about the high number of internal control auditing deficiencies the PCAOB's inspectors are continuing to identify.[1]

Soon thereafter, in September 2015, Helen Munter, PCAOB Director of Inspections and Registration, made a similar report to the PCAOB's Investor Advisory Group, noting that approximately 36 percent of integrated audits inspected in the 2013 inspections cycle had some deficiency related to internal control.[2]

Both Franzel and Munter reported seeing improvement at some auditing firms for 2014, based on preliminary results of those inspections, but that deficiencies were still high. We can expect that the PCAOB focus on internal control will continue.

Building pressure

The pressure to reduce inspections findings—and increase audit quality—has caused audit firms to change their audit methodologies and approaches, and to increase training of their professional staff. The pressure is also being felt by companies in at least two ways:

- Requests from their auditors for additional documentation related to both the design and operation of important controls
- Changes in audit approaches that frequently result in testing of additional controls not tested in previous audits

Does the fault for these findings rest solely with the auditors? The SEC staff has suggested that some of the PCAOB's inspection findings are indicators of similar problems with company management's evaluations of internal control, and thus potentially indicative of risk for unidentified material weaknesses.[3]

The PCAOB staff also has heard from auditors that the quality of a company's processes and controls affect the audit. When a company has well-documented processes and controls, audit quality tends to be higher.

How public companies can address demands

In addition to voicing their concerns, Franzel and Munter highlighted the nature of the most common internal control findings. This paper describes five of the most significant findings and discusses ways in which company management might respond to both improve its internal control and to help its auditors more efficiently obtain the evidence needed to support their internal control audit opinion.

1. Understanding the flow of transactions

Understanding the flow of transactions through the company's accounting system is a critical first step in planning an effective audit. This enables the auditor to identify where misstatements can enter the system and to identify and test the controls that are responsive to the risks. According to the PCAOB, many auditors have failed to gain an adequate understanding.

It is hard to imagine that so many auditors have failed in this fundamental objective. What could contribute to such failures? Two potential causes come to mind. The first is that the auditors did not perform the procedures necessary to understand how their clients' systems worked. Possibly, the systems walkthroughs were not performed by sufficiently competent personnel, were not properly supervised, or were not adequately documented. The second is that their clients' systems documentation was not complete or current, and the auditing procedures failed to identify the problem.

Companies obviously have the most control over the second potential cause. They can also play an active role in helping their auditors obtain and document the understanding and other information they need to appropriately plan and perform their auditing procedures.

There are several things every set of accounting systems documentation should include. These are:

A. **A description of how transactions flow through the system, from their initiation to their inclusion in the company's financial statements**

   This includes how transactions and other information, such as journal entries, are entered into the system, where transaction and other information that affects financial reporting is stored, and each process, including computer applications and manual processes, that affects the information. The description can be in the form of a flowchart, diagram, narrative, or a combination of these formats.

B. **Identification of the points in the system at which errors or fraud can occur**

   These points include:

   - When information enters the system (e.g., at the initiation of a transaction or the posting of a journal entry)
   - When information moves from one part of the system to another (e.g., from where the information is stored to an application that processes the information)
   - When data is summarized, aggregated, or otherwise changed (e.g., when a subledger posts to the general ledger or when the general ledger trial balance is summarized into financial statements)

C. **The controls in place at each point at which errors or fraud can occur that could cause the financial statements to be materially misstated**

   These controls normally should address the financial statement assertions implicit in the transactions or events that affect the company's financial information, which are:

   - Occurrence – the recorded transaction or event actually occurred
   - Completeness – all such transactions or events that occur are captured by the system
   - Accuracy – the details of the transaction or event are accurately recorded in the company's records

- Classification – the transaction or event is recorded to the correct account
- Cutoff – the transaction or event is recorded in the proper accounting period

Similar financial statement assertions also relate to:

- Ending balances in the financial statements – existence, rights and obligations, completeness, and valuation and allocation
- Presentation and disclosure of the financial statements – occurrence, rights and obligations, completeness, classification, and accuracy and valuation

Controls also are necessary to prevent or detect material misstatement to the ending balance and presentation and disclosure assertions.

The company should document all five internal control components, assuming management is using COSO's Integrated Framework, including the control environment, risk assessment, control activities, information and communication, and monitoring. The foregoing discussion is focused on the information and communication and control activities components.

2. Testing management review controls

After the first year of audits using Auditing Standard No. 2 (AS2)—the PCAOB's first internal control auditing standard—auditors were encouraged to adopt a top-down, risk-based approach to the identify controls that needed to be tested to increase the efficiency of their internal control audits without reducing their effectiveness.

Auditing Standard No. 5 (AS5), AS2's successor, incorporated this approach into the auditing standard itself. This was largely successful. Auditors replaced the testing of many process-level controls with fewer controls that operated at a higher level within the company, many of which were designed to address more than one financial statement assertion. Several forms of these higher level controls are referred to as management review controls, which often serve as a form of detective control that can help management identify misstatements, including fraud.

Unfortunately, a result of the PCAOB's increased focus on auditor compliance with AS5, which began with the 2010 inspections, the PCAOB has found that auditors:

- Were not able to show the PCAOB inspectors that the controls operated at the necessary level of precision
- Did not always obtain sufficient evidence that these controls operated effectively

Munter noted in her remarks that one explanation some auditors provided for these audit deficiencies is the lack of documentation to support the operation of the controls at the audit client. Thus, it is important to recognize that there are two forms of documentation the auditor is concerned with: documentation of the design of the controls (i.e., the design document) and documentation of their operation.

Company management should be satisfied that its documentation in these areas is sufficient to support both its own assessment of internal control effectiveness and its auditor's.

Precision of the control

Precision relates principally to the design of the control. The design elements of a management review control that ought to be described include:

- The objective of the control, which can be discussed relative to the financial statement assertions affected (e.g., expenses and accounts payable are complete), or the types of misstatements the control is designed to detect (e.g., to detect unrecorded expenses and accounts payable).
- The nature and sources of information being subjected to the control as well as other information used as a part of the control operation, including how the reliability of the other information is ensured. (See discussion on testing systems-generated data and reports.)

- The way in which the control is expected to be performed.
- The steps involved in performing the control and any necessary guidance on how the control operator should exercise judgment.
- The level of competence and authority of the control operator necessary to perform the control effectively.
- Characteristics of items, circumstances, or other criteria that require follow-up by the control operator, including monetary thresholds, where applicable. This point is critical to understanding the precision of the control, although other items in this list also are important to a control's precision.
- A description of the documentation that is generated as a result of the operation of the control—including how information/evidence used by the control operator is documented and retained, and how the control operator documents significant judgments made in performing the control. This documentation might be automated, or it may need to be prepared by the control operator, depending on the nature of the control.

Operating effectiveness

When testing the operating effectiveness of a control, the auditor must obtain evidence that the control actually operated and that its operation was effective. Ideally, management's process will capture this information contemporaneously with the control operation. Information that should be captured in the documentation includes:

- Evidence that the control operated
- The steps the control operator took in performing the control
- The matters identified for follow-up
- The information and evidence the control operator obtained and considered
- The significant judgments made by the control operator, his or her conclusions, and actions taken to resolve discrepancies
- Who performed the control and the date of its performance

3. Testing systems-generated data and reports

If a control selected for testing uses system-generated data or reports, the effectiveness of the control depends in part on the accuracy and completeness of the reports and data. Auditors did not always obtain sufficient evidence about the design and operating effectiveness of the controls over that accuracy and completeness.

Management might consider including, as a part of the design documents for management review controls, identification of the controls over the completeness and accuracy of data and reports used by the controls. This might help auditors to recognize that those controls are necessary for the effective operation of the higher-level control.

4. Selecting the right controls to test

Auditors did not always select the appropriate controls to test, missing some that were important to the auditor's conclusion about whether the company's controls sufficiently address the assessed risk of misstatement. This audit deficiency is probably closely related to the first one discussed above. If the auditor does not have a sufficient understanding of the flow of transactions through the system, it will be difficult to identify all the controls that require testing. Complete and accurate systems documentation should help auditors alleviate this issue.

When performing their systems walkthroughs (i.e., following transactions through the accounting systems from their initiation to their inclusion in the financial statements) and other procedures to obtain and update their understanding of a client's internal controls, auditors must interact with company personnel. Company personnel should understand the auditor's objectives. This will increase both the efficiency and effectiveness of the auditor's work. Company employees also can highlight the controls that they believe are most effective at addressing the misstatement risk.

5. Testing the design effectiveness of the controls selected for testing

Auditors did not always sufficiently understand or test the design of the control—that is, whether the control, if operating according to its design, satisfies the control objectives and effectively prevents or detects errors or fraud that could result in a material misstatement.

This is principally an evaluation made by the auditor, which may include the auditor reperforming the control. This test is dependent foremost on an accurate understanding of how the control actually operates. Frequently, the auditor will make this evaluation during the systems walkthrough, a procedure that is facilitated by the company's systems documentation and interaction with the employees responsible for the systems and controls.

Company management can be of the most help here by making sure that the systems documentation, including control design documents, is accurate. Management also can help its employees understand the walkthrough process and the objectives the auditor is trying to achieve, thereby increasing the likelihood that the auditors will perform an effective evaluation.

Use inspection findings to improve your controls

The intense focus on internal control auditing over the past several years has resulted in a more refined understanding of how a system of internal control over financial reporting should be designed and operated.

Although there are some concerns that expectations about internal control have gone too far, companies have an opportunity to learn more about internal control by understanding the information the PCAOB is sharing about its inspections findings.[4]

Management should think one step beyond the inspections findings as to how its own control systems, including documentation, could be a contributor to the findings, and how it can play a role in alleviating those findings—improving its controls in the process.

About the author

Thomas Ray is a Distinguished Lecturer in the Stan Ross Department of Accountancy at Baruch College, City University of New York. Previously, Tom served as Chief Auditor and Director of Professional Standards at the Public Company Accounting Oversight Board (PCAOB), where he oversaw the development of Auditing Standard No. 5 and numerous other PCAOB standards and rules. Tom also has held senior positions in KPMG LLP's national professional practice office and the AICPA, and was a member of COSO's Advisory Council for the 2013 update to Internal Control: Integrated Framework. Tom is a certified public accountant and provides auditing-related consulting services. He began his career with Grant Thornton LLP.

Resources

[1] Franzel, Jeannette. "Current Issues, Trends, and Open Questions In Audits of Internal Control over Financial Reporting." (2015). Public Company Accounting and Oversight Board. Retrieved from http://pcaobus.org/News/Speech/Pages/08102015_Franzel.aspx

[2] Munter, Helen. "Importance of Audits of Internal Controls." (2015). Public Company Accounting and Oversight Board. Retrieved from http://pcaobus.org/News/Speech/Pages/Munter-Audits-Internal-Control-IAG-09092015.aspx

[3] Croteau, Brian. "Remarks Before the 2013 AICPA National Conference on Current SEC and PCAOB Developments — Audit Policy and Current Auditing and Internal Control Matters." (2013). U.S. Securities and Exchange Commission. Retrieved from http://www.sec.gov/News/Speech/Detail/Speech/1370540472057

[4] Quaadman, T. (2015). Center for Capital Markets Competitiveness. Retrieved from http://www.centerforcapitalmarkets.com/wp-content/uploads/2015/05/2015-5.28-Letter-to-SEC-and-PCAOB.pdf

Wdesk

See what so many others have already discovered.

"With the time saved from Wdesk, we've become a better audit department. The team is able to add value in areas outside of SOX—especially in financial audits, operational audits, and looking at complicated contracts.

—***VP of Audit***, *Accretive Health*

Visit workiva.com/cw16 to learn more about Wdesk for SOX controls management.

Workiva