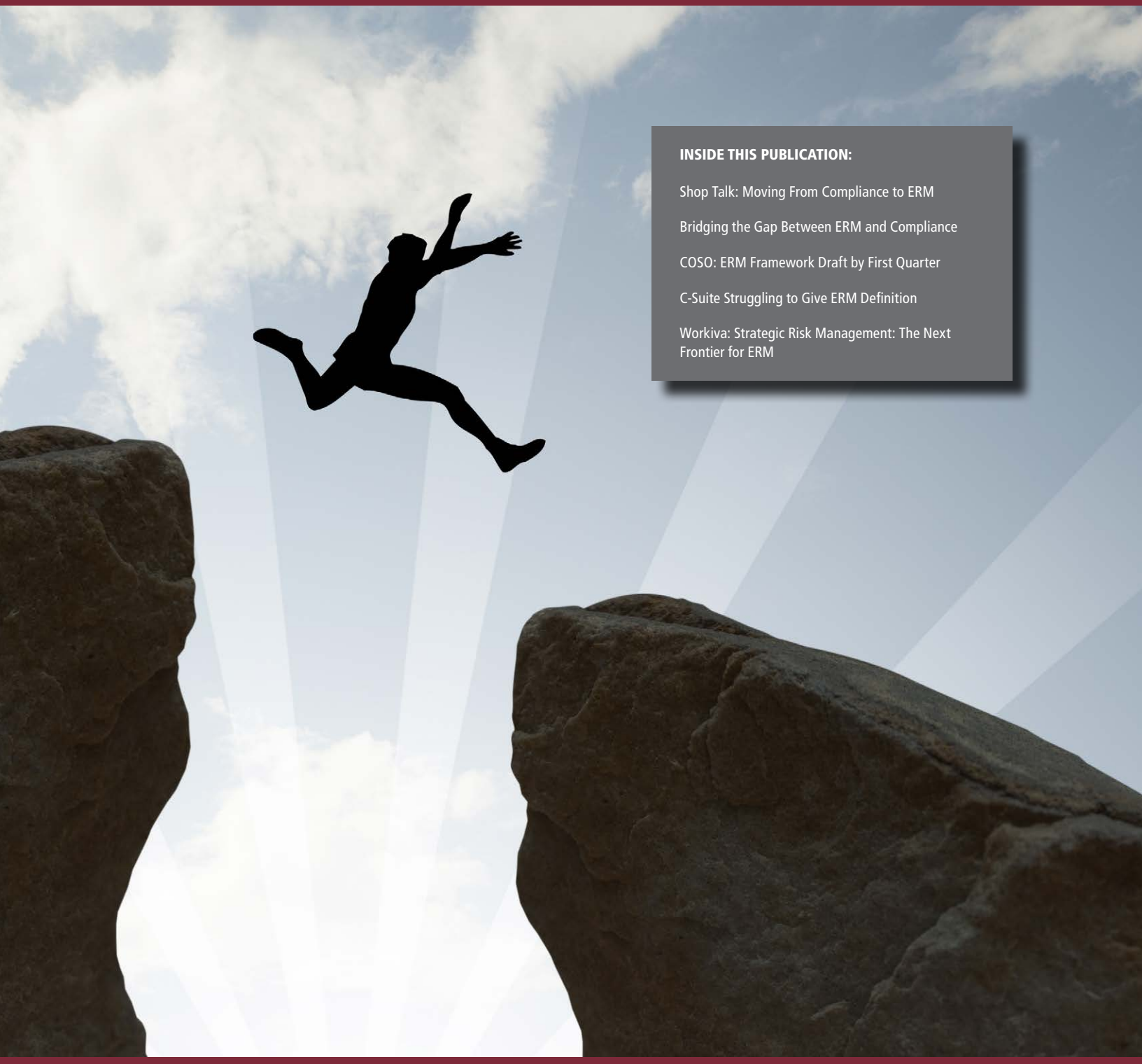
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Making the Leap

From Compliance to ERM

An e-Book publication sponsored by

workiva Wdesk

COMPLIANCE WEEK

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

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

Workiva (NYSE:WK) created Wdesk, a cloud-based productivity platform for enterprises to collect, link, report, and analyze business data with control and accountability. Thousands of organizations, including over 65 percent of the Fortune 500, use Wdesk for risk, compliance, or management reporting. Wdesk proprietary word processing, spreadsheet, and presentation applications are integrated and built upon a data management engine, offering synchronized data, controlled collaboration, granular permissions, and a full audit trail. Wdesk helps mitigate enterprise risk, improve productivity, and give users confidence to make decisions with real-time data. Workiva employs more than 1,000 people with offices in 15 cities. The company is headquartered in Ames, Iowa. For more information, visit workiva.com.

Inside this e-Book:

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 CW, Workiva roundtable

By Jaclyn Jaeger

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 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 commit-

tees 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. ■

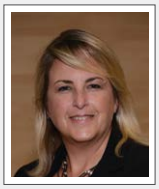
PARTICIPANTS

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

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

Bridging the Gap Between ERM and Compliance

By Matt Kelly

In September, I had the privilege of hosting another Compliance Week executive roundtable, this time to talk about moving from a compliance program to a broader enterprise risk management program: how you decide on an ERM structure, how you it that from clever idea to working program, and how you convince others at your company to go along with this latest request from those whacky folks in compliance and internal audit.

The conversation was excellent, as you have seen from the in-depth coverage of the discussion on page four of this e-Book. For now, let me recap a few of the main points here.

ERM is already here. We had 10 compliance and audit executives from a wide range of industries at our roundtable, and almost all of them said their businesses were trying enterprise risk management to some degree. Most added that they weren't too far along in their quest to implement ERM, and plenty of hurdles remain. (We'll get to those momentarily.) But the reality—for them and most other businesses, I suspect—is that enterprise risk management is already here.

Lots of that preliminary effort can trace back to Sarbanes-Oxley compliance and basic internal auditing principles. After all, a good internal audit department conducts its own enterprise-wide risk assessment every year. SOX compliance sparked a new era of attention to internal controls—yes, starting only with internal control over financial reporting, but by now that renewed interest has spread to matters such as anti-corruption, product quality, cybersecurity, and more.

Boards also pay much more attention to ERM these days. Several roundtable participants said their audit committees or other board directors specifically directed them to assess the state of enterprise risk management at their businesses. Others said their CFOs were big supporters of ERM because those CFOs served on boards elsewhere, where ERM is a hot topic.

And let's not forget that more broadly, the nature of corporate transactions today makes ERM a better idea. Forty years ago, the vast amount of assets a company owned were tangible: factories, inventory, real estate, and so forth. The risks inherent in those assets were fewer, and could be managed individually. Now the majority of your assets are intangible: customer data, patents, IT systems, and the like. To extract value from assets like that, you need to coordinate them more intricately and more skillfully—and if you don't, more can go wrong more quickly. You need orchestration, and that's what enterprise risk management is.

As always, data is the challenge. Numerous roundtable participants said the pace of merger activity at their companies is too fast; they cannot collect and rationalize data quickly enough to stay atop of all risks efficiently. (I hear that complaint about M&A a lot, actually, about everything from managing third parties to financial reporting.) As one person at the table put it, "I know what our risks are. I just can't get the data to tell me how those risks are going."

A data warehouse is a good idea, but a warehouse only works when people bother to make deliveries into it—and that's where compliance officers need some sharp inter-personal skills, to convince others to share their data.

One thing that struck me about difficulty with data, however, is how closely that ties into difficulty with human beings at your organization. We talked for a while about the need for data warehouses: one central repository where all information about your company and its risks can be stored, and then analyzed by the audit or compliance officer. A good idea unto itself, but a warehouse only works when people bother to make deliveries into it—and that's where compliance officers need some sharp inter-personal skills, to convince others to share their data.

A data warehouse is a good idea, but a warehouse only works when people bother to make deliveries into it—and that's where compliance officers need some sharp inter-personal skills, to convince others to share their data.

This might be one area where you could deputize your friends in internal audit and IT, to examine your business processes and determine the least painful way they might need to change for the sake of ERM. The ideal is that the owners of those business processes (in sales, marketing, IT, product development, and so forth) have a process where they "own the risk," but also own the control, and generate the data you need in some automated fashion that goes straight into your warehouse.

I'm not saying that's easy to engineer. It's just the goal you want to achieve.

Don't forget your board. We spent a fair bit of time talking about boards and their attention to ERM, and which committee on the board should take the lead on ERM issues. Naturally the audit committee was mentioned quite a bit, and it certainly is a plausible candidate—but even if the audit committee is the best choice you have, that doesn't mean it's the right choice.

My co-host for the roundtable, Mike Rost, vice president of strategy at Workiva, made this excellent point: that by their nature, audit committees tend to look backward at events that have already happened (investigations into misconduct, audits of last year's financials, and so forth). Savvy risk management, in contrast, is about looking forward, to outcomes and challenges that might happen. That means the best committee to tackle ERM really is a dedicated risk committee, a group that can look for "ignition sources," as Rost put it, whether they are igniting growth or igniting a crisis.

Good advice to close out a roundtable, and a column. ■

COSO: ERM Framework Draft by First Quarter

New framework expected to link risk management to risk governance and risk culture

By Tammy Whitehouse

More than a year after it launched an effort to revise its Enterprise Risk Management framework, COSO now expects to publish an exposure draft for public comment in the first quarter of 2016.

COSO's ERM integrated framework dates back to 2004 and suffers similar conditions that inspired COSO to update its Internal Control – Integrated Framework in 2013. Much has changed since COSO first released its ERM framework more than a decade ago, so the board decided to give it a refresh in light of modern business conventions and practices.


Hirth

"It will be a little different look and feel from the 2004 framework," says Bob Hirth, chairman of COSO. "Consistent with the updated internal control framework, you'll see the components, principles, and point of focus, but it will be much tighter than in the 2004 framework. It will be a more structured document, much like the updated internal control framework."

Hirth says the new ERM framework will be a "standalone" risk management framework, not something that is based on "a lot of cutting and pasting" from the internal control framework. "That's something people will look forward to," he says. "My hope is to see some modernization, updating, and refinement of things to make a good document even better and even more useful."

COSO updated its internal control framework in 2013, setting public companies on a journey to refresh their internal controls to the new framework so they would remain in compliance with Sarbanes-Oxley. The Securities and Exchange Commission doesn't explicitly require companies to follow COSO's internal control framework but the vast majority do to fulfill the SEC's requirement for public companies to follow "a suitable framework."

COSO put its old framework to pasture at the end of 2014, prompting SEC officials to wonder aloud how any company could regard a retired framework as "suitable." Most companies updated to the new framework in 2015, but some elected to take an extra year.

Public companies are not facing the same regulatory imperative when the new ERM framework is issued, as no regulatory body explicitly requires public companies to follow an particular framework to manage and report on the ERM activities. Still, Hirth says organizations will find it a useful tool to focus and direct their ERM initiatives. "This will help you meet move of your objectives more of the time," he says. "It's a little like exercise. Everyone who does it but with a program will do it better."

The update framework is expected to better link risk management to risk governance and risk culture, to strategy formulation and the setting of objectives, and to decision making, says Hirth. The objective is to facilitate the embedding of a risk management strategy into an organization rather than having it stand as a separate process, he says. ■

COSO ANNOUNCES UPDATE TO FRAMEWORK

Below, CW writer Tammy Whitehouse spoke with COSO's Robert Hirth in October 2014 when the ERM project was first announced.

The Committee of Sponsoring Organizations is launching a project to update its 10-year-old Enterprise Risk Management – Integrated Framework for the same reasons it refreshed the Internal Control – Integrated Framework. "We've come to the preliminary conclusion that there's probably been enough change from when the framework was issued in 2004 that we should start a questioning process just like we did with the internal control framework," says COSO Chairman Robert Hirth. "We will be asking a wide group of stakeholders how they use it and what value they get or don't get from it."

Hirth says the practice of risk management has changed considerable since it first entered the corporate scene, and some of the language of the framework could use some updating. "The two critical areas are around risk appetite and risk tolerance," he says. "We want to assure we have the latest thinking around those issues." Hirth estimates the process could take 18 to 24 months, depending on the extent of changes that are pursued and the nature of the feedback it receives.

When COSO proposed revisions to its internal controls framework, which was originally published in 1992, some internal control experts urged COSO to integrate the internal control and ERM frameworks into a single piece of guidance. COSO decided against it in part because many companies rely on the internal control framework to meet a specific regulatory mandate, but not so with the ERM framework, Hirth says, although companies are required to provide disclosures about their board oversight of risk. "The board risk oversight disclosures has been one impetus for this," he says.

It's too soon to say, in Hirth's view, whether an update to the ERM framework could re-open yet another examination of internal controls down the line. "In the risk assessment section of the new internal control framework, we think there's some good, updated thinking in there," he says.

—Tammy Whitehouse.

C-Suite Struggling to Give ERM Definition

By Tammy Whitehouse

Despite consensus that risk is a big deal—something companies should be managing aggressively—recent academic data suggests public companies in particular have a long way to go to deal with risk effectively.

A recent study out of North Carolina State University shows almost 60 percent of nearly 1,100 companies surveyed through the American Institute of Certified Public Accountants say they are facing a greater volume and complexity of risks than they were five years ago. A slightly higher percentage says they were caught off guard by some operational surprise in the same timeframe.

The total population includes private and not-for-profit companies, but only about one-third of larger companies, public companies, or financial services organizations within the sample said they would describe their enterprise risk management process as "mature" or "robust." Less than half of the larger companies or financial services firms reported that their boards extensively review top risk exposures when considering their strategic plans.

The findings suggest a disconnect between a view that today's business environment is generally pretty risky and the decision by organizations to tackle risk. "I see it as a little bit of overconfidence on the part of management," says Mark Beasley, an ERM professor at NC State. "We are seeing a little bit of a leveling off. There was some initial investment in ERM in 2009 and 2010, but the last few years it has been flat."

NC State also produced a survey result in connection with Protiviti that shows another disconnect. When asked what kinds of risks are most significant to their organizations, responses were all over the map. Board members and executive management focused their attention on economic conditions, political factors, global financial markets, and an ability to obtain sufficient capital and meet growth objectives under those conditions. Fair enough.

Operational leaders, however—those who run the finance, audit, risk, and other functional areas—focus more on operational risks: hiring the right talent, managing cyber-threats, and beating competitor performance. They also worry that risks won't be identified in a timely way and escalated to the right level in the organization so the risk can be addressed in connection with the company's strategy.

In tandem, the separate survey results suggest companies may have work to do to better address risk, and to assure everyone agrees upon what the most important risks to address are. "I wonder if there is a lack of understanding of the views of risk across the management team," Beasley says. "The presumption may be that we are more on the same page than we really are."

The findings on ERM maturity are disappointing to Scott Mitchell, chairman of the Open Compliance & Ethics Group. "One wonders what's wrong with ERM and why ERM hasn't matured as quickly as quality management or strategic management," he says. "Obviously OCEG's point of view is the possibility that ERM is too myopic in its focus. A lot of ERM programs struggle to integrate with performance, and that's why they struggle."

Divergent Views, or Splitting Hairs?

The suggestion that boards and senior management may have a different view of risk compared with functional leaders isn't as much of a concern to Mitchell. "You have different departments or different units that have different priorities," he says. "That's the point of running a business."

Jim DeLoach, managing director at Protiviti, says the findings imply that some companies might need to review the basics in terms of their risk assessment processes. Companies might go about it in different ways, which might affect the results. "You want to have different perspectives that are captured, integrated, and assimilated," he says. "In that way, you come up with the organizations' best collective view of its risk profile. That's not easy." Beasley points out that one key finding of the studies is concern that corporate culture might not adequately encourage key risks to be elevated to the right levels in a timely manner so they can be addressed. "I've heard some say in certain cultures, if I elevate a risk, I could be incriminating myself as an ineffective manager," he says. "So are you comfortable you have the right process to assure risks are being elevated among multiple players in the C-suite team?"


DeLoach

Also crucial, says Brian Schwartz, U.S. GRC leader for PwC, is assuring a well-defined risk appetite. "Risk appetite will tell the company how many and which types of risks should be taken on based on pursuing their business objectives," he says. "A lot of companies build elaborate risk assessment programs before they've defined appetite. It's like building a bridge without knowing how wide the river is." On the plus side, he says, he sees chief risk officers increasingly stepping back and asking what they can do to make the ERM process more relevant to the organization.

For Mike Kearney, national managing partner for strategic risk services at Deloitte, the recent data provide a wake-up call to companies to spend more time considering how key risks affect strategy. "There's just not enough time spent talking about it," he says. "There's not enough time really getting beneath what the risks are and what they mean to the longevity of the organization and the strategy chosen." Too often, he says, companies view the ERM program as a standalone function with an annual assessment process. "It's not necessarily based into the business management process as much as it could be."

Norman Marks, a retired internal auditor turned governance activist, says risk programs fail to operate effectively for any number of reasons: not being recognized by the board as contributing to success, not being embraced by functional managers throughout the organization, and not being aligned with the strategy of the organization. Companies can move further along the ERM maturity curve by assuring their risk is aligned with strategy and managed at acceptable levels, he says. "We've got to move away from periodic reviews of risk to risk being an integral part of how we run the business," he says. ■

WHITE PAPER

workiva

Strategic Risk Management: The next frontier for ERM

By James Lam

Introduction

Sweat the big stuff first. Senior management should—and usually does—focus on major decisions that have a significant impact on a company. Perhaps the most important task senior management ever tackles is setting appropriate priorities to deploy the limited resources available.

Take, for example, the capital spending approval process. Proposed investments generally exceed the allocated budget, so each must undergo rigorous evaluation to determine which projects offer the most attractive risk/reward trade-offs. But the amount matters too—a $20 million strategic investment in a new product launch may require board approval, while a department head may have authority to spend $200,000 on a software upgrade. Senior management handles the big-ticket items and delegates authority for smaller-scale capital investments to middle management.

Why do most enterprise risk management programs reverse this approach? 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).[1] Yet in practice, many ERM programs downplay strategic risks or ignore them altogether.

This misdirected effort assumes greater importance because so many strategic initiatives fall short of expectations. Although the oft-quoted 70 percent failure rate enshrined in management lore lacks empirical support,[2] complete success is still the exception rather than the rule. In 2008, John Kotter, a leading expert in change management, summed up his experience:

> "From years of study, I estimate today more than 70 percent of needed change either fails to be launched, even though some people clearly see the need, fails to be completed, even though some people exhaust themselves trying, or finishes over budget, late and with initial aspirations unmet."[3]

Whatever the true failure rate for strategic initiatives, companies have every incentive to improve

1. Lam, J."Risk Management: The ERM Guide from AFP." (2011). Association for Financial Professionals. Retrieved from http://www.jameslam.com/images/PDF/AFP%20Enterprise%20Risk%20Management%20Guide_Lam%202012.pdf

2. Hughes, M. (2011). "Do 70 Percent of All Organizational Change Initiatives Really Fail?" *Journal of Change Management.*

3. Kotter, J. (2008). *A Sense of Urgency.* Boston, MA: Harvard Business Review.

performance through higher outright or partial success of their strategic plans.

If the goal of ERM is to enable management to identify, prioritize, and manage risk, ERM programs ought to focus first on strategic risks, followed by operational risks. The financial risks that dominate ERM today should come a distant third.

ERM professionals have focused on financial risks because they are easy to quantify and universally applicable. Several high-profile trading disasters at financial firms have shifted attention over the past decade toward operational risks even though they are harder to measure.

The difficulty lies in the nature of operational mishaps—the vast majority of which are commonplace but financially insignificant. On the rare occasions when operational controls do break down, the consequences can be devastating, and not only for banks. The 2010 Deepwater Horizon catastrophe inflicted enormous financial and reputational damage on British Petroleum, Transocean, and Halliburton.

But the latest yardsticks developed to measure financial risk, economic capital and risk-adjusted return on capital (RAROC), can be applied to operational and strategic risks as well. These measures pave the way for strategic risk management to become a top priority for ERM practitioners—the next frontier in the struggle to control and manage risk.

What is the difference between operational and strategic risk? A company that has unmatched manufacturing processes will still fail if consumers no longer want its products. Whether they knew it or not, even the most efficient buggy whip makers faced an existential threat in 1908 when Henry Ford introduced the Model T. In more recent times, Apple transformed the competitive landscape for cellular handset makers the day it launched the first iPhone. Good strategy means doing the right things, while good operations means doing things right—successful companies must do both.

The ability to recognize and manage strategic risks is critical to the sustainable success of any company. The rest of this paper explains:

- How to integrate strategic risks into the planning process
- The use of economic capital and risk-adjusted return on capital to measure these risks
- How to apply the results in practice

Strategic planning

Companies often start their strategic planning with a SWOT (strengths, weaknesses, opportunities, and threats) analysis to determine where best to focus new initiatives.

Having established priorities for future investments, many companies use Kaplan and Norton's Balanced Scorecard to evaluate each initiative from different perspectives, including customers, internal business processes, organizational capacity (knowledge and innovation), and financial performance. Others prefer Michael Porter's Five Forces model, which analyzes how new initiatives are affected by supplier power, buyer power, competitive rivalry, threat of substitution, and threat of new entry.

Companies that ignore risk in the planning process forgo the opportunity to manage the shape of [the risk bell curve].

These popular strategic planning tools bring structure to the process, but risk professionals have long recognized they suffer from a major flaw—they do not take risk into account.[4] In the aftermath of the 2008 financial crisis, Kaplan himself acknowledged the shortcoming, "…the measurement, mitigation, and management of risk have not been strongly featured in David Norton's and my work."[5]

Rigorous use of standard planning tools generates an expected value for each strategic initiative, without regard to the distribution of outcomes around the expected value if things do not work out as planned. This kind of risk can also be expressed as a bell curve centered on the expected value. Companies that ignore risk in the planning process forgo the opportunity to manage the shape of that curve.

For example, two initiatives with identical expected values may have quite different risk profiles. One may have a narrow bell, which implies a high probability the expected outcome

4. "A good case can be made that the balanced scorecard (or any other business reporting methodology) should include a risk assessment, either as a separate category or as a part of each of the four performance components." Lam, J. (2003). *Enterprise Risk Management, First Edition.*Hoboken, NJ: John Wiley & Sons.

5. Kaplan, R. "Risk Management and the Strategy Execution System." (2009). Balanced Scorecard Report, Vol. 11, No. 6. Retrieved from http://www.exed.hbs.edu/assets/Documents/risk-management-strategy.pdf

will occur, low risk of failure, and little opportunity for an unexpected windfall. The other may have a wide bell, which suggests an outcome other than the expected value—for better or worse—is more likely. Planning tools give no guidance on how to choose between the two, and the right choice will not be the same in every case because companies have different appetites for risk.

What qualifies as a strategic risk? Again, it's the big stuff—any risks that affect or are inherent in a company's business strategy, strategic objectives, and strategy execution. The list includes:

- Consumer demand
- Legal and regulatory change
- Competitive pressure
- Merger integration
- Technology change
- Senior management turnover
- Stakeholder pressure

Other risks may qualify for particular companies depending on the nature of their businesses. In a 2013 Deloitte report, Siemens, the European conglomerate, captures the spirit in its broad definition of strategic risk: "everything, every obstacle, every issue that has the potential to materially affect the achievement of our strategic objectives."[6]

Measuring strategic risk

Identification is the first step, but before a company can manage risks, it must measure them. One of the best available metrics is economic capital—the amount of equity required to cover unexpected losses based on a predetermined solvency standard, typically derived from the company's target debt rating.

Applying a consistent measure of volatility, the economic capital required to support individual risks can be calculated and the results aggregated across all risks, taking correlation effects into account. Economic capital is a common currency in which any risk can be quantified. It also applies the same methodology and assumptions in determining enterprise value. For strategic risks, the calculation is forward-looking—for example, the cushion required to support new product launches, potential acquisitions, or withstand anticipated competitive pressure.

Dividing the anticipated after-tax return on each strategic initiative by the economic capital generates RAROC (risk adjusted return on capital). If RAROC exceeds the company's cost of capital, the initiative is viable and will add value. If RAROC is less than the cost of capital, it will destroy value.

However, the decision whether to back an initiative should not depend on a single case reflecting the expected value. The company should run the numbers for multiple scenarios to see the distribution of results in both more and less favorable circumstances, or in combinations of better and worse conditions over time. The final decision will depend on the specific company's risk appetite.

Risk management is a dynamic process in which information flows from line managers up to senior managers who monitor progress and, when necessary, develop action plans and send instructions back down to line managers.

Economic capital and RAROC analyses work for both organic growth initiatives and potential acquisitions. In mergers and acquisitions, a company can leverage economic capital and RAROC to evaluate how the enterprise risk profile of a potential acquisition would complement its own. As decision support for the board and management, this analysis can quantify the risk/return economics of the merger, including diversification benefits, debt rating impacts, enterprise value and earnings, as well as the maximum price that the company should be willing to pay.

A decision tree that maps the probabilities and consequences[7] of different outcomes not only provides a better feel for the risks and rewards, but also helps identify trigger points for action if the initiative lags behind expectations. The optimum risk management profile resembles a call option: limited

6. "Exploring Strategic Risk."(2013). Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-exploring-strategic-risk.pdf

7. 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.

downside exposure with unlimited upside potential. The sooner a company recognizes an initiative is in trouble, the sooner it can take corrective action—whether that be to steer the initiative back on track, deploy risk mitigation strategies, or shut it down.

Managing strategic risk

Risk measurements have limited value unless the company has a robust procedure for monitoring, feedback, and action. Suppose a company does the preliminary analysis described above and approves a new initiative. Six months later, if results come in ahead of expectations, the company could decide to accelerate the plan to take advantage of the early success—but only if senior management knows what has happened.

Risk management is a dynamic process in which information flows from line managers up to senior managers who monitor progress and, when necessary, develop action plans and send instructions back down to line managers.

The nature of new initiatives approved and the triggers for acceleration or corrective action all depend on a company's risk appetite. ERM implementation requires a company to create a risk appetite statement that defines how much risk it will take in pursuit of its business strategy. For strategic risks, the risk appetite metrics are typically defined through the potential impact on earnings, enterprise value from adverse business decisions, or lack of response to industry changes.

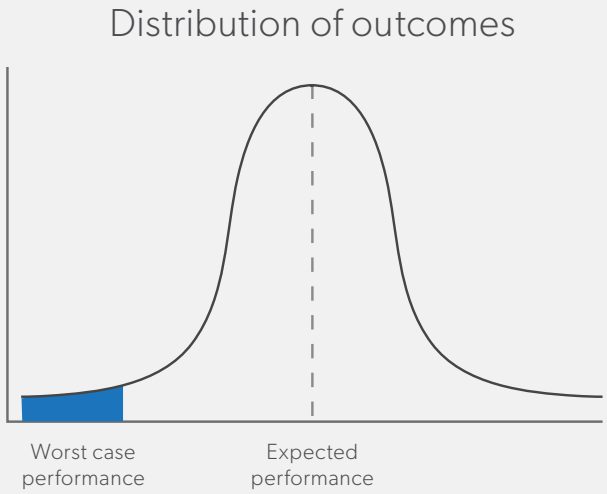
To support strategic risk management decisions, the company's performance management system must integrate key performance indicators (KPIs) and key risk indicators (KRIs). This process is illustrated in exhibit A. As with any other risk, strategic risk can be depicted as a bell curve, with the expected level of performance in the center of the distribution. ERM should focus on mitigating downside risk, i.e., worst-case performance, but also help management optimize overall risk-return trade-offs.

In this integrated process, the company:

1. Defines its business strategy and a defined set of strategic objectives
2. Establishes KPIs and targets based on expected performance for those strategic objectives
3. Identifies strategic risks that can drive variability in actual performance for better or worse through risk assessments
4. Establishes KRIs and risk tolerance levels for those critical risks
5. Provides integrated reporting and monitoring in support of strategic risk management

Unfortunately, many companies perform steps 1 and 2 through the strategic planning and/or finance functions and report the results to the executive committee and full board. Separately, they perform steps 3 and 4 through the risk function and report the results to the risk and audit committees. In order to effectively manage strategic risks, these steps must be fully integrated.

Exhibit A: Integrating performance and risk monitoring



Integrating strategy and ERM

1. Define business strategy and objectives
2. Establish KPIs based on expected performance
3. Identify risks that can drive variability in performance (risk assessments)
4. Establish KRIs for critical risks
5. Provide integrated monitoring with respect to 1–4

Source: James Lam & Associates

Practical examples

Duke Energy – In the late 1990s, the market for electric power went through wrenching change when states began to deregulate utilities. At a strategy session in July 2000, Duke Energy identified three possible scenarios for its future business environment:[8]

- Economic Treadmill, in which U.S. economic growth would stagnate at 1 percent per year
- Market.com, in which the internet would revolutionize the relationships between buyers and sellers
- Flawed Competition, in which uneven deregulation would continue in the energy industry, causing significant price volatility in different regions

The timing proved prescient. Duke had appointed its first chief risk officer earlier that year, and the U.S. economy had begun the slide that burst the internet bubble.

Duke set early warning signals for each scenario:

- Macroeconomic indicators
- Regulatory trends
- Technology changes
- Environment issues
- Competitive moves
- Patterns of consolidation in the energy industry

It soon became apparent that Flawed Competition was the most likely outcome, which enabled Duke to take evasive action against potential adverse consequences. Unlike many competitors, Duke scaled back its capacity expansion and concentrated on maximizing returns from its existing portfolio—even if that meant shedding assets. Anticipating oversupply of power generation in Texas in the coming years, Duke sold some new plant projects in the state before construction was complete.

Duke reaped the rewards of its foresight in subsequent years and has continued to perform well relative to its competitors. As shown on their company website, in the five years through November 2014, Duke stock rose by 69%.[9]

Citigroup – In the early 1990s, Citigroup suffered severe losses from three separate crises: developing nation debt default/restructuring, U.S. residential mortgages, and commercial real estate. Senior management recognized the need for a global process for scenario planning and risk management to flag potential problems earlier, which resulted in its Windows on Risk program.

Upon launch in 1994, Citigroup called it a system that "regularly monitors the state of the economy in different countries and the extent to which the bank's exposure to lending, underwriting, or trading might be affected according to 12 key factors." In 1999, Windows on Risk had expanded into "a forum for reviewing risk tolerance and practices," and by 2002 it was embedded in Citigroup's Balanced Scorecard planning.[10]

In essence, Windows on Risk involves the development of a global business outlook, risk analyses, and tripwires in 16 windows, e.g., country risk, industry concentration, technology risk, etc., as well as preemptive plans for risk management strategies to mitigate each risk if it occurs. The process soon proved its worth: In 1997 Citigroup weathered the Asian currency crisis better than most of its competitors.[11]

GE Capital – During the 1990s, GE Capital created Policy 6.0, a strategic risk management framework applied to all new businesses, products, and investments. It requires a detailed analysis of strategic risks associated with any new initiative and quarterly reviews between business leaders and GE corporate executives to check that the business is performing at or above expectations. The major components of Policy 6.0 include:[12]

- Key assumptions: The new business must identify the key assumptions that support its feasibility, which often represent the most critical strategic risks, including business trends, customer needs, and disruptive technologies.

---

8. Wysocki, B. (2000, July 7). Power Grid: Soft Landing or Hard? *Wall Street Journal*. Retrieved from https://business.illinois.edu/~s-darcy/Fin590/2005/WSJ_July%207%202000.pdf
9. "Stock Information." (2015). Duke Energy Corporation. Retrieved from http://www.duke-energy.com/investors/stock-information.asp.
10. Gilad, B. (2003). *Early Warning: Using Competitive Intelligence to Anticipate Market Shifts, Control Risk, and Create Powerful Strategies*. Ney York, NY: AMACOM.
11. "Weathering financial crises: bond markets in Asia and the Pacific." (2012). BIS Papers: No. 63. Retrieved from http://www.bis.org/publ/bppdf/bispap63.htm
12. "GE Capital Finance Overview." (2008). GE. Retrieved from http://www.ge.com/pdf/investors/events/12022008/ge_webcast_presentation_12022008.pdf

- Monitoring systems: For each assumption, the business must identify monitoring systems for key performance indicators, key risk indicators, and early warning indicators. They must also specify the individuals responsible for oversight.
- Trigger points: For critical metrics, the business must establish predefined positive, expected, and negative trigger points, which initiate management action between quarterly reviews. Breaches of significant thresholds may trigger immediate escalation and special reviews.
- Management decisions and actions: Positive signals mean things are going better than expected, which may prompt management to accelerate the business plan or take more risk. Negative signals give management the opportunity to initiate risk mitigation strategies, or, if key metrics and trends are well below expectations, an exit strategy.

A strategic risk management framework helps management allocate scarce human and financial resources to the most successful initiatives and take corrective action to forestall losses from unsuccessful projects.

Although these companies are engaged in quite different businesses, their strategic risk management has three common themes:

1. Strategic planning and analysis
2. Metrics and trigger points
3. Decisions and actions

A strategic risk management framework helps management allocate scarce human and financial resources to the most successful initiatives and take corrective action to forestall losses from unsuccessful projects.

Conclusion

Although strategic risks pose the greatest threat to most companies, few have yet incorporated strategic risk management into their ERM program. Strategic initiatives always involve risk, and some will not pan out as expected no matter how carefully planned.

Companies that manage strategic risk skew the outcome in their favor. They can ramp up initiatives that exceed expectations and spot potential losses in time to take corrective action before significant losses accumulate. Risk management should improve the percentage of successful initiatives, but even if it does not, the process creates a financial profile similar to a call option, with limited downside risk and unlimited upside potential.

One key benefit of strategic risk management is early warning of potential problems. If an initiative falls behind expectations, alarms sound. Management then has the opportunity to redirect the effort, lay off risk, or if the project is unable to be salvaged, implement an exit strategy early on. The ability to fail faster will improve a company's financial performance.

Lack of reliable metrics is no longer an obstacle to strategic risk management. Economic capital is a common currency in which any risk can be quantified, and the RAROC expected in various scenarios allows management to determine which initiatives mesh best with the company's risk appetite.

Even Robert Kaplan recognizes how important risk management has become to companies and their executives: "…despite the difficulty of risk management, senior executives who avoid, de-emphasize, or delegate it do so at their peril."[13]

Robust ERM programs already boast a lower cost of capital, higher growth, and greater appreciation in the stock market. Companies that integrate strategic risk into their ERM frameworks will likely further enhance all three attributes to the benefit of shareholders, other stakeholders, and society at large.

13. Kaplin, R. "Risk Management and the Strategy Execution System." (2009). Balanced Scorecard Report, Vol. 11, No. 6. Retrieved from http://www.exed.hbs.edu/assets/Documents/risk-management-strategy.pdf

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.

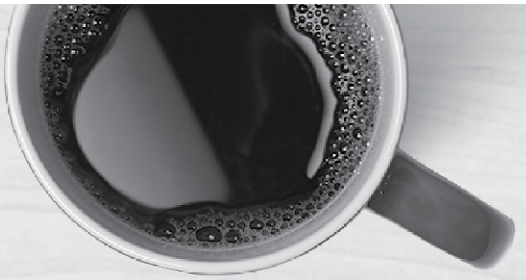
After receiving his BBA from Baruch College and graduating summa cum laude, Lam completed his MBA with honors at UCLA. In addition to lecturing at Harvard Business School, he has taught courses in risk management at Babson College and Hult International Business School.

About Workiva

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. See what we can do for you at workiva.com.

workiva.com
info@workiva.com
+1.888.275.3125

wdesk



Redefining the way enterprises work.

Risk | Audit | Finance | Compliance

Turn risk into opportunity with a comprehensive enterprise risk management solution.

workiva.com | info@workiva.com | +1.888.275.3125

Workiva