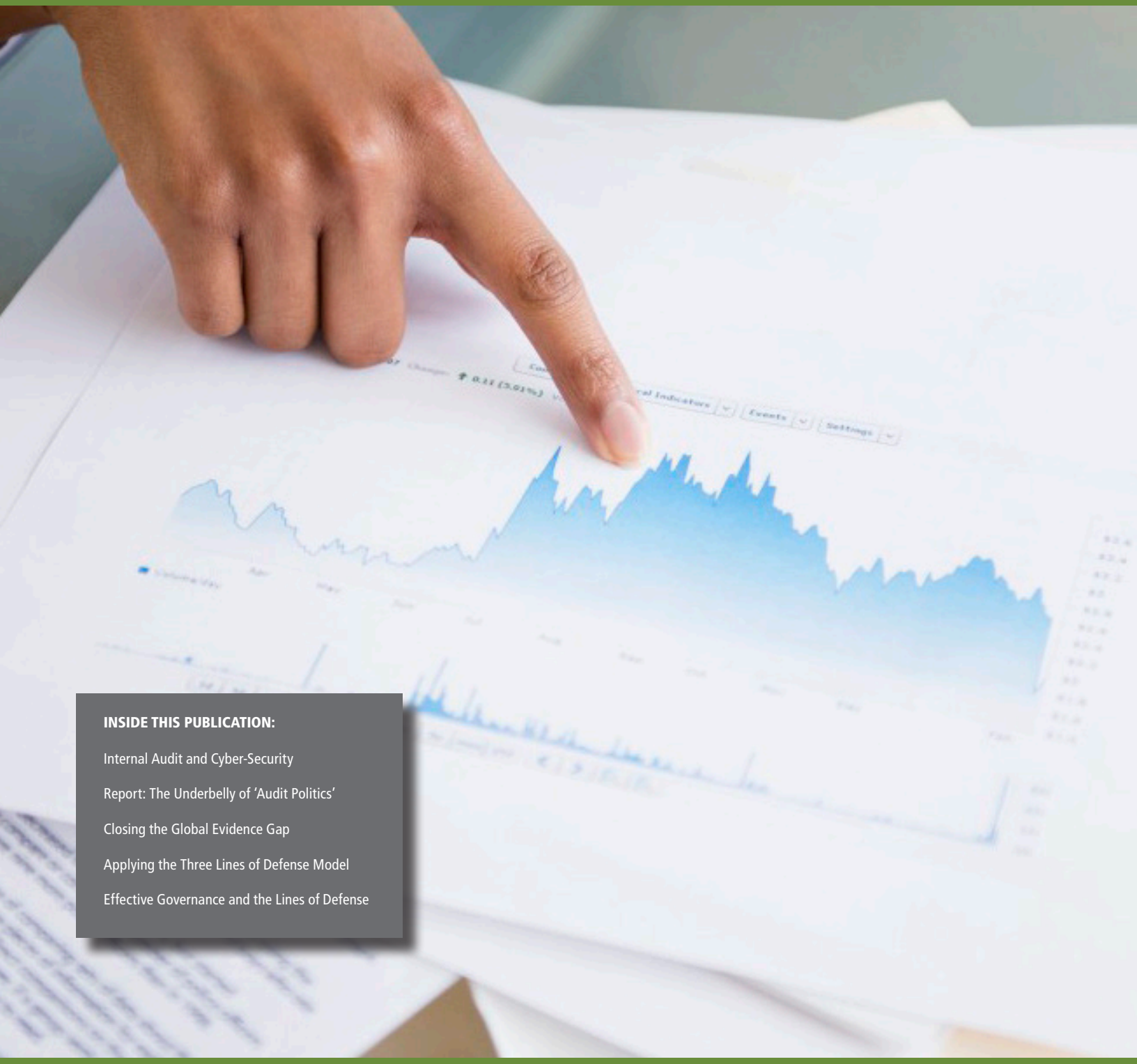
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

The Evolving Role of Internal 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 resources 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 platform for enterprises to collect, manage, report, and analyze business data in real time. Wdesk includes a sophisticated productivity suite for business data collaboration and reporting that is used by thousands of corporations, including more than 65 percent of the Fortune 500. Wdesk proprietary word processing, spreadsheet, and presentation applications are fully integrated and built upon the Workiva data management engine. Wdesk helps reduce enterprise risk and increase productivity with synchronized data, controlled collaboration, granular permissions, and a full audit trail. This gives users confidence to make decisions with real-time data. Workiva employs more than 950 people with offices in 15 cities. The company is headquartered in Ames, Iowa. For more information, visit workiva.com.

Inside this e-Book:

Internal Audit and Cyber-Security

By Tammy Whitehouse

With yet another potentially catastrophic data breach hitting Corporate America—add insurance giant Anthem to the list of recent victims—internal audit departments are trying to pinpoint what expertise they can bring to the company's cyber-security risk assessment, and where they might need to rely on more technical help.

"There is so much technical nuance to cyber-security; when people hear terms like firewalls, domains, vulnerability testing, and segmented networks, a lot of internal auditors become intimidated," says Tom O'Reilly, director of internal audit at Analog Devices. Even executive management and audit committees may wonder whether internal audit is up to the task of assessing a company's vulnerability to a cyber-breach and readiness to address one when it occurs.

The answer is yes, O'Reilly says. "There are technical aspects of these projects, but regardless of the technicality, internal audit can add a lot of value to this."

The debate over what internal audit can or cannot do is not uncommon, although it is perhaps renewed by the technical nature of cyber-threats now shaking Corporate America. "This is a criticism that has been in organizations since internal audit has existed," says David Brand, global head of IT audit for Protiviti. "'You don't know my business. You're not an expert in my area'—that's just a stonewalling technique."

In reality, Brand says, internal audit is equipped to do much of the work necessary for companies to grasp their cyber-risks. "Like most things, it's 80 percent process-based," he says. "It's things that anyone with a good audit skill set should be able to review."

Companies using the National Institute of Standards and Technology cyber-security framework (released last year) will find cyber-risk assessments to be a top-down exercise, he says. "The first questions are understand the business, the strategy, and objectives; what type of information the company produces; what it is the company wants to protect. Those are core questions. That doesn't require a deep technical skill set."

Richard Chambers, president and CEO of the Institute of Internal Auditors, says the current cyber-security threat is somewhat similar to the Y2K concern that gripped companies at the end of the 1990s. "It was a business process issue as much as it was an IT issue," he says. "In that regard, cyber-security is not unlike a lot of business issues in terms of how internal audit would address it."

Skip Westfall, managing director at Grant Thornton, says he sees companies getting away from the notion that cyber-security is an IT problem. "Because of recent breaches, the approach has been: We need to stop sitting back on our laurels and saying we checked the box. Are we doing all we can do on a day-to-day basis?" he says.

Shuaib Shakoor, a partner at internal audit outsourcing firm Sunera, says many companies still struggle to break away from a check-the-box approach to cyber-security concerns. The first step to taking initiative, he says, and gather the company's experts in privacy, governance, IT, legal, and other areas to plan an approach. "Band together and figure out what you can do holistically as a company to come up with a preventive and a detective plan," he says.

What's In-House, What's Out-House

Internal audit departments possess many of the skills and tools to perform the cyber-security risk assessment, O'Reilly says—especially if they have or (will soon have) implemented the new COSO framework for internal control over financial reporting. The framework is a useful tool for addressing cyber-security risks as well, audit experts say. "That's something internal audit can definitely drive," O'Reilly says.

Identifying and inventorying the company's most important data is another task for internal audit to lead, O'Reilly says. "When someone asks, 'What is the company's most precious data?' not every internal auditor or even management team would be able to talk about all the key documents or physical things that would include the company's crown jewels," he says. "So what is the key data? Where does it reside? Who has access to it? And test the rights to that data." For public companies, this shouldn't be a foreign exercise, as it's already required for Sarbanes-Oxley compliance purposes, he says.

Internal audit might want to look for more advanced cyber-expertise as the analysis digs deeper into specific technical vulnerabilities. Carolyn Holcomb, a partner with PwC focused on privacy and cyber-security, says internal audit might be able to perform some vulnerability testing, but most companies will rely on IT or third parties to perform more technical attack-and-penetration studies. "That's typically a management function," she says. "If internal audit does performs such testing, it might impair their independence because internal audit departments should not be performing management functions."

With vulnerabilities determined, internal audit can help illuminate the potential consequences of those vulnerabilities, as well as the controls in place (or the lack thereof) to remediate the risks. "Internal audit can walk through this process and tee up the questions, like any other accounting control testing," O'Reilly says. By identifying the potential consequences of any weak spots, internal audit can help reach conclusions about whether the company is performing the right testing and protecting the right data, Westfall says.

Internal audit also can play a role in validating a company's response plan, O'Reilly says. "What are the steps to be taken after a breach?" he asks. "Do we know what the intruder has accessed? How do you communicate with your suppliers, customers, other stakeholders?"

Theresa Grafenstine, inspector general of the U.S. House of Representatives and international vice president of ISACA, says government auditors have already been down this path and discovered they could learn a lot about the technical side of cyber-security risks by shadowing third parties who do the technical work. "It looks daunting, but you have to start somewhere," she says. "If you keep relying on outside contractors, you never gain the skills yourself. So write into the contract as the contractors perform their audits, we want to sit with them through every step and learn."

Internal audit departments also should prepare for a world where cyber-security risks are a subject to ongoing monitoring, rather than an annual or biannual exercise, Holcomb says. "There's a lot of enthusiasm today about building a program and getting it into place," she says. "We recommend that internal audit monitor and periodically test the effectiveness of the company's information security and privacy program." ■

Report: The Underbelly of 'Audit Politics'

By Tammy Whitehouse

Try not to faint when you hear this, but—corporate political pressure on chief audit executives to alter their audit plans or results is "extensive and pervasive," according to a new report from the Institute of Internal Auditors.

Based on the IIA's latest research—which included survey results, personal interviews, and focus group discussions among some 500 chief audit executives—more than half of audit executives said they have experienced pressure to omit or modify an audit finding during their careers; nearly 20 percent said it has happened more than three times. Almost half said they were directed, usually by someone in executive management, not to audit a high-risk area. Nearly one-third said they were directed to audit a low-risk area so that an executive could investigate or retaliate against someone.

"We were really surprised by the extent of pressure," says Larry Rittenberg, co-author of the research report and past chairman of COSO, the Committee of Sponsoring Organizations. "We found political pressure came from all parts of the organization. We really could not sort out just one individual function where most of the pressure came from."

Rittenberg and his co-author Patty Miller, formerly with Deloitte, say in their report that they spoke with audit executives who told harrowing stories of job loss and physical threats in the most extreme cases. "CAEs with impeccable service records in both the private and public sector lost their jobs or were encouraged to take other positions or early retirement for challenging management on political issues," they wrote. But pressure could be much more subtle too, they said, such as staffing or budget cuts, or transfers to lower-level positions within the company.

Warren Stippich, GRC leader for Grant Thornton, has witnessed plenty of political pressure on the internal audit function, he says. "The statistics did not surprise me," he says. "I'm glad to see they undertook this research. It's something that probably needs a little light shed upon it. We all know there's political pressure. It's a bit like the unspoken elephant in the room."

In Stippich's view, no company is immune to the problems that stem from office politics. "Chief audit executives can't be so naive as to say they will work for an organization that has no politics," he says. "That's not possible. The chief audit executive has to learn to be politically savvy. If he or she carries on too much about politics, they will perhaps be viewed as being too weak or politically immature."

Stephen Shelton, a chief audit executive at a Fortune 500 company, says he's never been inappropriately asked to add or subtract something from an audit report. "Where it does happen, it probably doesn't come out of the blue," he says. "It would be representative of an environment that wasn't very strong from a governance perspective."

In Shelton's view, a fine line exists between political pressure that's inappropriately directed at the CAE and varying perspectives among stakeholders that have to be managed. "Sometimes what somebody sees as pressure really just represents different points of view," he says.

Rittenberg and Miller raise that issue in their research as well, as they say it points to one of the critical skills necessary for a chief audit executive to be successful: navigating the human element of large organizations. Regardless of an auditor's technical skills and competence, he or she also needs to be politically astute to anticipate and manage the political side of things.

Brian Christensen, executive vice president of internal audit for consulting firm Protiviti, says he's not sure how extensive or pervasive true political pressure may be, but enduring difficult situations is certainly an everyday part of the job. "They encounter those because when you're auditing a process and there's potential for observations that could impact someone's job or career, those are going to be difficult conversations," he says.

Where auditors experience pushback, he believes it comes more from the operational leaders whose work is being audited, not necessarily from management or the board. "I'm less convinced it's at the board level or senior management level given the current environment that everyone operates in with the corporate governance at that level," he says.

Echoing the sentiment that auditors must be politically savvy to navigate any pressure, Christensen says auditors need "to become outstanding communicators." That means assuring that senior leadership and operational leaders understand the role of internal audit and how audit gets its work done, and then conveying the results of internal audit work clearly and objectively. "It's not enough to be fluent in a topic or technically competent," he says. "The qualitative factors are what will make an auditor successful going forward."

Michael Cangemi, a business adviser and author with Big 4 and corporate audit experience, says the independent mindset of internal audit is critical to enable auditors to stand up to politically driven demands or pressures. He remembers well his own experience of facing pressure when he assumed the head audit job at a company where the prior head of audit had been persuaded to steer clear of certain operations. "When I set up the internal audit practice, I had to be all about what's good for business," he says. "I had to focus on helping try to improve the internal controls and business practices of the company. That was the way I answered everything."

Gary Sturisky, national consulting leader for McGladrey, says he likes to focus on the relational aspects of the audit leader's duties. Audit leaders need to be adept at forming relationships with audit stakeholders so they won't be viewed as the corporate police officers. "The challenge is where do you draw the line between working with the business while still maintaining independence and knowing when to push back?" he says. "It's got to be a very astute individual to navigate that and find that balance."

Tom Harper, general auditor for Federal Home Loan Bank of Chicago, says he can't recall ever facing a senior executive who asked him to overlook an audit finding or steer the audit plan away from a particular area. "Maybe I've just been lucky," he says.

If faced with an inappropriate demand, Harper says, he might begin by having a private conversation with the individual. "If that doesn't work, I would maybe find suitable people who might be their peers, say general counsel," he says. Then the discussion would likely elevate to senior executives. "The last resort is to start talking to the audit committee." ■

Closing the Global Evidence Gap

Sometimes absence of evidence is evidence of absence

Written by Joseph Howell and Curtis Matthews

A host of laws and regulations make it clear that the managers of public companies, not their auditors, are responsible for establishing and maintaining effective internal control over financial reporting and regularly assessing the effectiveness of those controls.

External auditors are charged with assessing the effectiveness of management's efforts and forming an opinion as a basis for designing their audits. For certain large companies, auditors must also express a separate written opinion on those controls.

In recent months, regulators responsible for reviewing the work of auditors in the United States and from around the world have found a growing number of cases where auditors "failed to obtain sufficient appropriate evidence to support its opinion on the effectiveness of internal control."

Audit firms have taken criticisms from regulators seriously and have changed their approach. For many audit clients, the new approach means more extensive procedures related to internal controls. For some companies, though, audit changes have caused big problems, including lengthy delays in issuing financial statements, drastic increases in audit work, and millions of dollars of additional audit fees.

The vast majority of companies may believe that they have plenty of evidence to support their assessment of internal control. But a growing number of auditors and their regulators aren't so sure.

In a recent speech, Andrew Ceresney, director, Division of Enforcement for the Securities and Exchange Commission, said a company was cited for having inadequate internal controls when it recorded revenues—without sufficient proof that customers had accepted goods sold. "Senior leadership was not asking the tough questions—and sometimes not even asking the easy questions," he said. "Senior management, in some cases, was just not engaged in any real discussion about the controls. As a result, employees did not properly focus on them, and the firm and its shareholders are put at risk."

The message for public companies is clear: Regulators and auditors have begun to demand that companies adopt a more evidence-based approach to manage their risks and assess their controls.

What is evidence-based risk management?

Evidence-based risk management is the practice of integrating evidence collection, organization, and analysis for the purposes of risk identification, assessment, and control.

Each year, companies make bold statements in their Form 10-Ks, such as: *Our management conducted an evaluation on the effectiveness of our internal control over financial reporting based on the Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 Framework). The evaluation concluded that our internal control over financial reporting was effective.*

On top of those bold statements, CEOs and CFOs sign individual certifications stating that they, personally, evaluated the effectiveness of their financial reporting controls and concluded on their effectiveness.

Yet, CEOs, CFOs, and other senior executives are often far removed from the details of such controls. What could possibly give them confidence to take personal responsibility for their effectiveness? In one word—evidence.

Having said that, few senior executives attribute their success to gullibility. Many are quite proud of their professional skepticism. As semiconductor pioneer Andy Grove once put it, "Only the paranoid survive." What kind of evidence would prove sufficient to convince a professional skeptic? Does your internal controls process provide that quality of evidence?

To answer that, let's take a look at two common situations where auditors frequently criticize companies for lack of adequate evidence.

Recognizing the evidence gap

Situation 1

Managers often point to management meetings held to review operational and financial performance as a key management review control. After all, each of the managers who participate is actively engaged in the business and has a deep understanding of how the business operates and the likely results. If the reported results were materially wrong, these managers would certainly spot the errors and correct them.

Unfortunately, despite conducting these important meetings, key details are often missed in the final record. Specifically there is often:

- No agenda, meeting minutes, or follow-up e-mails that demonstrate that the managers actually reviewed the results, had questions about them, followed-up on those questions, and resolved them successfully
- Absence of the criteria the managers used to identify exceptions worth considering
- No record of the evidence the managers considered to explain variances, or lack of variance, from what they expected

Situation 2

Managers often point to their reviews of analyses and the critical calculations prepared by their staff to support important assertions in their financial statements. They sign and date the documents to prove that they reviewed them.

Unfortunately, signatures do not provide needed information about the depth of their review. In many cases, there is:

» No record that they tested the calculations to ensure that they were accurate

» Little to no supporting documentation or validation evidence

» No explanation of why and how they concluded that assertions were consistent with GAAP or company policy

» Failure to document why and how they concluded the analyses and/or critical calculations were reasonable

If you were CEO and relying on managers to perform these and similar controls, would you feel comfortable declaring that you were personally responsible for their effectiveness? If not, what kind of evidence would help, and how would you get it without adding to the workload of the people involved?

Closing the evidence gap

Companies fail to collect the evidence they can trust for several reasons:

1. The individuals charged with the work aren't told that they need to collect evidence, and/or there is no consistent way to check their progress throughout the process
2. They lack a consistent, cost-effective way to collect and organize the evidence
3. They struggle with multiple versions of key documents and templates which often have inconsistent data
4. They lack a single repository where they can store, organize, and access the evidence quickly and easily

Further, adding more people and procedures, or making processes more complicated usually compounds the problem.

What can be done?

The problem isn't your people. It's the tools they have to work with, or rather the lack of integrated risk management tools to help them do their job. The key word here is integrated.

Collecting, organizing, and managing large amounts of disconnected pieces of evidence manually, and usually on an adhoc basis, simply doesn't cut it in today's complex business environment—as evidenced by the auditing problems highlighted by the SEC, the Public Company Accounting Oversight Board, and other international regulators.

These approaches are doomed to failure because they don't scale to enterprise requirements any more than doing your company's accounting using columnar sheets and calculators. Your financial team members need tools that blend seamlessly into their day-to-day routine, helping make what is otherwise a near impossible job, easier.

Fortunately, there are new cloud-based, reporting platform technologies designed specifically to address the problems of evidence collection, organization, and management—making evidence-based risk management a reality.

Companies adopting these technologies have been able to improve control performance, eliminate version control problems, automate storage and retrieval practices, and reduce the time demands on their jobs—in addition to improving the quality, timeliness, and usefulness of evidence.

Make it easy to trust

Evidence-based risk management gives us the ability to trust the results. Collecting evidence also provides an effective reminder of the steps we must take to earn trust.

It's evidence that enables managers of public companies to be confident and demonstrate to their auditors and senior executives that their internal controls are effective. However, if the act of collecting, organizing, or managing evidence is too hard, it does not get done, at least not consistently, and therein lies the problem.

New cloud-based tools have proven that they can help streamline and simplify the processes, and in doing so, make people's jobs easier. They make it possible to close the global evidence gap and provide managers and their auditors the ability to trust their results.

About the authors

Joseph Howell is a co-founder and Executive Vice President of Workiva. Joe has over 25 years of experience in senior financial management and SEC reporting, and has served as a chief financial officer for several public companies, including EMusic.com, Merix and Borland, and several private companies, including Eid Passport and Webridge. Joe also served as managing director at Financial Intelligence LLC, a company that provides accounting and SEC disclosure advisory services. A certified public accountant (inactive), he earned a BA from the University of Michigan and an MS in accounting from Eastern Michigan University.

Curtis Matthews, CPA, is the partner in charge of the Moss Adams Business Risk Management and Control Solutions Practice. Curtis has deep experience in a wide variety of areas including internal audit, outsourced internal audit, Sarbanes-Oxley Act compliance, construction risk management, information system application controls, and federal government contracting compliance. He is responsible for helping clients perform risk assessments and implement internal audit functions and other risk mitigation capabilities. Curtis earned a BA in business administration (emphasis on accounting) from California State University, Fullerton, and an MS in management in science and technology from Oregon Graduate Technical Institute.

Applying the Three Lines of Defense Model

By Jose Tabuena
Compliance Week Columnist

The Three Lines of Defense model for compliance and risk management, where internal audit is positioned as an independent function in the third line of defense, is considered a good practice to enhance oversight over a company's control environment. It describes the interaction among operating units that manage risks (the first line), departments that provide oversight (the second line), and groups that provide independent assurance (third line).

Jose Tabuena
Columnist

Internal audit not only provides independent assurance that risks are managed at acceptable levels; it also provides assurance that second-line oversight functions work as desired.

Each line of business owns the risks inherent in its operations and is accountable for maintaining effective internal controls to safeguard the company. Risk and control functions (the second line) typically include risk, compliance, and legal, along with control units from finance and human resources. They each have their own responsibilities but work together to provide collective oversight of the businesses and firm-wide control policies.

In a recent column, I described the overlaps and distinctions among the lines—particularly the control functions in the second line. In this column: Given those blurred lines, how should organizations implement the model?

One approach is first to focus on confirming the company's individual risks and then let control activities (managing, monitoring, assurance, issue tracking, reporting, and so forth) flow from those risks. The company's risk tolerance and monitoring should drive how these risks are mapped. For example, some companies could choose to have all risks mapped to all three lines; others may focus only on significant risks and be content with mapping one or two lines for other risks.

Ideally, all three lines should exist in some form at every organization, regardless of size or complexity. In reality, the boundaries among the activities relating to internal auditing, risk management, and compliance are not always well defined. Companies have merged certain functions within the second line, as well as between the second line with internal audit in the third line.

Combining Second-Line Functions

Management establishes second-line functions to ensure that processes and controls are properly designed, in place, and operating effectively, and that identified risks are mitigated. Some companies believe that combining the second line functions provide efficiencies and cost savings. Various combinations in the second lines are possible. Most integrations seem to involve the compliance function.

In sectors such as financial services, regulations may require separate risk management and compliance functions. Yet risk management has become even more hardwired into more financial industry rules and regulations since the 2008 financial crisis. For financial services, some parts of a compliance function may be involved in designing controls for the first line of defense, while other parts monitor controls as the second line of defense.

Recently, Bank of America moved its compliance function out of the legal department and into the bank's risk-management organization. This shift comes amid a push by bank regulators for financial institutions to do a better job of integrating compliance efforts with risk mitigation. Bank of America said that combining risk and compliance "aligns all risk-management oversight under our chief risk officer simplifying how we operate and is consistent with steps we have been taking as our company continues to normalize" since the end of the financial crisis.

In another example from financial services, JPMorgan Chase issued a report that describes efforts to improve compliance, culture, and internal controls, detailing the investments it has made. Until 2013, compliance at JPMorgan Chase was part of a joint legal and compliance group. Compliance was then separated from legal to give it dedicated leadership, resources, and support. In the report, JP Morgan states that this move "emphasized the importance and stature of compliance, as well as the company's commitment to maintaining a culture of compliance and control."

Whether compliance should be merged or be separate from legal or risk should be evaluated carefully, as each model has advantages.

> As the third (and sometimes considered the last) line of defense, internal audit should avoid duplicating the efforts of the control and risk oversight functions unless necessary.

Combining Internal Audit and the Second Line

As the third (and sometimes considered the last) line of defense, internal audit should avoid duplicating the efforts of the control and risk oversight functions unless necessary. Still, combinations of internal audit with second-line-of-defense functions such as risk management, compliance, and internal control do exist.

The IIA Netherlands recently published a white paper on the pros and cons of combining internal audit and second-line-of-defense functions. The paper addresses the question on whether internal audit can work independently and objectively if support is provided on risk-management, compliance, and internal controls.

The paper notes that while combining the internal audit and second-line-of-defense functions is not preferred, situations may arise where combination benefits the organization so long as basic conditions are met and adequate safeguards exist to ensure the independence and objectivity of the auditor. The following are the conditions and safeguards pro-

vided in the white paper:

- **Effectiveness not to be compromised:** Lines of defense should not be combined or coordinated in a manner that compromises their effectiveness in providing independent and objective assurance.
- **Make consequences explicit:** Internal audit should clearly communicate the effect of the combination to senior management and the governing bodies (and obtain their approval).
- **No management responsibility:** Internal audit should not assume any managerial responsibilities with respect to the audit objective. Internal audit can facilitate and support, but should never assume ownership.
- **Formalize:** Roles and responsibilities are to be described in the audit charter, to avoid ambiguity and provide clarity in the organization. Potentially conflicting roles for internal audit should be allocated to different individuals or departments.
- **Maturity:** In case of a temporary role where internal audit supports the setup of second-line-of-defense functions or design of methodology, the approach is to be approved by the audit committee.
- **Outsourcing:** If internal audit is involved in second-line-of-defense activities, providing objective assurance regarding these specific activities should be outsourced, either externally or internally to other departments.

Office of Governance?

An interesting new trend for global companies is the creation of a "governance" office that centralizes governance, risk, and compliance activities into a unified function. Because governance entails oversight of the systems that guide the control and management of a company, it seems that a governance function would be uniquely situated to collate and coordinate risk control activities.

One example along these lines is Walmart. In 2013 Walmart revamped its compliance department and aligned its corporate structure to have the global compliance, ethics, investigations, and legal functions under one organization, reporting to its executive vice president for global governance. Walmart split compliance and legal into separate departments: The chief compliance officer and general counsel are peers that report to the head of global governance. The CCO also reports directly to the audit committee, as does the Walmart chief audit executive who serves in a third line of defense role.

Another example is Boeing. The compliance function at Boeing combines internal audit as the Office of Internal Governance. The senior vice president for the Office of Internal Governance oversees Boeing's compliance and ethics program, including ethics, trade controls, compliance risk management, and a team of professionals who comprise internal audit. The senior vice president reports to the Boeing chairman and CEO and also has a direct reporting relationship with the board of directors through the board's audit committee. In this approach, both compliance and internal audit can be viewed as playing a second and third line of defense.

Clearly innovative approaches for applying the Three Lines of Defense model are emerging. Various combinations are possible, and what works will depend on the distinct risks and operational challenges a company faces. ■

Jose Tabuena provides a unique perspective on internal auditing issues bringing Big 4 firm experience and having held a variety of audit-related roles, including compliance auditor, risk manager, corporate counsel, and chief compliance officer. He has conducted sensitive internal investigations and assessed the performance of internal audit and ethics and compliance functions in highly regulated industries. Tabuena has held major compliance management roles at Kaiser Permanente, Texas Health Resources, Orion Health, and Concentra | Humana. Tabuena is certified as a fraud examiner, in healthcare compliance, and he is an OCEG Fellow.

Tabuena can be reached at jtabuena@complianceweek.com.

RECENT COLUMNS BY JOSE TABUENA

Below are recent columns by CW Columnist Jose Tabuena. To read more from Tabuena, please go to www.complianceweek.com and select "Columnists" from the Compliance Week toolbar.

Escalation Processes to Avoid Personal CCO Liability
CCOs have become targets for regulators because of what they (may) know and advise about regulatory rules. Now they face personal liability for failure to act. Columnist Jose Tabuena explains how escalation processes provide protections for compliance and the firm.
Published online 02/24/15

Applying the Three Lines of Defense Model
CW's Jose Tabuena continues his look at the Three Lines of Defense model by examining how a firm can parcel out all its oversight functions across the three lines. Can compliance report to the risk-management function? Can internal audit and compliance be combined?
Published online 01/21/15

Effective Governance and the Three Lines of Defense
CCOs, internal auditors, fraud investigators—these days, they all may work at one firm jointly to assist in managing risk. The trick to effective governance, however, is to assign all those professionals to their proper places in the Three Lines of Defense model. Jose Tabuena explores the logic behind that model.
Published online 12/16/14

Information Governance: Creating Order in a World of Chaos
The massive accumulation of information can overwhelm companies, creating compliance risks, so companies are mapping out existing systems where data resides and may be managed. Columnist Jose Tabuena looks at how companies are dealing with data overload.
Published online 11/11/14

Effective Governance and the Lines of Defense

By Jose Tabuena
Compliance Week Columnist

Some pundits would say that battles have steadily been brewing between the risk and control assurance functions. Should compliance report to legal, or be separate? Should compliance and internal audit be combined? Should audit take on risk management, or vice-versa? These are some of the simmering debates on how best to structure governance-related functions at a large enterprise.

Jose Tabuena
Columnist

Lately I've been getting inquiries about the value of combining risk and control functions. While efficiencies can be gained, organizations should heed whether integrating these areas can impair the ability of these functions to provide needed levels of assurance effectively. New approaches have emerged rolling these areas into an "office of governance" to facilitate information flow among them. I've even been asked about the old bugaboo of placing all risk and control functions (even internal audit) under legal, to better preserve attorney-client privilege.

Blurred Lines

I've seen confusion arising from the lack of awareness of the overlaps among the frameworks each specialty uses. For example, internal audit is not fully familiar with the U.S. Sentencing Guidelines that drive compliance in the legal department, while lawyers don't know about the COSO framework used by internal auditors. Each function knows its own framework quite well, but can be unfamiliar with other frameworks outside their realm and doesn't recognize the connections and duplication in their activities.

The activities of a chief compliance officer illustrate the point. One of the key components of a compliance program is to conduct monitoring and auditing to detect criminal conduct. But which departments should perform monitoring and auditing activities? The best approach may depend on factors unique to an organization.

Another example is the compliance program conducting a periodic risk assessment to evaluate the threat of criminal conduct. Is this performed by compliance, or should it be done by (or in collaboration with) enterprise risk management? Even more blurred is the handling of "incidents" including calls to a whistleblower hotline.

The Three Lines of Defense

The Three Lines of Defense in Effective Risk Management and Control, a position paper published by the Institute of Internal Auditors, offers a good framework for a company to organize communications on risk and control activities. The model can help a business with its governance structure by helping to clarify roles and duties.

The Three Lines of Defense model distinguishes three groups (or lines) involved in effective risk management:

» **First line, operations and business units.** Business-unit management is responsible for identifying and managing risks directly. This group should regard risk management as a crucial element of their everyday jobs.

» **Second line, management assurance.** These are groups responsible for ongoing monitoring of the design and operation of controls in the first line of defense, as well as providing advice and facilitating risk-management activities. They are usually management functions that may have some degree of objectivity, but may not be entirely independent from the first line.

» **Third line, independent assurance.** These functions provide independent assurance over managing of risks. In addition to internal audit, external audit and regulators are included, as long as the scope and nature of their work aligns with the company's risk-management objectives.

As every organization is unique, no single "correct" way exists to coordinate the three lines of defense. When assigning specific duties and coordinating among risk control functions, the underlying role of each group should be kept in mind.

What Comprises the Second Line?

Obviously the second line of defense is most relevant to us reading Compliance Week. Management establishes second-line risk and control functions to ensure the first line of defense is properly designed, in place, and operating as intended. Each of these functions has some degree of independence from the first line of defense, but they are by nature management functions. As such, they may intervene directly in modifying and developing the internal control and risk systems.

Exactly what might constitute a good second line of defense? The IIA and other commentators have a few suggestions:

> Companies will be well served to apply the Lines of Defense Model and communicate the expectation that information be shared and activities coordinated among the groups responsible for managing the organization's risks and controls.

» A risk-management function that facilitates and monitors the implementation of effective risk-management practices by operational management and assists risk owners in defining their target risk exposure and reporting adequate risk-related information throughout the organization.

- A compliance function to monitor specific risks involving non-compliance with laws and regulations. In this capacity, a separate function reports directly to senior management or even to the governing body. Multiple compliance functions may exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, environmental, or quality monitoring.

- A controllership function that monitors financial risks and financial reporting issues. This includes internal control activities that support management in identifying key process risks, and in implementing preventive and detective controls to mitigate these risks.

- Business ethics and special investigations units that focus on communicating and providing training on the company's code of conduct; overseeing the whistleblowing process; and promoting fraud awareness. Often these activities are part of the compliance program though separate in some companies.

What the IIA's position paper doesn't explicitly discuss is how support departments such as finance, legal, and HR fit in the model. Are they part of the first line owning specific risks? Or do they support the second-line monitoring risks in the business units? For instance, finance can be viewed as part of the first line for developing and operating internal controls for financial reporting risks, while the controllership function within finance provides a second line of defense in monitoring and evaluating those financial controls.

How a group actually puts this model to work matters more than the title or name of the function; each line needs adequate skills to discharge its responsibilities. This is typically straightforward in the first line, but can be more complex in the second and third lines. Thus in some organizations, legal or compliance may have only second line of defense responsibilities, while in others they may have first and second-line roles. Moreover, some chief compliance officers report independently to a board committee, which arguably puts them in the third line of defense along with internal audit.

Combining Lines of Defenses

Particularly in less-regulated industries and small organizations, risk control activities are often combined. For example, you might see internal audit asked to establish or manage the organization's risk-management activities, as well as audit the effectiveness of them. Opinions differ about the wisdom of combining risk, compliance, and assurance functions in that manner. The key question is whether the internal audit and compliance functions can work at an appropriate level of independence and objectivity when roles are merged.

Ultimately compliance and audit roles can't simply be inserted into existing functions and reporting lines. Integration must be carefully engineered so it effectively meshes with business lines and a wide variety of department and operational units. At the same time, compliance and internal audit must have the right level of independence to raise concerns, play a role in investigations, and influence culture.

The primary insight I find with the concept of governance, risk, and compliance is that it stresses the importance of coordinating risk control activities so that management and governing bodies are not filtering through mounds of duplicate (and often conflicting) information. Companies will be well served to apply the Lines of Defense Model and communicate the expectation that information be shared and activities coordinated among the groups responsible for managing the organization's risks and controls.

In next month's column I will discuss recent examples that depict the challenges of combining separate functions including internal audit with second-line defense functions, and the safeguards to consider when doing so. ■

Jose Tabuena provides a unique perspective on internal auditing issues bringing Big 4 firm experience and having held a variety of audit-related roles, including compliance auditor, risk manager, corporate counsel, and chief compliance officer. He has conducted sensitive internal investigations and assessed the performance of internal audit and ethics and compliance functions in highly regulated industries. Tabuena has held major compliance management roles at Kaiser Permanente, Texas Health Resources, Orion Health, and Concentra | Humana. Tabuena is certified as a fraud examiner, in healthcare compliance, and he is an OCEG Fellow.

Tabuena can be reached at jtabuena@complianceweek.com.

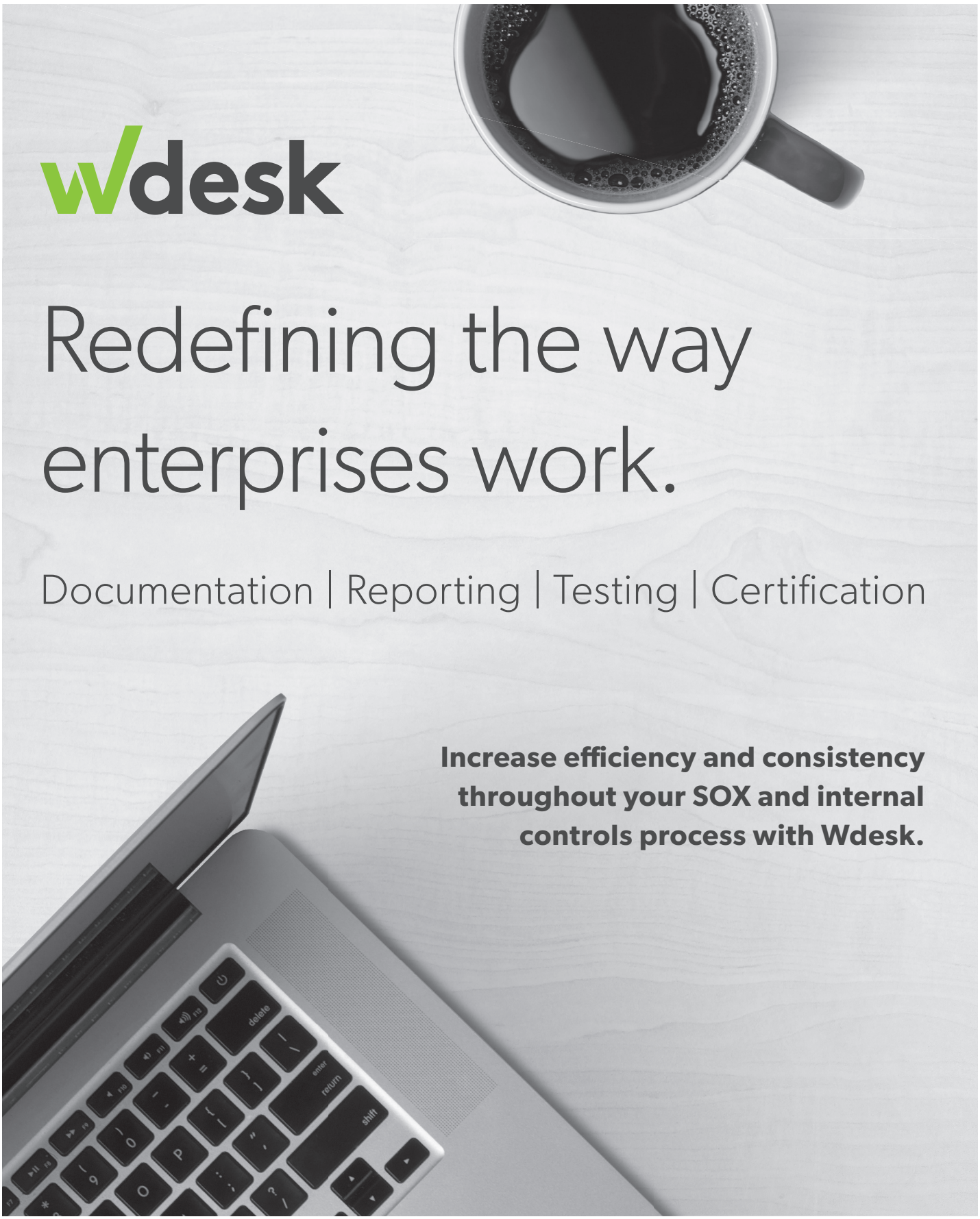
RECENT COLUMNS BY JOSE TABUENA

Below are some recent columns by Compliance Week Columnist Jose Tabuena. To read more from Tabuena, please go to www.complianceweek.com and select "Columnists" from the Compliance Week toolbar.

Escalation Processes to Avoid Personal CCO Liability
CCOs have become targets for regulators because of what they (presumably) know and advise about regulatory requirements. Now they face personal liability even for failure to act. Columnist Jose Tabuena explains how escalation processes provide protections for compliance, as well as for the company.
Published online 02/24/15

Applying the Three Lines of Defense Model
CW's Jose Tabuena continues his look at the Three Lines of Defense model by examining how a company can parcel out all its oversight functions across the three lines. Can compliance report to the risk-management function? Can internal audit and compliance be combined?
Published online 01/21/15

Effective Governance and the Three Lines of Defense
CCOs, internal auditors, fraud investigators—these days, they all may work at one firm jointly to assist in managing risk. The trick to effective governance, however, is to assign all those professionals to their proper places in the Three Lines of Defense model. Jose Tabuena explores the logic behind that model.
Published online 12/16/14


wdesk
Redefining the way enterprises work.
Documentation | Reporting | Testing | Certification
Increase efficiency and consistency throughout your SOX and internal controls process with Wdesk.
workiva.com | info@workiva.com | +1.888.275.3125
Workiva