Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

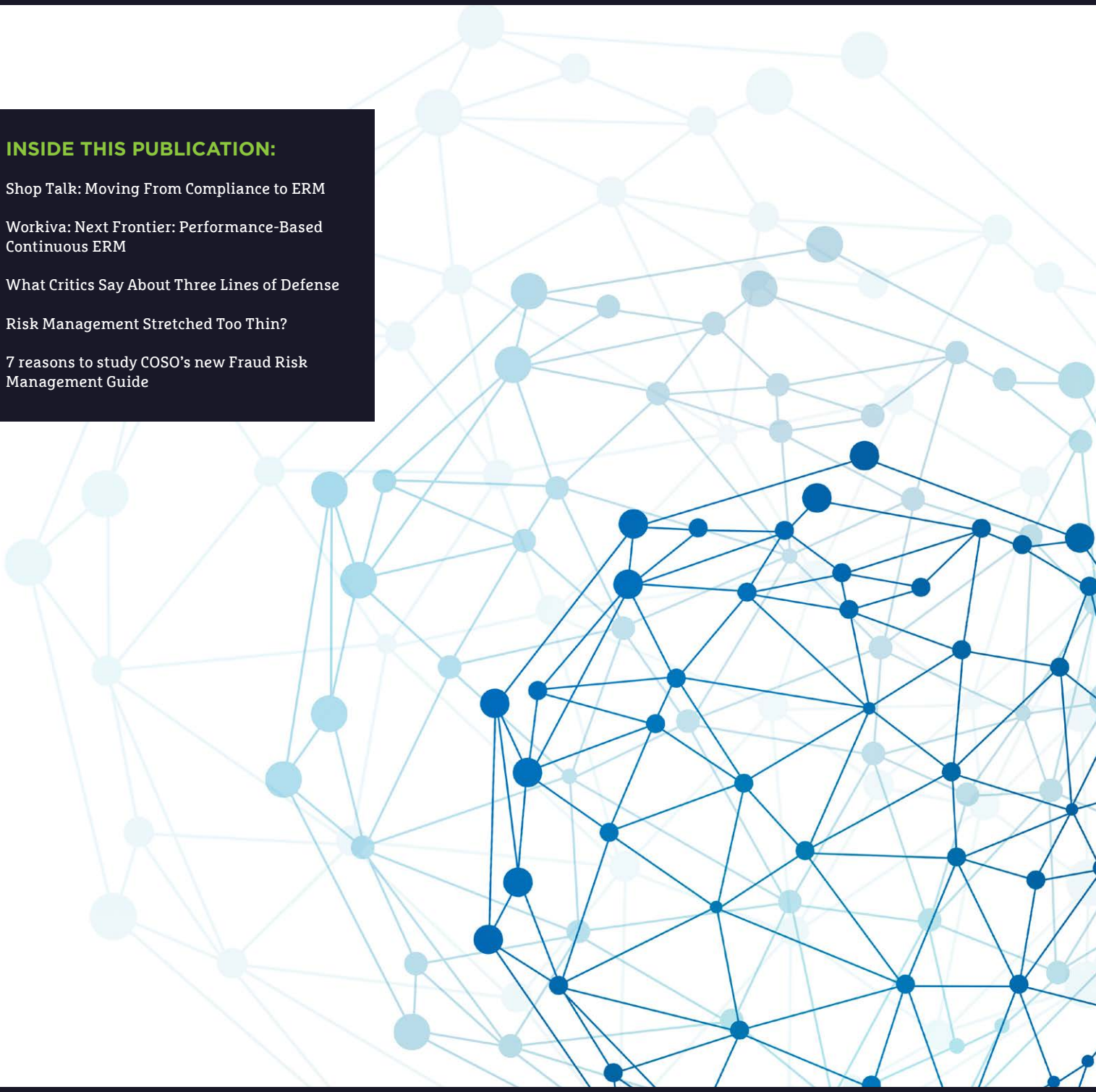
Shop Talk: Moving From Compliance to ERM

Workiva: Next Frontier: Performance-Based Continuous ERM

What Critics Say About Three Lines of Defense

Risk Management Stretched Too Thin?

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



ERM

Understanding the risks, realizing the opportunities

An e-Book publication sponsored by workiva

About us

COMPLIANCE WEEK

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

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

workiva

Workiva is a leading provider of enterprise cloud solutions for improving accountability and insight in business data. Wdesk, a cloud-based productivity platform, helps enterprises collect, link, report, and analyze business data with control and collaboration. Thousands of organizations, including over 65% of the 500 largest U.S. corporations by total revenue, use Wdesk.

Inside this e-Book

Shop Talk: Moving From Compliance to ERM 4

Workiva: Next Frontier: Performance-Based Continuous ERM 8

What Critics Say About Three Lines of Defense 21

Risk Management Stretched Too Thin? 24

7 reasons to study COSO's new Fraud Risk Management Guide 28

Shop Talk: Moving From Compliance to ERM

Where should ERM sit within the company? How do you win support from business units? Compliance, risk, and audit executives sat down to answer those questions at a recent executive roundtable. **Jaclyn Jaeger** has more.

More and more companies want to build their enterprise risk management programs, particularly as emerging risks like cyber-security force their way on to board agendas. The trick is in getting from your compliance routines of today to a more coherent ERM program tomorrow.

To debate the finer points of shifting from a compliance program to ERM, Compliance Week and Workiva recently hosted 10 compliance, risk, and audit professionals in Orlando for an executive roundtable on the subject. "Risk management is not a sequence after compliance," said Mike Rost, vice president of vertical solution strategy with Workiva. "It is its own thing, and every organization is going to come at it differently.

The good news: Most participants said that they are implementing ERM to some degree, even if many are still in the early stages. Some of that effort traces its origins back to compliance with the Sarbanes-Oxley Act, plus good internal auditing principles that require an annual enterprise risk assessment. Little surprise, then, that numerous participants said their internal audit departments still drive their organization's ERM efforts.

For compliance officers, however, housing ERM in internal audit provides only a fraction of the picture, as the risk landscape has rapidly evolved beyond internal control over financial reporting, spilling into other risk areas—such as anti-corruption, anti-money laundering, and cyber-security.

And over the last few decades, companies have moved from possessing mostly tangible assets (factories, land, inventory) to intangible goods (customer lists, marketing data, intellectual property), Rost noted. That means new risks such as reputation management must be fit into ERM programs that never originally anticipated them.

"That's the essence of ERM: How do I know what I don't know? How do I find out what I don't know?" said one executive. Those "black swan" risks—low likelihood, but high impact—that companies have to worry about, the executive said.

Such uncertainty has some audit, compliance, and risk executives doing an intricate dance through the usual Three Lines of Defense model. As one executive put it: "We're figuring out how not to step on each other's toes, but rather how to inform each other in a better way."

Executives with a professional auditing background are in a great position to be involved in the discussion of ERM, another executive said, but "I don't know that they should drive it."

In that aspect, companies may want to take a page from Brambles Ltd. The $5.4 billion global supply-chain logistics company has a vice president who oversees global internal audit and risk management areas together, "so it's housed pretty close together from a global perspective," said George Lewis, senior manager of risk and compliance for CHEP North America, Bramble's subsidiary here.

Data Challenges

Several roundtable participants said the pace of merger activity at their companies often makes it difficult to gather data and understand risks at the enterprise level, since the size of the enterprise keeps changing. "When these mergers and acquisitions happen, it doesn't mean all the technologies come together," said Marie Blake, chief compliance officer at BankUnited.

Following M&A activity, data often is housed on several different systems. That makes like-to-like comparison of key risk metrics difficult. "It's still a challenge," Blake said, and underlines the need for a data warehouse—one central repository where all information about the company and its risks can be stored and then analyzed by audit, compliance, or risk leaders.

In the pharmaceutical industry, for example, regulatory initiatives involving the reporting of payments to healthcare professionals drove the need for data warehouses to capture all data that needs to be reported to the state and federal government.

"This data sits on multiple systems and in various formats," said Deborah Penza, chief compliance officer of Impax Laboratories. "None of these systems ever spoke to one another, so we had to create data warehouses to gather all this data from the various systems and then implement additional systems to aggregate the data and format it to meet the reporting requirements."

The shortcoming with data warehouses, however, is that they depend on people to feed data into it. "The only way to get that data is to beg for it," one executive quipped.

"It is a lot of relationship management," said Aaron Sundquist, compliance data analytics manager for BankUnited. "It's learning to speak other people's language. I often ask the folks in IT, 'How can we communicate better?' It's making sure I get not only what I ask for, but also what I need, and sometimes those are different things."

And getting the data is just the first hurdle; getting value from that data is the second. "One of

Participants gather to discuss enterprise risk management at the recent CW, Workiva roundtable held in Orlando

the challenges is getting people to understand that centralizing compliance information is not centralizing compliance," said Lindsay Koren, senior associate counsel for ethics and compliance at Darden Restaurants. Rather, it's about helping businesses use data effectively to get to a more predictive state, she said.

Board Engagement

Boards are paying more attention to ERM these days. Several roundtable participants said their audit committees or other directors and officers direct them to assess the state of enterprise risk management, particularly those who come from other companies where ERM is a hot topic.

Boards are also getting savvier in the type of information they ask about. "The conversations are around the effectiveness of the controls," Koren said. Putting yourself on the same side of the table as your business partners and catching internal control weaknesses together, as opposed to enforcement authorities coming in and finding those weaknesses, "has been valuable on the relationship-building side, and has given me a lot more insight in terms of whether we've tested the controls," she said.

Where many companies falter in their ERM efforts is that they have several "fire extinguishers" (that is, controls), but "they don't have any clue where their ignition sources (that is, risks) might be," Rost said. Those ignition sources could be with your brand, your third parties, cyber-security—the list is long. Companies should spend less time testing all their controls that have little material impact, and instead focus on their highest risk areas, he said.

Participants also spoke a great deal about which committee of the board should take the

lead on ERM issues. Word of advice: Don't assume the audit committee is your best choice.

"By nature, your audit committee is backward-looking," Rost said. So while it focuses on "blocking and tackling," he said, the company should separately have a board-level risk committee to think creatively about risks. The lack of a formal risk committee makes it difficult to assess all the risks that the company should be thinking about, Rost added.

Audit committees "often are concerned with fire drills, rather than emerging risks," Blake said. Their focus typically is on what happened and what is being fixed. "Banking regulators really are pushing for more board engagement, but that's a tough corner to turn," she said.

Some boards are more sophisticated than others, depending on who sits on that audit committee. "In some cases, the audit committee is becoming the all-risk committee," one executive said. They're being forced by the oversight bodies like the Securities and Exchange Commission to become a forward-looking organization, he said.

Companies still have room to improve, however, in articulating their risk tolerance to the board. "It's an emerging practice for a lot of organizations," Rost said. "Most organizations are in that evolutionary stage of getting there."

For companies that have already identified their risks and laid out mitigation plans, the next hurdle to overcome is how to ensure that the lines of business are actually employing those mitigation measures, attendees said.

"I think we've done it pretty well creating strong cheerleaders along the lines of business to champion the cause when we need them to," Sundquist said. That was achieved by "bringing them direct value through actionable information they can take to monitor their risk."

"ERM is one of those journeys that will never end," Rost said. "Even if you're not a global company, you're still impacted by global factors." That fact alone will continue to elevate ERM at the board level years down the road. ■

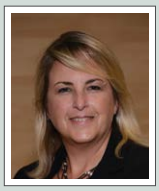
PARTICIPANTS

The following panelists participated in the Sept. 15 CW & Workiva roundtable on compliance collaboration to drive ERM.

Marie Blake
EVP, Chief Compliance Officer,
BankUnited

Lindsay Koren
Senior Associate Counsel, Ethics & Compliance,
Darden Restaurants

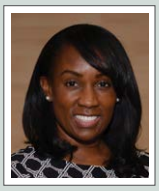
George Lewis
Senior Manager, Risk & Compliance,
CHEP North America



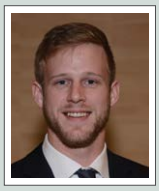
Deborah Penza
SVP & Chief Compliance Officer,
Impax Laboratories

Bryan Rhode
VP, Internal Audit & Compliance,
CSX Corp.

Craig Roshak
Senior Manager, Head of ICFR/SOX and ERM,
Fiat Chrysler Automobile



Michelle Scott
Director,
Corporate Compliance,
SeaWorld



Aaron Sundquist
AVP, Compliance Data Analytics Manager,
BankUnited

WHITE PAPER

workiva

Next Frontier: Performance-Based Continuous ERM

Written by James Lam

The evolution of ERM

From its beginnings in the early 1990s to its current incarnation, enterprise risk management (ERM) has undergone a dramatic transformation. Over the past three decades, ERM has evolved in response to a number of large-scale macroeconomic events as well as the business and regulatory changes those events precipitated. In so doing, ERM has continuously adjusted its core focus and expanded the scope of risk it covers.

Phase One: Tackling financial and operational risk

ERM's first incarnation dates back to the early 1990s. Companies developed ERM programs to address financial concerns such as aggregate market risk and credit risk. In 1993, one of the first authoritative guidance documents to receive wide-scale adoption was the Group of Thirty's (G30) "Derivatives: Practice and Principles." The landmark study provided first-of-its-kind analysis detailing risk exposure within the derivatives marketplace, and offered 24 core risk management recommendations.[1] These recommendations addressed areas such as credit risk, market risk, operations and systems, accounting, and disclosures. Many, if not all, of these topics continue to be primary focal points of ERM functions, especially within the banking and financial services industry.

Unfortunately for a number of derivatives end users—including Orange County, Proctor & Gamble, Gibson Greetings—the G30 report didn't arrive on time to prevent them from reporting significant losses in 1994. At about the same time, risk professionals began addressing operational risk, which grew to prominence thanks to the trading scandals that rocked the marketplace in the mid-1990s. The most prominent of these were the 1994 Kidder Peabody bond trading scandal and the unauthorized futures trading scandal at the British bank Barings in 1995. These incidents highlighted the importance of applying risk management techniques to ongoing operational processes, and ensuring that protocols, policies, and procedures are aligned with the organization's risk appetite. It is also during this period that the role of the chief risk officer (CRO) began to take shape as the executive leader for ERM.

A rash of accounting fraud cases in the early 2000s, headlined by the dramatic failures of Enron and WorldCom, made clear that risk was not limited to market and credit risks. These incidents underscored the risks posed by negligence and fraud within the accounting

1. The G30 report on the Derivative Market provided foundation for risk management frameworks and areas of focus. *Derivatives: Practices and principles.* (1993). Washington, DC: Group of Thirty.

and finance functions of any organization. As a result, many risk management functions quickly adopted operational controls specifically aimed at fraud prevention and detection.

Not surprisingly, these events drew the attention of regulators and lawmakers, who incorporated aspects of operational risk management into new regulatory efforts such as the Sarbanes-Oxley (SOX) Act of 2002.[2] SOX established the foundation for increased oversight with a set of detective and preventative controls to ensure integrity in the financial reporting processes for publicly listed companies.

A few years later in June 2004, The Basel Committee on Banking Supervision published the second installment of its Basel Accords, commonly known as Basel II.[3] Basel II sought to provide a framework within which financial institutions could manage their financial and operational risks. The framework involved the establishment and maintenance of minimum capital requirements, enhancements to supervisory and regulatory oversight and review, and increased marketplace transparency.

Together, these two regulatory actions helped shape the development and adoption of ERM. The increased scrutiny of regulators across the world spotlighted the need for a coordinated risk management effort at the enterprise level. We must keep in mind, however, that such regulations are inherently reactive. Although they addressed unexpected losses resulting from certain financial and operational risks, their limitations would become all too clear.

Phase Two: A compliance-based approach

The world of risk management fundamentally changed in late 2007 with the arrival of the global financial crisis. Longstanding financial institutions such as Bear Stearns and AIG were left to fail, while many other banks and non-banks received bailouts from nervous national governments around the world. It was clear that excessive and fatally compounded risks were the primary driver of the crisis. What's more, a relatively strong global economy had disguised the fact that many institutions were betting on unsustainable levels of growth in pursuit of greater market share and increased profitability.

The regulatory landscape that emerged post-recession was vastly different from what existed prior to the 2007–2008 period. Regulators demanded that banking institutions increase capital and liquidity reserves, enhance transparency, curb risk appetite and tighten controls. In the United States, the Federal Reserve implemented a series of formal stress-testing requirements designed to allow banks to better understand their vulnerability to various risk scenarios. The Comprehensive Capital Analysis and Review (CCAR) assessment implemented by the Federal Reserve provides independent review of the capital plans for banks and bank holding companies in excess of $50 billion in assets. Additionally, the adoption of the Dodd-Frank Wall Street Reform and Consumer Protection Act established that all banks with greater than $10 billion in assets must conduct stress testing on an annual basis.[4] In light of that, the Office of the Comptroller of the Currency (OCC) published final rules in 2014 to meet the stress-testing requirement laid out on Dodd-Frank. Known as DFAST (Dodd-Frank Act Stress Test),[5] the rule requires all banking institutions not covered by CCAR to conduct and report results of formal stress testing exercises.

These laws and regulations also shaped risk governance and oversight at the board level. Section 165 of the Dodd-Frank Act specified that "FRB (Federal Reserve Bank) must require each publicly traded bank holding company with $10 billion or more in total consolidated assets … to establish a risk committee [of the board] … risk committee must … include at least 1 risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms."

---

2. Sarbanes-Oxley increases oversight of publicly registered companies and the methods and processes used in their public financial reporting and disclosure mechanisms through formalization of control structure and the appointment of an independent oversight body over public accounting firms, the Public Company Accounting Oversight Board (PCAOB). *Sarbanes-Oxley Act of 2002*, Pub.L. 107-204, 116 Stat. 745, enacted July 30, 2002.

3. Basel provides recommendations on banking law and regulations. The Basel II Accord sought to address capital needs and reserves necessary to guard against an institution's financial and operational risk. The Office of the Comptroller of the Currency implemented as a final rule the advanced approaches of Basel II on November 1, 2007.

4. Section 165(i)(2) of the Dodd-Frank Wall Street Reform and Consumer Protection Act introduced the stress testing regulatory requirement. The *Dodd–Frank Wall Street Reform and Consumer Protection Act* (Pub.L. 111–203, H.R. 4173).

5. DFAST established the formal program for stress-testing review and reporting, and the OCC's role in that process. *Company Run Stress Test Requirements; Final Rules*, (12 CFR Part 252).

For better or worse, compliance quickly became a primary driver of the risk management function. The formalization of regulatory scrutiny in the financial services industry fundamentally increased the scope and responsibility of the risk management function. The same held true in other sectors. The insurance industry has implemented the Own Risk and Solvency Assessment (ORSA)[6] in order to determine the ongoing solvency needs of insurance institutions with regard to their specific risk profiles.

Economic hardship provided a second driver. The crisis and subsequent recession created hardship that for some companies was an exercise in survival. For many, risk management became risk avoidance in response to grim market conditions. As companies focused on survival and viability, they placed little emphasis on forward-looking risk management initiatives.

These two drivers served to dramatically increase the cost of risk, compliance, and audit activities. Between an unprecedented regulatory burden and reactive risk aversion, ERM programs appeared to be driven by compliance and risk prevention objectives, but yielded little in the way of adding business value. Is there a way for companies and their shareholders to realize a return on their risk management investments?

"The ever-evolving globalization of competitive markets exposes many organizations to a new breed of risks..."

Next Frontier: Creating shareholder value

Today, companies face greater uncertainty in a wide array of new and emerging risks, including cyberrisk from the "internet of everything," climate change, and geopolitical conflicts. The ever-evolving globalization of competitive markets exposes many organizations to a new breed of risks, much of which was not planned for nor could have even been anticipated.

Recent headlines have focused our attention on Federal Reserve interest rate policy, economic slowdown in China, declining oil prices, Middle East instability, international and domestic terrorism, and cybersecurity.

In its ***Global Risks Report 2016***,[7] the World Economic Forum identified five global risks with the greatest potential impact:

1. Failure of climate change mitigation and adaption
2. Weapons of mass destruction
3. Water crises
4. Large-scale involuntary migration
5. Severe energy price shock

Globalization is the common driver among these five risks. No industry, geography, or business model is immune to them. These global risks are also similar in a way that underlies their significance: they are all systemic in nature. If any of these risks—much less a confluence of them—comes to fruition, the downstream impact on business would be catastrophic. In order to respond to these risks tomorrow, institutions must understand their interrelationships and potential impacts today.

Clearly, addressing these major risks reactively is not a viable solution. The scope and severity of risk is so great that doing so could mean economic destruction. Instead, risk management should become proactive, not simply minimizing negative risk but also maximizing opportunity. To do so, ERM must be a continuous process, constantly monitoring and assessing risk in a forward-looking way that provides companies with a path toward opportunity.

For these reasons, ERM is entering a third phase in its development focused on continuous monitoring, business decision support, and shareholder value maximization. Figure 1 provides a summary of the three phases of ERM as discussed above. The next section will discuss the shape of performance-based continuous ERM.

---

6. ORSA was the primary output of the Solvency II initiative and follow-up Solvency Modernization Initiative. The National Association of Insurance Commissioners (NAIC) adopted a formal ORSA rule in 2012. *Risk Management and Own Risk and Solvency Assessment Model Act*, Financial Condition Committee of the National Association of Insurance Commissioners (NAIC), September 6, 2012.

7. *Global Risk Report 2016*, 11th Edition, The World Economic Forum, 2016.

Figure 1: The past, present, and future of ERM

State of ERM	Major events and risks	Key developments

Phase One:
Early 1990s to mid-2000s
	• Derivatives losses (1994): Orange County, Proctor & Gamble, Gibson Greetings
	• Rogue traders (1994–1995): Barings, Kidder, Daiwa
	• Accounting fraud (2000–2001): Enron, WorldCom, Tyco
		• Group of 30 Report
		• Sarbanes-Oxley
		  • VaR models
		  • Real-time market risk management
		  • Operational risk management

Phase Two:
Mid-2000s to present
	• Global financial crisis (2008): Lehman, Bear Sterns, AIG
	• Recent events: Oil price drop, China slowdown, negative interest rates, cyberattacks
		• Dodd-Frank
		• Basel II; ORSA
		  • Stress testing
		  • Scenario analysis
		  • Strategic risk management

Next Frontier:
Coming 5–10 years
	• Cybersecurity
	• "Internet of everything"
	• Climate change
	• Geopolitical risks
	• Global terrorism
		• Basel III
		• Cybersecurity Disclosure Act
		  • Continuous ERM
		  • Collaborative reporting
		  • Performance-based feedback

Performance-based continuous ERM

We now live and work in a new world that is more volatile and uncertain. The speed of change and the velocity of risk have increased significantly. In addition to the uncertain business environment caused by globalization, companies must also deal with shifting consumer preferences, emerging technologies, demographic and workforce changes, climate-change impacts, and natural-resource constraints.

ERM programs must adapt expeditiously. A monthly or quarterly process is no longer sufficient. Just as risks and opportunities are changing continuously, ERM programs monitor and respond on a continuous basis. This is not a pipe dream. It has a precedent in market risk management. Back in the 1990s, trading firms that operated in global financial and commodity markets successfully transitioned from daily to real-time risk management.

In addition to becoming a continuous process, ERM must support key business decisions and add shareholder value. Companies must measure the effectiveness of their ERM programs with objective performance metrics and closed feedback loops.

There are seven key attributes of evidenced-based continuous ERM:

1. **ERM is a continuous** management process that provides early warning indicators for business leaders.
2. **Strategic risk management** receives the highest priority.
3. **Dynamic risk appetite** is well-defined in risk policies to balance business objectives and prudent risk-taking.
4. **Risk optimization** is the primary objective of ERM. This is achieved by influencing the likelihood of positive and negative results along the risk bell curve.
5. **ERM is embedded into business decisions** at all three lines of defense, supported by integrated risk assessment and analytics.
6. **A collaborative dashboard reporting system** delivers ongoing risk and performance monitoring.
7. **Performance feedback loops** assure ERM effectiveness and support continuous improvement.

Let's look at each of these in greater detail.

Attribute #1: ERM is a continuous process

ERM is moving from a periodic monthly or quarterly process to a continuous one. This is essential to align the cadence of ERM with the velocity of risk. As a continuous process, ERM can provide business leaders with timely risk information and predictive analytics on key business drivers, including:

- **Macroeconomic environment:** In an interconnected world, regional, national, and global economic trends can impact the financial performance of any company. A continuous ERM process monitors leading economic indicators on interest rates, energy prices, manufacturing activities, economic growth, business investment, and capital flows. Management can compare these new economic datasets with the assumptions used in the business plan to support timely decisions regarding spending and capital investments.
- **Business processes and operations:** On a daily basis, changes in the business and operating environment can have a significant impact on a company's risk profile. For example, management must respond immediately if there is a supply chain disruption. It may need to take mitigation actions if a key investment falls below expectations or a risk exposure exceeds appetite. Conversely, the company may want to increase risk if the market presents attractive risk-adjusted return opportunities.
- **Employee support and oversight:** Employees represent the lifeblood of any organization. A continuous ERM process supports front line employees in their day-to-day work, including decisions on risk acceptance or avoidance, product pricing, risk transfer strategies, and risk escalation and communication protocols. Employee behavior can also have a material impact on a company's operational and reputational risk. Continuous ERM supports management oversight with respect to employee performance and feedback, compliance with policies and regulations, workplace safety, and risk-mitigation strategies.
- **Customer service:** On average, U.S. corporations lose half of their customers every five years, which an have a large impact on profitability. Given the importance of customer service and retention, business managers should continuously monitor customer service levels, customer complaints and time to resolutions, and customer retention metrics against risk tolerance levels.
- **Counterparties and business partners:** Companies increasingly rely on third parties to support their business and financial operations, including suppliers and vendors, business and outsourcing partners, and financial counterparties. The performance and creditworthiness of these third parties can have an immediate and long-term effect on a company's business model. A continuous ERM process monitors vendor performance against service-level agreements, counterparty stock prices and credit spreads, and problem-resolution updates.
- **Environmental and social impacts:** Long-term sustainability, relative to environmental standards and social expectations, has become a top corporate priority. This includes how a company impacts its environment as well as how the environment impacts the company. The former requires a continuous monitoring of environment and social performance indicators, daily press coverage, and social media posts. The latter requires monitoring extreme weather patterns, natural-resource constraints, and business contingency readiness.
- **IT infrastructure and cybersecurity:** Companies rely increasingly on their IT infrastructures. With the advent of cloud computing, big data, predictive analytics, and the "internet of everything," IT performance and cybersecurity requirements have become a top risk concern for most organizations. A continuous ERM process monitors IT availability and performance as well as cybersecurity metrics such as patch management, incident rate, and mean time to detection and recovery.

Attribute #2: Strategic risk management

Strategy and ERM should be integrated to support the development, execution, and performance monitoring of corporate and business-unit strategies. Companies ignore strategic risks at their peril. Independent studies of

the largest public companies have shown time and again that strategic risks account for approximately 60 percent of major declines in market capitalization, followed by operational risks (about 30 percent) and financial risks (about 10 percent).[8] Yet, in practice, many ERM programs downplay strategic risks or ignore them entirely.

Strategic risk can arise throughout the strategy development and execution processes. The integration of strategy and ERM, or strategic risk management, can add long-term shareholder value in a number of important ways. Strategic risk management lets companies:

- Choose between alternative corporate strategies—organic growth, acquisition, stock buyback—based on their impact on enterprise intrinsic value.[9]
- Ensure that corporate strategies are well-aligned with the company's core mission, business-unit strategies, and operating budgets.
- Assess the strategic and resultant risks from the execution of corporate strategies, including the utilization of risk appetite and risk capacity.[10]
- Support the execution of corporate strategies to achieve key organizational objectives.
- Monitor the actual performance of corporate strategies against management assumptions and expectations, and make timely adjustments as appropriate.

To support strategic risk management decisions, the company's performance management system must integrate key performance indicators (KPIs) and key risk indicators (KRIs). An integrated performance and risk monitoring process would include the following steps:

1. Define the business strategy through a set of measurable strategic objectives.
2. Establish KPIs and targets based on expected performance for those strategic objectives.
3. Identify strategic risks that can drive variability in actual performance, for better or worse, through risk assessments.
4. Establish KRIs and risk tolerance levels for those critical risks.
5. Provide integrated reporting and monitoring in support of strategic risk management.

Unfortunately, many companies perform these actions in two distinct siloes. As part of strategic planning, they perform steps 1 and 2 and report the results to the executive committee and full board. Separately, as part of risk management, they perform steps 3 and 4 and report the results to the risk and audit committees. In order to effectively manage strategic risks, these steps must be fully integrated.

Attribute #3: Dynamic risk appetite

An integral part of continuous ERM is the development of key risk metrics, exposure limits, and governance and oversight processes to ensure enterprise-wide risks are within acceptable and manageable levels. A best-practice approach to addressing these requirements is to implement a formal risk appetite statement (RAS). Corporate directors who are ultimately responsible for overseeing their companies' risk management recognize this need. According to a National Association of Corporate Directors (NACD) survey, only 26 percent of companies have a defined risk appetite statement.[11]

An RAS is a board-approved policy that defines the types and aggregate levels of risk that an organization is willing to accept in pursuit of business objectives. In determining the appropriate risk appetite, an organization should also consider its risk capacity (also known as risk-bearing capacity), which represents a company's overall ability to absorb potential loss. Risk capacity can be measured in terms liquidity and capital reserves, as well as management capabilities and track record in managing the specific risks.

---

8. James Lam, *Enterprise Risk Management: From Incentives to Controls, Second Edition*, Wiley 2014, pp. 434-436.

9. A strategy will add to enterprise intrinsic value if the risk-adjusted return on capital (RAROC) is higher than the company's cost of equity (Ke). See *Strategic Risk Management: The next frontier for ERM*, Workiva, 2015.

10. James Lam, *Implementing an Effective Risk Appetite, IMA®* (Institute of Management Accountants) Statement on Management Accounting, August 2015.

11. National Association of Corporate Directors, "Public Company Governance Survey," 2013-2014.

A dynamic RAS would include the following components:

1. Qualitative statements and guidelines, as well as quantitative metrics and risk tolerance levels for all key risks.
2. A cascading structure of risk tolerance levels with drill-down capability from the board (Level 1) to executive management (Level 2) to business units (Level 3).
3. Continuously updated RAS dashboard reports, including commentaries and expert analysis.
4. Risk-mitigation strategies and exception reporting in the event risk exposures are above tolerance levels.
5. Dynamic adjustments to tolerance levels at the business level to reflect risk-return opportunities. For example, if the market provides return opportunities and the company has excess risk capacity, the risk tolerances may be increased accordingly.

The following example breaks down a strategic RAS into its three primary components:

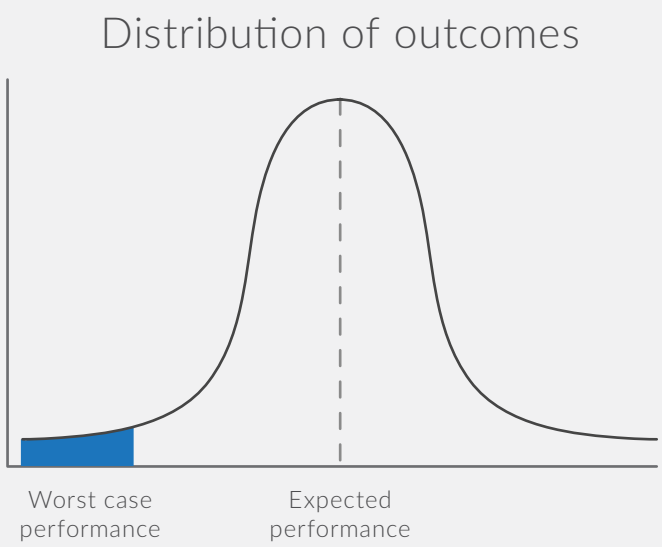
- **Qualitative statement:** To ensure strategic alignment, we will not engage in business activities that are not consistent with our overall strategy and core competencies.
- **Metric:** Non-core investment capital ÷ total capital
- **Risk tolerance level:** Non-core capital ratio will not exceed 10 percent

Attribute #4: Risk optimization

Risk is a bell curve. The bell curve is a graphical depiction of risk with respect to probabilities and outcomes, including expected value (the mean or middle area of the bell curve) as well as the potential upside and potential downside (the tails). The objective of performance-based ERM is to assess, quantify, and optimize the shape of the bell curve for all of the key risks on an ongoing basis.

Although all key risks take the form of a bell curve, not all bell curves are alike. Figure 2 shows how the bell curve can be used to capture various risks.[12]

Figure 2: Risk as a bell curve



Examples:

1. **Strategic risk:** Enterprise value vs. value drivers
2. **Business risk:** Expected EPS vs. earnings drivers
3. **Financial risk:** Net interest margin vs. interest rate changes
4. **Operational risk:** IT performance vs. SPOFs (single points of failure) and cybersecurity
5. **Regulatory risk:** Regulatory standing vs. compliance requirements

12. For simplicity, a symmetrical or normally shaped bell curve is shown. But the specific shape of the bell curve (e.g., shape, skewness) will depend on individual risks faced by an organization.

Interest rate risk or market risk can be plotted on an essentially symmetrical curve, as interest rates or market prices have an equal chance of moving favorably or unfavorably. On the other side of the spectrum, operational and compliance risk have a limited upside but a lot of potential downside. After all, not having any IT, compliance, or legal issues simply means business as usual. But a major negative event, such as a security breach, IT downtime, or regulatory issue, can have tremendous negativedownside consequences.

If managed well, strategic risk is unique in that its downside can be limited while its upside can be unlimited. For example, the maximum loss of a new investment is 100 percent of the investment, but a new business venture can produce multiples of the investment. An asymmetrical bell curve with significant upside risk can describe any new product or business opportunity, whether that opportunity is part of a corporation's growth strategy or a venture capital firm's new investment.

Consider a decision tree that maps the probabilities and consequences of different decision paths.[13] This map not only provides a better picture of the risks and rewards involved, but also helps identify trigger points for action if the initiative lags behind expectations. Taken this way, the optimum strategic risk profile resembles a call option: limited downside exposure with unlimited upside potential. A company can also limit downside risk by failing faster. The sooner a company recognizes an initiative is in trouble, the sooner it can take corrective action—such as getting the initiative back on track, deploying risk mitigation strategies, or shutting it down.

Minimizing downside risk and increasing the upside is the objective of real option theory. A real option is the right, but not the obligation, to undertake a business investment or change any aspect of that investment at various points in time, given updated information. The beneficial asymmetry between the right and the obligation to invest under these conditions is what generates the option's value.

Venture capital (VC) firms take advantage of this asymmetry as part of their business model. According to research by Shikhar Ghosh, a senior lecturer at Harvard Business School, about 75 percent of venture-backed firms in the United States do not return investors' capital, 20 percent achieve subpar returns, and only 5 percent achieve or exceed the projected return on investment.[14] To maintain an ideal risk profile, VCs carefully stagger funding rounds in order to reap outsized returns on the 5 percent of firms that are successful while exiting or minimizing their investments in the other 95 percent.

Pharmaceutical companies take a similar portfolio approach. They invest in drug development internally or acquire promising patents or entire drug companies. They can then continue to make limited, iterative investments in successful ventures and bow out of those that fail to achieve expected performance levels.

Attribute #5: ERM-based decision support

In order to add value, the continuous ERM process must be integrated into the strategic, financial, and operational decisions of the organization. Generally speaking, organizations have the following options available to them in response to risk:

- **Risk acceptance or avoidance:** The organization can decide to increase or decrease a specific risk exposure through its core business, mergers and acquisitions, and financial transactions. This includes new product development, market expansion, acquisitions and divestitures, and capital budgeting and financing activities.
- **Risk mitigation:** An organization can establish risk control processes and strategies in order to manage a specific risk within a defined risk tolerance level. This includes constructing a risk appetite statement with explicit risk tolerance levels, corporate risk policies, risk measurement and monitoring systems, and risk control strategies and contingency plans.
- **Risk-based pricing:** All firms take risks in order to be in business, but there is only one point at which they can get compensated for the risks that they take. That is in the pricing of their products and/or services. A product's price must always incorporate its share of the cost of risk. Similarly, companies should fully account for the cost of risk to measure the risk-adjusted profitability of business activities.

---

13. The classic decision tree is a similar construct as a bell curve, except that it is displayed sideways and used to support decision making at critical junctures.

14. Deborah Gage, "The Venture Capital Secret: 3 out of 4 Start-Ups Fail," *The Wall Street Journal*, September 20, 2012.

- **Risk transfer:** An organization can decide to execute risk transfer strategies through the insurance or capital markets if risk exposures are excessive and/or if the cost of risk transfer is lower than the cost of risk retention. Risk transfer strategies include hedging with derivative products, corporate insurance and captive insurance strategies, and securitization programs.

- **Resource allocation:** An organization can allocate human and financial resources to business activities that produce the highest risk-adjusted returns in order to maximize firm value. This includes rationalizing the allocation of staff resources, economic capital, and financial budgets based on projected risk-adjusted performance.

While it is important to understand the general categories of choice an organization can make as discussed above, in practice, each risk management decision is made by a specific committee, function, or individual. These decision-makers can be the members of the board, corporate management, or business and functional units. Here is a summary of key risk management decisions based on the three lines of defense model:

- **Business units and support functions** represent the first line of defense. The first line is ultimately accountable for measuring and managing the risks inherent in their own businesses and operations. Since they must assume some level of risk to achieve their business objectives, the goal is to take intelligent risks. Key business and risk management decisions include accepting or avoiding risks in day-to-day business activities and operations; establishing risk-based product pricing; managing customer relationships; and implementing tactical risk mitigation strategies and contingency plans in response to risk events.

- **Corporate management,** supported by the ERM and compliance functions, represents the second line of defense. Management is responsible for establishing and implementing risk and compliance programs, including risk policies and standards, risk appetite and tolerances, and reporting processes for the board and management. The second line of defense is accountable for ongoing risk monitoring and oversight. Key business and risk management decisions made at this level include allocating financial and human capital resources to business activities that produce the highest risk-adjusted profitability; implementing organic and/or acquisition based growth strategies; and devising risk transfer strategies to reduce excessive or uneconomic risk exposures.

- **The board of directors,** with the support of internal audit, represents the third line of defense. The board is responsible for establishing the company's risk governance structure and oversight processes; reviewing, challenging, and approving risk policies; and overseeing strategy execution, risk management, and executive compensation programs. The third line of defense is also accountable for the periodic review and assurance of risk management effectiveness. Key business and risk management decisions include establishing the statement of risk appetite and risk tolerance levels; reviewing and approving management recommendations with respect to capital structure, dividend policy, and target debt ratings; and reviewing and approving strategic risk management decisions, including major investments and transactions.

Attribute #6: Collaborative dashboard reporting

One of the key objectives of continuous ERM is to promote risk transparency with enhanced reporting. The old adage "what gets measured gets managed" certainly holds true in risk management, and business leaders appear to be getting the message. In a 2011 Deloitte study of approximately 1,500 executives across various industries, 86 percent identified "risk information reporting" as a high or moderate priority, making it the most highly prioritized of 13 risk initiative options.[15] What's more, this priority was followed closely by "risk data quality and management" (76 percent) and "operational risk measurement system" (69 percent). Clearly, management understands that establishing a robust risk measurement and reporting system is critical to ERM success.

The ideal way to achieve this objective is with a real-time collaborative dashboard reporting system. This system would produce role-based reports designed for the decision-making requirements of each recipient. When

15. *Global Risk Management Survey, 7th Edition: Navigating in a Changed World*, Deloitte, February, 2011, p. 42.

designing a role-based dashboard report, it is useful to determine the key questions each recipient needs to address. For example, the ERM dashboard for the board and senior management may address the following five basic questions:

1. **Are any of our business objectives at risk?** As discussed, a company's RAS defines risks according their effects on primary business objectives. The ERM dashboard should similarly organize risk information (e.g., quantitative metrics, qualitative risk assessments, early warning indicators) within the context of key strategic and business objectives. For each objective, the dashboard report might show green, yellow, or red indicators to signal that its achievement is on track, threatened, or off track, respectively. For objectives with yellow or red indicators, the board and management should then be able to drill down to underlying analyses.

2. **Are we in compliance with policies, regulations, and laws?** The ERM dashboard should indicate at a glance the company's compliance status in regard to key policies, regulations, and laws. Again, traffic light signals would highlight whether the company is in full compliance (green), approaching violation (yellow), or in violation (red). Drill-down capabilities would support further analysis with respect to more detailed compliance metrics and reports.

3. **What risk incidents have been escalated?** The ERM dashboard should be able to escalate critical risk incidents to the appropriate board members, executives, or managers in real time. This capability would require a system to capture incidents throughout the company that meet a defined threshold (e.g., customer impact, financial exposure, reputational impact, etc.). Moreover, the ERM dashboard needs an embedded algorithm that prioritizes risk incidents and escalates them to the proper individuals. The most critical incidents should prompt alerts via email, text, or other system for immediate response.

4. **What key performance indicators (KPIs), key risk indicators (KRIs), or early warning indicators require attention?** A key goal of an ERM dashboard is to highlight potential problems before they become critical. For that reason, the dashboard should include early warning indicators that help foreshadow such issues. A well-designed ERM dashboard would provide KPIs and KRIs that are most relevant to the decision-making needs of each user, whether at the board, management, or business-unit level. Ideally, each metric would include performance thresholds and/or risk tolerance levels to provide benchmarks for evaluation.

5. **What risk assessments must we review?** Risk assessment is an ongoing process, with top-down risk assessments, bottom-up risk/control self-assessments (RCSAs), regulatory examinations, and audit reports taking place on a regular basis. Given that these assessments include mainly qualitative information, the dashboard need only provide a summary of key findings and analyses. Each such summary should indicate whether it meets board and management expectations (green), is near those expectations (yellow), or falls short (red). When more detailed review is necessary, the actual risk assessments and reports would be available via drill-down.

"One of the key objectives of continuous ERM is to promote risk transparency with enhanced reporting."

In addition to the above components of dashboard reporting, new features are surfacing that are becoming part of the emerging reporting standards. An established dashboarding system should incorporate the following elements for streamlined reporting:

- **Single-source publishing:** Software that publishes the same data in multiple places at once across a platform effectively eliminates duplicate content. Single-source publishing not only makes reporting more accurate, it also increases efficiency and frees up time for making important business decisions instead of managing data. The same technology can also produce dynamic charts that respond to data as it changes.

- **Collaborative real-time editing:** Advanced software platforms, often cloud-based, permit multiple users to work on a single document at the same time, with changes displayed in real time.

Such functionality permits each user to have up-to-date data as soon as it becomes available. This technology is becoming increasingly powerful and simpler to deploy across the organization, making it essential to support continuous ERM reporting.

- **Data visualization:** Many dashboarding applications now have the ability to create graphs or presentations seamlessly with underlying data, making it far more impactful and actionable. Consider the impact and clarity of a pie chart or bar graph compared to a dense table of numbers. Whether the user is a chief risk officer or an IT manager, being able to clearly visualize risk data can dramatically improve risk monitoring.

- **Interactive data displays:** The best data presentation is dynamic, allowing users to see summaries but giving them the ability to drill down into the underlying details. The next step in interactivity, however, will allow users to have a conversation with the data, by asking human-readable questions of the database and receiving answers pertinent to business objectives. While this is still a mostly experimental feature of dashboarding, the advances in artificial intelligence should make such features available in the coming years.

"Well-crafted feedback loops support self-correction and continuous improvement..."

Attribute #7: ERM performance feedback loops

Well-crafted feedback loops support self-correction and continuous improvement by adjusting a process according to the variances between actual and desired performance. As a foundational component of the scientific method, the feedback loop has long been an essential tool used to support advances in many fields, including economics, engineering, and medicine. More recently, the innovative use of feedback loops has been reported in the hedge fund industry[16] and the effective altruism movement.[17] It would be difficult to evaluate and improve any process efficiently without a performance feedback loop. Risk management is no exception.

Unfortunately, the most common practice is to evaluate the effectiveness of risk management based on the achievement of key milestones or the lack of policy violations, losses, or other unexpected events. However, qualitative milestones or negative proves should no longer be sufficient. Organizations need to establish performance metrics and feedback loops for risk management. Other corporate and business functions have such measures and feedback loops: business development has sales metrics, customer service has customer satisfaction scores, HR has turnover rates, and so on.

In order to establish a performance feedback loop for ERM, companies must first define its objective in measurable terms. One could define the objective of ERM, for instance, as minimizing unexpected earnings volatility. The goal in this instance is not to minimize absolute levels of risks or earnings volatility, but just that from unknown sources.

Once we define the objective, we can create the feedback loop. Figure 3 illustrates the use of earnings volatility analysis as the basis of such a performance feedback loop.

At the beginning of the reporting period, the company performs earnings-at-risk analysis and identifies several key factors (business targets, interest rates, oil price, etc.) that may result in a $1 loss per share, compared to an expected $3 earnings per share. At the end of the reporting period, the company performs earnings attribution analysis and determines the actual earnings drivers. The combination of these analyses provides an objective feedback loop on risk management performance. Over time, the organization strives to minimize the earnings impact of unforeseen factors. Bear in mind that this is simply one example. While this may not be the right feedback loop for an individual organization (for example, nonprofits), every company should establish one or more feedback loops for risk management.

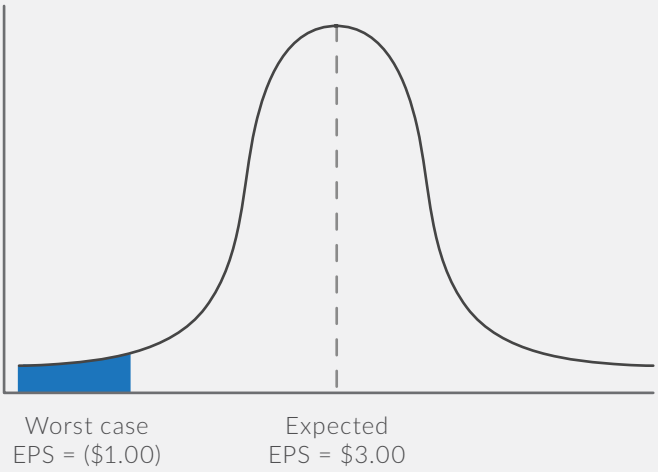
---

16. Bridgewater is one of the largest and most successful hedge funds in the world. The founder, Ray Dalio, argues for the use of a performance feedback loop to monitor and shape organizational effectiveness. Ray Dalio, Principle #66, *Principles*, www.bwater.com, 2011.

17. Effective altruism is a new, evidence-based approach to charitable giving. The cofounder, William MacAskill, advocates the use of objective feedback loops to determine the effectiveness of altruistic pursues. William MacAskill, *Doing Good Better*, Gotham Books, 2015.

Figure 3: Establishing a feedback loop on ERM

Earnings-at-risk analysis ⟷ Earnings attribution analysis



Expected EPS :	$3.00
Actual EPS:	$1.00
Difference:	**$2.00**

Business plan:	$1.00
Interest rates:	$0.50
Key initiatives:	$0.10
Unforeseen factors:	$0.40
	$2.00

1.	Business plan:	$2.00
2.	Interest rates:	$1.00
3.	Oil price:	$0.50
4.	Key initiatives:	$0.30
5.	Expense control:	$0.20
		$4.00

Key questions:

1. Did we identify the key risk factors?
2. Were our EPS sensitivity analyses accurate?
3. Did risk management impact our risk/return positively?

Summary

The global economy and business world have evolved significantly over the past three decades, and so has the practice of ERM. As companies face large financial and reputational damage from derivatives losses, unauthorized trading, accounting fraud, global recession, and cybersecurity threats, the scope and focus of ERM has expanded to include financial risk, operational risk, strategic risk, regulatory-compliance risk, and cybersecurity risks. Given the increase in macroeconomic and business uncertainties, regulatory standards, and risk velocity, ERM must continue to evolve.

Acknowledgements

The author would like to thank members of the Workiva ERM Team, Joe Boeser, Mark Ganem, Jay Miller, and Sholanki Sarkar, for their invaluable contributions.

About Workiva

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. For more information, visit workiva.com.

About the author

With over 25 years of risk management experience, James Lam is often cited as being the first Chief Risk Officer. An early advocate for enterprise risk management, he served as Partner of Oliver Wyman, Founder and President of ERisk, Chief Risk Officer of Fidelity Investments, and Chief Risk Officer of GE Capital Market Services.

Lam is currently the president of James Lam & Associates, a leading risk management consulting firm. In addition, he is a member of the Board of Directors at E*TRADE Financial Corporation where he was named Chair of the Risk Oversight Committee. James also serves as a Senior Advisor for Workiva.

Lam's many accolades include receiving the inaugural Risk Manager of the Year Award from the Global Association of Risk Professionals in 1997. Additionally, he was named one of the "100 Most Influential People in Finance" three times by *Treasury & Risk Management* magazine.

After receiving his BBA from Baruch College and graduating summa cum laude, Lam completed his MBA with honors at UCLA. In addition to lecturing at Harvard Business School, he has taught courses in risk management at Babson College and Hult International Business School.

The information contained herein is proprietary to Workiva and cannot be copied, published, or distributed without the express prior written consent of Workiva © 2016.

workiva

workiva.com
info@workiva.com
+1.888.275.3125

What Critics Say on Three Lines of Defense Strategy

The Three Lines of Defense model for risk oversight has been hugely popular in recent years. Critics, however, say the Three Lines model is too simplistic a vehicle for a challenge as complex as risk management. **Joe Mont** takes a contrarian look.

The Three Lines of Defense model for risk oversight—business units in the first line, compliance in the second, internal auditors in the third—has been all the rage in the last few years. Proponents have come to love it, and regulators have come to expect it.

And now some thinkers in corporate compliance have come to attack it.

The critics, and plenty of them are out there, challenge the very premise of the Three Lines model as flawed. One risk-management consultant has even called it "asinine."

The strategy in a nutshell: business units are the first line and responsible for assessing and controlling their own risks; the second line of risk management, compliance, and legal ensures that those risks are identified and managed; the final backstop, internal audit, independently assesses the effectiveness of the processes created in the previous lines.

What could be wrong with that ostensibly common-sense approach? Plenty, says Norman Marks, a self-described "evangelist for better run business," former chief compliance officer, and prolific writer on these issues.

A recent blog post Marks wrote, "The Three Lines of Defense Model Is the Wrong Model," along with a debate on the model hosted in December by the consulting firm Risk Audit Professional Development, has fired up what was previously just an academic discussion. "The model perpetuates the silly idea that risk managers and internal auditors are there to stop operating managers from taking too much risk," Marks wrote. "That model is one of confrontation, and not how the best risk managers work."

Marks stresses that "risk management is not about avoiding risk"—rather, it is about "taking the right level of the right risk."

"You need to be able to take risk, and the management of that risk is how you manage the business," he says. "It is how you address the uncertainly that lies between where you are and where you want to go. If you want to be successful you have to know what risks to take and which to leave behind."

The Three Lines, built around the concept of defense, "sets the image from the beginning that it is all about protecting the value of the organization, rather than actually embracing the management of risk as a path to success," Marks adds.

Marks appreciates the sentiment that internal audit does not have responsibility for management decisions or operating the business; that's a point any audit or compliance executive would wholly support. But the Three Lines model makes it "in the wrong context," he says.

"If risk management is seen as a compliance exercise or to avoid disasters, but not as part of how you are going to achieve your earnings objectives or grow revenue, it is not being positioned properly and not going to get the resources it needs," Marks says.

Mixed Messages on Risk

Richard Anderson, director of the Anderson Risk consulting firm in London, says one side effect of the clear-cut divisions of responsibility is that they may stifle important conversations about risk that should take place across the whole enterprise. "Where you have rigid adherence to the model, the quantity and quality of those conversations decreases," he says. "It

is affecting the quality risk management, because if people aren't talking about risk, they are not going to be managing risk."

The model also "codifies the creation of silos," he says.

"It is really important that everybody is focused on risk and control, as well as doing their business," Anderson says. "If you say someone is responsible for doing the business, somebody else is responsible for setting the policy for risk, and somebody else is re-

BREAKING DOWN THE LINES

The following, from a position paper issued by the Institute of Internal Auditors, looks at the responsibilities and interactions at each level of the Three Lines of Defense.

The First Line of Defense: Operational Management

- As the first line of defense, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies.
- Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.
- Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives.
- Through a cascading responsibility structure, mid-level managers design and implement detailed procedures that serve as controls and supervise execution of those procedures by their employees.
- There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events.

The Second Line of Defense: Risk Management and Compliance Functions

The specific functions will vary by organization and industry, but typical functions in this second line of defense include a risk management function (and/or committee) that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization. The responsibilities of these functions can include:

- Supporting management policies, defining roles and responsibilities, and setting goals for implementation.
- Providing risk management frameworks.
- Identifying known and emerging issues.
- Identifying shifts in the organization's implicit risk appetite.
- Assisting management in developing processes and controls to manage risks and issues.
- Providing guidance and training on risk management processes.
- Monitoring implementation of effective risk management practices by operational management.
- Alerting operational management to emerging issues and changing regulatory and risk scenarios.
- Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.

The Third Line of Defense: Internal Audit

Internal auditors provide the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organization. This high level of independence is not available in the second line of defense. Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives.

Source: The IIA.

sponsible for checking it, you are immediately imposing a level of dysfunction that is counter-productive."

The intentional simplicity of the Three Lines' underlying metaphor also worries critics. The push for plain English descriptions of complex business practices is a growing trend, they say—well-meaning, but filling conversations about risk, compliance, and regulatory oversight with vague terms. What exactly is "culture," "tone at the top," or "risk appetite," anyway?

"There is a belief that if you over-complicate anything, you can't explain it to the board," Anderson says. "But these guys aren't stupid. They are all bright people, and that's how they got to where they are. We've got to understand the complexity and then find ways of reporting it. There is no point in imposing simplicity before you have done the more complex analysis."

Peter Bonisch, a partner with Paradigm Risk Consulting, agrees. "All this simplification is fine, but when you simplify away essential elements of the story, all you are doing is introducing a different form of complexity at a different stage in the process," he says. "You just end up building in problems elsewhere."

Nor are the Three Lines critics pleased that its simple approach has worked its way into the mindset of regulators.

"It worries me that a flawed metaphor has been grasped so firmly by regulators," Bonisch says. "Why is it that when we are talking about corporate financial principles we can't use the language of corporate finance? Why is that that when we talk about accounting principles we can't use the language of accounting? Why do we have to lay over this presumed simplicity which just means a different thing to everyone who hears it, and therefore introduces complexity?"

There are, of course, many voices supporting the Three Lines approach. It is "a brilliant philosophy," says Robert Croft, an executive director at Nomura International, who squared off with Anderson at the Risk Audit Professional Development debate. "What can be simpler than having the people who take the risk in the first line, the people who monitor the people taking the risk in the second line, and then people who check what the first line and the second line are doing in the third line?"

"Simple and elegant" is how Richard Fowler, a senior audit specialist at shipbuilder Huntington Ingalls Industries, described the model in a written response to Marks. "All it is suggesting is that there is a hierarchy within the organization in treating risks."

"Suggesting that the model is wrong seems to be reaching too far and discrediting all the effort put forth by many valuable internal auditors to develop it," says Tom Brothers, director of internal audit and enterprise risk management at First Guaranty Bank in New Orleans.

Where does the debate go from here? While nobody expects the Three Lines model to transform radically or go away any time soon, there is hope that businesses will take a broader view of how they approach risk and the roles various parts of the enterprise play in risk management.

"We should be looking at the proper positioning and understanding of risk management and internal audit, because this model affects both," Marks says. "It is making everybody the 'Department of No,' instead of the 'Department of How.' We need to say that risk management is there to help the board and management take the right risk, with internal audit there to provide assurance over the processes that management uses to take the right level of the right risk."

Anderson fears that the Three Lines model, like many other post-crises reactions from Sarbanes-Oxley to the Dodd-Frank Act, will be enshrined and seen as a cure-all.

"I've heard a number of people say that if only we had implemented the Three Lines of Defense properly in the banks before the global financial crisis, it wouldn't have happened," he says. "What a load of utter and complete codswallop. All of these things are looking at simple prescriptions and simplicity is the enemy of understanding risk and risk management." ■

"If risk management is seen as a compliance exercise or to avoid disasters, but not as part of how you are going to achieve your earnings objectives or grow revenue, it is not being positioned properly and not going to get the resources it needs."

Norman Marks, Audit Expert

Risk Management Stretched Too Thin at Some Companies

Prioritizing risks in order of magnitude may make sense, but some risk managers say that those efforts could miss less common, but more severe events or scenarios. **Joe Mont** has more.

Will the current Ebola outbreak wreak havoc on your supply chain? Could hackers successfully breach your security perimeter and steal sensitive information without you even knowing about it? Will geopolitical unrest, notably conflict in the Ukraine and political demonstrations in Hong Kong, complicate dealings with partners in those regions? Could another volcano in Iceland ground air travel from Europe, adding shipping delays? Perhaps some other natural disaster?

Of all the risks that keep company executives up at night, there may be no bigger nightmare than a threat they don't see coming.

There is a very long list of large firms that have blamed (rightly or not) black swan events for their woes: MF Global, Arthur Anderson, Bear Stearns, Lehman Brothers, AIG, and BP among them. "What you can gather from the length of the list is that black swans are not rare," says Mark Hale, director of business and operations for CHAPS, a payment processing firm.

A flurry of new regulations and a long list of massive fines against companies for violating bribery, money laundering laws, and other rules have required companies to take a risk-management approach to compliance, devoting the most resources to the potentially most costly risks. But some risk-management experts say that those efforts are stretched too thin and could miss less common, but potentially more devastating events or scenarios.

The term "black swan," coined by author Nassim Nicholas Taleb in his 2001 book "Fooled by Randomness," became a catch-phrase throughout the financial crisis to describe the perfect storm that sank financial giants like Lehman Brothers. By definition, these are unexpected, unpredictable disasters that can only be picked apart and explained after the fact. These unwanted surprises once considered rare, are becoming increasingly common.

Back to the Breach

Cyber-security failures are a unique twist on black-swan events. It isn't that breaches and the theft of customer data by hackers is unheard of—big breaches at Home Depot, Target, and JPMorgan have amplified concerns. The problem is that a company may not even know its security measures failed until that one fateful morning it finds regulators knocking on its door because millions of customer records have been pilfered.

"The threat of outsider attacks by black-hat hackers is not a new phenomenon," Michael McGovern, managing director and CIO for Brown Brothers Harriman says. "It has been going on for many years, but a number of things have happened. There is the emergence of state-sponsored hackers. Target is also a great example because it was one of their suppliers that had a breach, so the extended ecosystem is an area that regulators are increasingly focused on. The level of sophistication of hackers and the evolving threat matrix firms have to contend with has created a situation where there is a tremendous need to stay ahead of the frontier and anticipate the next wave of vulnerabilities."

"The good news is that there are tremendous tools available," he adds. "But hackers are only getting

more sophisticated, so it is a war that has to be fought constantly by investing in talent and the tools."

The current regulatory environment can both alleviate some risks and exacerbate others. Although the term black swan may not pop up in the Federal Register, regulators are making these unpredictable risks a priority.

The Securities and Exchange Commission, for example, expects to soon finalize Regulation SCI (the acronym stands for "systems, compliance, and integrity"). It would require exchanges and clearinghouses, to have comprehensive policies and procedures in place to secure their technology. It requires that systems have adequate capacity, integrity, resiliency, availability, and security, and that they are well-positioned to promptly take appropriate corrective action when problems arise. The rule requires designating individuals or firms to participate in the testing of business continuity and disaster recovery plans at least once annually and to coordinate testing on an industry or sector.

In the wake of Hurricane Sandy, a black-swan weather event that hit New York and New Jersey, the SEC also issued guidance that stressed the need for firms to have response plans, redundancies, and business continuity efforts in place in response to a natural disaster or terrorism attack. Much of that guidance drew from lessons learned following the 9/11 attack on the World Trade Center, the blackest of black-swan events.

Much of the Dodd-Frank Act also focused on big risk events, requiring financial firms to put more protections in place and adequate recovery mechanisms to rebound in tough times. The legislation, for example, requires that banks hold sufficient capital buffers to weather unexpected disasters like a credit market collapse or a run on deposits. Annual stress tests ordered of banks by financial regulators is another tool intended to ensure they can weather any storm, expected or unexpected.

But the flurry of new regulations and recordbreaking fines may open companies up to new risk. Because companies devote a limited amount of resources to risk assessment and mitigation, some will consider merely shuttering any business line that could cause trouble. It is a fear activists had when the SEC implemented its Conflict Minerals Rule, for example. "Certain companies are getting out of certain business lines because they say it doesn't make sense anymore because of the risk compared to revenues," Luc Vantomme, chief risk officer for Euroclear, a firm that specializes in settlements for securities transactions, says.

Another response is to prioritize risks, rather than deal with them holistically. An example is how banks respond to the potential for money laundering in trade finance, the practice of financial institutions underwriting cargo shipments, says Hugh Jones, president and CEO of Accuity. These shipments, through falsified records, can be used for money laundering. "Currently in trade finance we don't see a lot of fines, so we don't see a lot of banks rushing into the trade finance arena with new investments to even investigate whether there is fraud going on," Jones says

Given the unpredictable nature of black swan events, and the temptation to de-emphasize under-the-radar risks, how should compliance and risk officers respond? To start with, a company's enterprise risk management system can indeed assess all risk factors, big and small, Alison Clew, global leader of AML sanctions and compliance for Deloitte, says.

"If you do a risk assessment, you are evaluating all kinds of inherent risks and you have to be super creative and challenge yourself about what the inherent risks are," she says. "You are also constantly challenging your controls evaluation. The control side is where you have to push the envelope."

"I truly believe that if you treat your risk assessment as a living and breathing tool and you bring that external knowledge into your controls assess-

"If you don't think you are subject to cyber-attack now, that probably means you have been compromised already. That tells us that we have to change our approach from preventative and move to the assumption that something has already happened."

Mark Hale, Director of Business and Operations, CHAPS

ment, you have a better chance of prioritizing even small things," she adds.

Ditch the Rear-View Mirror

Another suggestion is to look forward, not backward. How an event unfolded in the past may not mirror the threat you eventually face. "History is not always a good guide," Vantomme says. "Many firms have been building their systems looking backward to what has happened before to try to predict what the future is. We need to learn not to do that."

McGovern suggests table-top exercises and role play, bringing together a variety of in-house expertise to brainstorm imaginative threats they might face. "The collective expertise can help expand each other's thinking about what is in the realm of the possible in terms of a black swan event and then from there developing plans," he says, adding that suppliers and partners may be part of this process.

Companies shouldn't be afraid to reach out to others in their sector, or collaborate with those outside their industry, suggests Hale. "You should be prepared to learn from other organizations that do this sort of stuff very well," he says. "For banks, secrecy and data protection is in their DNA. The nuclear industry, however, understands the extreme effect of black swan events and it is a regular practice for their IT and risk teams to get together and share everything so they can have collaboratively reduced risk thresholds."

"You have to go through failure to understand what success might look like," Hale adds. "I see really smart organizations take in people who have had failures under their belt. Nobody is better prepared to prevent something from happening than somebody who has already experienced the pain." ■

BUTTONING DOWN BUSINESS CONTINUITY

The following is from a Securities and Exchange Commission advisory on business continuity plans for investment advisers.

Hurricane Sandy caused significant and wide-ranging damage across the northeast coast of the United States on Oct. 28 and Oct.29, 2012, which led to the closure of the equities and options markets. The storm prompted the SEC's National Examination Program to review the business continuity and disaster recovery plans of approximately 40 advisers in the impacted areas to assess their compliance with applicable laws, rules, and regulations relating to business continuity plans (BCPs).

Observations

- Advisers generally adopted and maintained written BCPs. The degree of specificity of the advisers' written BCPs varied; some had also developed specific BCPs for Hurricane Sandy just prior to the storm's arrival.
- Advisers also generally distributed their BCPs widely within their businesses and operations. In some cases, employees were required to sign that they have received the plan annually, along with the compliance manual and code of ethics.
- Some advisers' compliance personnel worked collaboratively with the advisers' various business lines to develop the BCPs and sought to achieve redundancy in key services and operations.
- Some advisers required all business units to identify contingency scenarios that would affect operations and derive multiple solutions to help ensure the advisers could meet their fiduciary duty to clients.
- Some advisers formed special committees to plan, develop, test and, if necessary, execute the advisers' BCP.

Weakness Noted

- Some advisers adopted BCPs that did not adequately address and anticipate widespread events. These advisers generally experienced more interruptions in their key business operations and inconsistent communications with clients and employees. For example, some advisers did not have adequate plans addressing situations where key personnel, such as portfolio managers, were unable to work from home or other remote locations.

Source: SEC.

wdesk

Wdesk helps teams work smart.

Strengthen your risk culture and enable better risk-based decisions by connecting real-time data across all lines of defense.

To see how Wdesk can help you improve enterprise risk management,
visit workiva.com/erm

workiva

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bob Hirth, Chair, COSO