Corporate Treasurers Council®

CTC GUIDE TO

Enterprise Risk Management
Beyond Theory: Practitioner Perspectives on ERM

Underwritten by:

pwc

Corporate Treasurers Council®

CTC GUIDE TO

Enterprise Risk Management
Beyond Theory: Practitioner Perspectives on ERM

By Nilly Essaides

Contents

Enterprise Risk Management
Beyond Theory: Practitioner Perspectives on ERM

Introduction

This is not the typical Enterprise Risk Management (ERM) guide. Often, when financial executives read guides about ERM, those reports are in the form of a best-practices list under headings such as Oversight, Governance and Structure, and include checklists for factors such as Risk Identification and Assessment. This guide focuses instead on the experiences of five companies and their ERM programs (see Case Studies on page 14). Based on extensive interviews with corporate risk practitioners and experts and including quantitative data, this practitioner's guide presents detailed examples of the ways in which companies have approached ERM and how their efforts provide valuable insight into leading ERM practices.

"A lot of organizations shy away from ERM because they can't see how it provides [anything] other than just a list of the exposures they're already aware of," said a risk practitioner who built the ERM program for a major airline. At the time, he said, "we had a consultant who was talking about an ERM program and they [sic] had some interesting slides." But at the end of the presentation, the CFO asked what the program would look like. "They had lovely bullet points, but how do you make it real? That's the challenge."

The companies highlighted in this guide offer views into how that challenge can be met. Their risk champions carry different titles. Some programs are more complex than others. But all of them exhibit several or all of these differentiating factors:

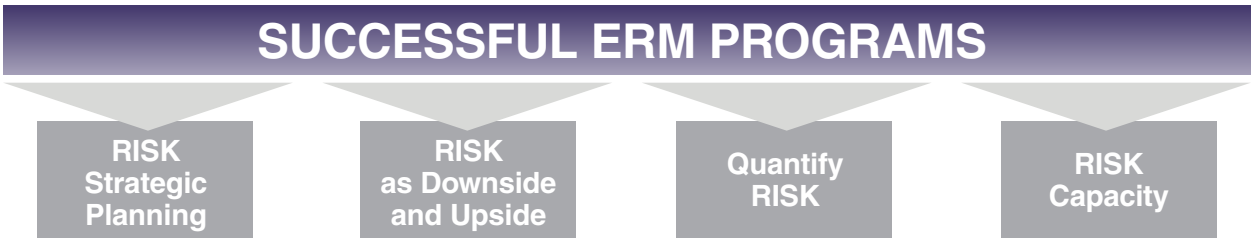
- They connect risk and strategic planning
- They think about risk as downside and an upside
- They put numbers around risk
- They consider risk capacity

According to Peter Frank, Partner at PricewaterhouseCoopers (PwC), whether or not there's a formal ERM program is a separate question than whether or not a company is successfully managing its risks. Some companies have very sophisticated risk cultures and do not necessarily overlay those cultures with an explicit ERM process. "The companies that do [ERM] well have to combine a cultural appreciation for risk with rigor of process," noted Frank. Certainly companies in industries such as chemicals, oil and banking have a history of developing sophisticated risk awareness programs. Yet, some of the most spectacular risk failings in recent history have occurred within such organizations. "A forensic review typically indicates a failure in risk management," said Frank. For ERM to work, he said, "There needs to be a culture and a process, and general sophistication of risk. Without all three there's not going to be success."

What success looks like

Each of the companies in this guide is in a very different phase of what they all call a journey, from the earliest stages of ERM to the most mature programs, based on the rigor of the program and how embedded ERM already is into their strategic planning process.

- At a **very large industrial equipment dealer** (see Case Study 1: The ERM Pivot on page 14), a recent enterprise resource planning (ERP) implementation gone "bad" spurred a rethinking of risk management in the company. That led to the hiring of a VP-level risk executive, a former consultant. According to this ERM practitioner, there are various ways ERM can add value. "From our perspective," he said, "the emphasis is going to be on being more proactive



about risk. That's where we're driving the program." Of course before you can get to that level, "you have to have all the foundational things," this risk professional said, e.g., a common language, rating scales, etc. "That's what we're on right now. Down the road, I'd like to broaden out [the program] to include policies around risk. That's where I want to take it." According to this ERM expert, having a sense of what the "end state" would look like is critical to taking the right steps going forward.

- At **HCA Healthcare** (see Case Study 3: HCA Holdings, Inc. on page 19) the ERM program began small and grew over time. "In our company, ERM is a tool for executive management," said David Hughes, HCA's Assistant Vice President, Enterprise Risk Management and Business Continuity Planning. "If it's too detailed and drills down too deeply, you can lose that connection and it doesn't really translate into executive management decision-making," he said. "You can always get more detailed later. It's easier to start at a high level and get some early successes. That's how we started." With ERM, "people start thinking about risk differently," Hughes said. Initially, risk was viewed as a way to say "no." Now, noted Hughes, "it has evolved into people considering risk as we start new initiatives," he said. "This has made it okay to think about what our risks are within the strategy, and how to mitigate and manage those risks so we can make sure the strategy is successful," he said.
- **IAMGOLD** (see Case Study 2: IAMGOLD Corp. on page 16), a mid-size Canadian gold-mining company had a strong ERM program long before it made revisions to its policies and procedures in 2012. According to a team of senior executives at IAMGOLD, "ERM is not a one-time program, it's a process." There's always been a form of ERM displayed in the way the business is managed; however, "having the process more formalized helps with the communication with the directors and the investment community."

  The risks the company identifies through its process are integrated into the highest level of management decisions as well as day-to-day operations at the site level. "We look at risks to the business and the strategic plan. We identify mitigating activities for any risk that might prevent us from achieving those plans," the executive team explained. "We go through this level of rigor at the project level. It gives us insight into risk management not just at the corporate level. ERM goes into every aspect of the business including managing our balance sheet and capital structure."
- At $43 billion automotive company **Johnson Controls** (JCI) (see Case Study 4: Johnson Controls on page 22), ERM is baked into the strategic planning process. Since 2007, the company's ERM initiative has been owned by the VP of Strategy, John Sibson. That the vice-president of strategy "owns" ERM is unusual, but it makes perfect sense given today's realities. Sibson pointed to a study by the Corporate Executive Board (CEB) showing that in 80 percent of cases, the reasons behind a significant market capitalization decrease are not compliance or legal. "The real drivers are basic strategic issues," Sibson explained, including "poor post-M&A integration, competition, price wars and bad products, which supported the concept of strategic planning ownership."

  To ensure risks are properly identified, ranked, mitigated and managed within the big picture, the company pursues a very structured process using a simple, web-enabled tool that allows participants to rank risks based on a four-dimensional model. The ERM and Strategic Planning processes move in unison, and decisions about reducing and taking on additional risk are managed within an explicit risk-tolerance framework.
- At **Zurich USA** (see Case Study 5: Zurich in North America on page 27), Chief Risk Officer Barry Franklin sits at the intersection of risk and business. The U.S. arm of the Swiss insurance giant has a long ERM tradition that shows what best practice ultimately may look like. "When I look at the foundation for a company such as ours, you have to have a mature program that rests on the company's entire financial management and capital management discipline," Franklin explained. At Zurich, "ERM is first and foremost about effectively managing capital. Second, it's about encouraging and supporting risk based-decision making. And third, it's about supporting and encouraging a risk-aware culture."

Time to Shift Gears

There's no question that many in business have developed a sense of disenchantment with ERM – so much so that some risk experts have rebranded it Strategic Risk Management or SRM. "In separating the two terms, the thinking is that SRM says that 'at the end of the day you use risk to drive successful strategy'," said Chris Mandel, a risk management expert for more than 20 years and SVP of Strategic Solutions at Sedgwick, a provider of technology-enabled insurance claims and productivity management solutions. "That's really what ERM was supposed to be all about. A lot of people who have tried this and not done well, feel that they need to rebrand what they're doing," Mandel explained.

"We've hit a tipping point," said Sally Bernstein, Principal at PwC Risk Advisory. "People have been talking about risk management and completing risk assessments for a number of years. Now they are looking at those assessments and asking: "Where's the value?" Companies have ended up with risk *lists* and not risk *programs.* Bernstein and her colleague, Ken Hooper, Director-Risk Advisory, see a shift. "People are asking us that question: We've got this list and it's not helping us make thoughtful decisions, so what's the point?" noted Hooper.

Many companies follow the same "M.O.," according to Frank at PwC. "They interview a whole bunch of people and have a series of workshops where they ask participants throughout the organization 'what keeps them up at night.' That's my least favorite question," he said. "The output is literally a list of risks." However, often the starting point is wrong because the questions are not asked within the right context, "which is how risks can affect the objectives and strategies of the organization."

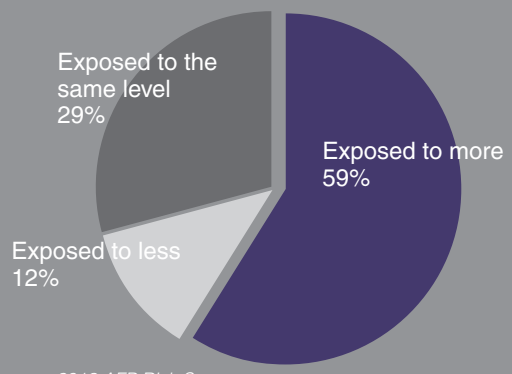
"ERM is happening whether you have a formal program or not. The issue is how well you're doing it," said Gary Bierc, CEO of rPM3 Solutions LLC, a provider of a risk measurement software tool and a former risk management practitioner (see also sidebar on page on this page). Where a lot of companies went wrong was during the early- to mid-2000s with a laser-focus on compliance. "I believe that SOX (Sarbanes-Oxley) regulations and Enron and WorldCom were the best and worst thing(s) for ERM," said Bierc. On the upside, SOX focused management attention on risk. On the downside, it placed the focus on the wrong risks and methods:

Why ERM Matters Now

As a recent survey by Deloitte & Touche (see page 4) demonstrated, the majority of companies are rethinking their ERM approach. That is due in part to the 2008 financial and ensuing economic crisis; some of it is the natural evolution of the concept. But there are other factors that are enhancing board and financial manager focus on ERM:

Greater Uncertainty. "There's a sense that the world appears more uncertain and risky than it did seven to ten years ago," according to McKinsey & Co. Senior Risk Expert Martin Pergler. "One can debate whether it's truly so or whether we just didn't see it before, which is interesting but somewhat academic," he said. "What's important is that when you ask senior management about their confidence level, there's a whole lot more risk awareness and concern. People care about risk management." *The 2013 AFP Risk Survey*, sponsored by Oliver Wyman, shows that nearly 60 percent of financial executives report their companies are facing greater earnings volatility today than they did five years ago.

Change in Exposure to Uncertainty in Earnings Relative to Five Years Ago



Source: 2013 AFP Risk Survey

Board pressure. "There's increasing pressure from boards and sometimes regulators," according to Pergler. "They seek more systematic risk management and they want to be more confident that risk is being well managed." (See also sidebar on page 5.)

New Technologies. According to PwC's Ken Hooper, new risk technologies are also helping companies improve their processes. While the common advice is to fix the process before implementing a new system, often the reality is that a system implementation is the driver of process change. "There's also an increasing focus on analytics, which is where risk management needs to go next," Hooper said, "so companies can get more sophisticated in understanding their risks."

Figure 1: Changes in Mindset towards Risk Management
(Percentage Distribution)

	North America	Europe	Revenues Under $1 Billion	Revenues At Least $1 Billion	Publicly Traded	Privately Owned
Continue to see risk as a threat to the organization and actively manage it, but not in an integrated manner	38%	40%	39%	34%	35%	38%
Now see risk as part of business and we actively manage both the opportunities and threats, but not in an integrated manner	28	38	23	38	33	24
Recently decided to approach risk in integrated manner across functions, business lines and risk classes	26	8	24	19	26	19
Continue to see risk as a threat to the organization, but we still do not manage it actively	6	11	14	6	2	19
Other	2	3	1	3	4	0

Source: 2013 gtnews Treasury Risk Survey

compliance and financial reporting. But things are changing. "We have experienced a period of time over the last decade where the less effective ways of doing ERM have worked their way out, where management is now looking for the measured value of ERM."

"The [ERM programs] that I've seen that had real success are ones that center their focus on the strategy connection," said Mark Beasley, Deloitte Professor of Enterprise Risk Management and Director, ERM Initiative at the North Carolina State University Poole School of Management. "Many companies end up with long lists, an inventory of 1000 risks, and then what?" Beasley said. The problem with these lists is that they often skip over the important part: providing a strategic lens into risk. "Those [companies] that have been successful are trying to say: in the context of our products, services and strategic plan, what are the big risk factors that would make it difficult to be successful?"

These observations are supported by the results of the *2013 gtnews Treasury Risk Survey,* conducted by the Association for Financial Professionals (AFP) in collaboration with Zanders Treasury and Finance Solutions. The survey shows that companies are in the midst of a mindset transformation, and are increasingly aware of the value-added potential of a risk management function that examines risk as a two-sided coin. More than half the survey respondents indicate their companies are considering making or have recently made a shift to viewing risk on an integrated basis and 87 percent see business improvement as a key objective of risk management (see Figures 1 and 2). According to the survey analysis, "this realization supports the transformation of the risk management function to a more strategic one that exists to enable and support business goal realization."

What's more, a majority of organizations say ERM is the most promising development for risk management.

A 2012 study of 200 companies by Deloitte & Touche LLC confirms these findings. It found that 79 percent of respondents "were significantly reworking their risk management process, activities, strategy

Figure 2: Greatest Opportunity to Improve Risk Management
(Percentage Distribution)

	All	North America	Europe	Revenues Under $1 Billion	Revenues At Least $1 Billion	Publicly Traded	Privately Owned
Enterprise wide risk management approach	34%	33%	30%	36%	33%	37%	30%
Integrated (holistic) financial risk management approach	25	22	22	33	17	21	32
Redesign of internal processes	20	22	27	18	22	21	19
More advanced risk measurement techniques	13	12	16	6	17	13	10
Use of new hedging instruments	4	6	3	3	5	3	6
Dedicated GRC systems	2	2	0	3	2	4	0
Other (please specify)	2	4	3	1	4	3	3

Source: 2013 gtnews Treasury Risk Survey

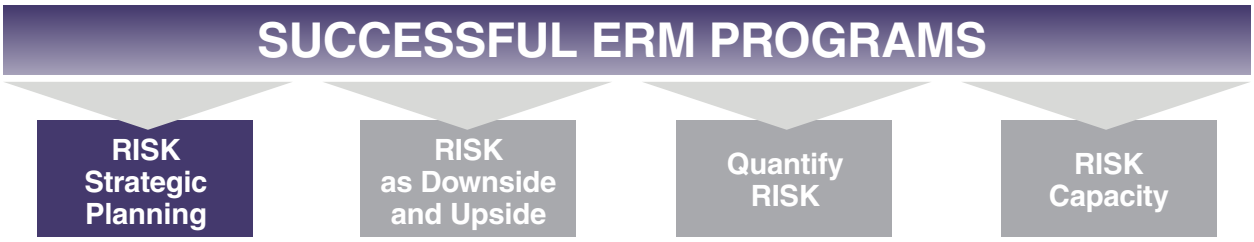
and tools, indicating the residual concern about risk management in the wake of the credit and economic crisis," said Henry Ristuccia, Partner and Global Leader, Governance, Risk and Compliance Services for Deloitte. In the past, practitioners thought financial institutions were the primary "leaders" of effective ERM. But 2008 changed all that (see sidebar on page 3). While some financial institutions have excellent programs (see Case Study 5: Zurich in North America on page 27), they're by no means the only ones in the forefront. "To say financial institutions are in the lead is a fallacy," Ristuccia said. "Actually when you think about broader cultural and strategic programs, I see a lot of examples among commercial enterprises."

"When it comes to ERM overall, I think there's been a very strong movement by risk-intensive businesses to adopt ERM practices," said James Lam, President, James Lam & Associates, Director and Risk Oversight Committee Chair, E*TRADE and author of *Enterprise Risk Management: From Incentives to Controls* (John Wiley & Sons, 2003). "When you look back 15 to 20 years, many skeptics considered ERM as 'flavor of the month'," Lam said. However, things changed radically post the 2008 financial crisis. "The overwhelming majority of risk intensive companies are in some stage of implementing ERM," he said.

Boards Zero-in on Risk

Everyone agrees the current focus on ERM is driven primarily by visionary boards. Indeed, said John Sibson at Johnson Controls: "My program is easy to run because I set the tone at the top, starting with the board telling the CEO and the chairman that this [ERM] is a priority. Ergo, it's a priority for the CEO," said Sibson. To back up the rhetoric, the CEO attends every meeting of the risk committee. "I have perfect attendance from the CEO,' said Sibson. "The tone from the top is a very big deal."

"In 2009-2010, stakeholders were saying: Boards, where were you?" said Mark Beasley at North Carolina State University. "Were you aware and did you approve it? There was more pressure on boards in the wake of the crisis." According to Beasley, boards have had increasing motivation to adopt ERM practices, with more audit committees directly responsible for risk oversight and other stakeholders, like S&P, beginning to shine a spotlight on the quality of company's risk management efforts. (see also sidebar on page 8).



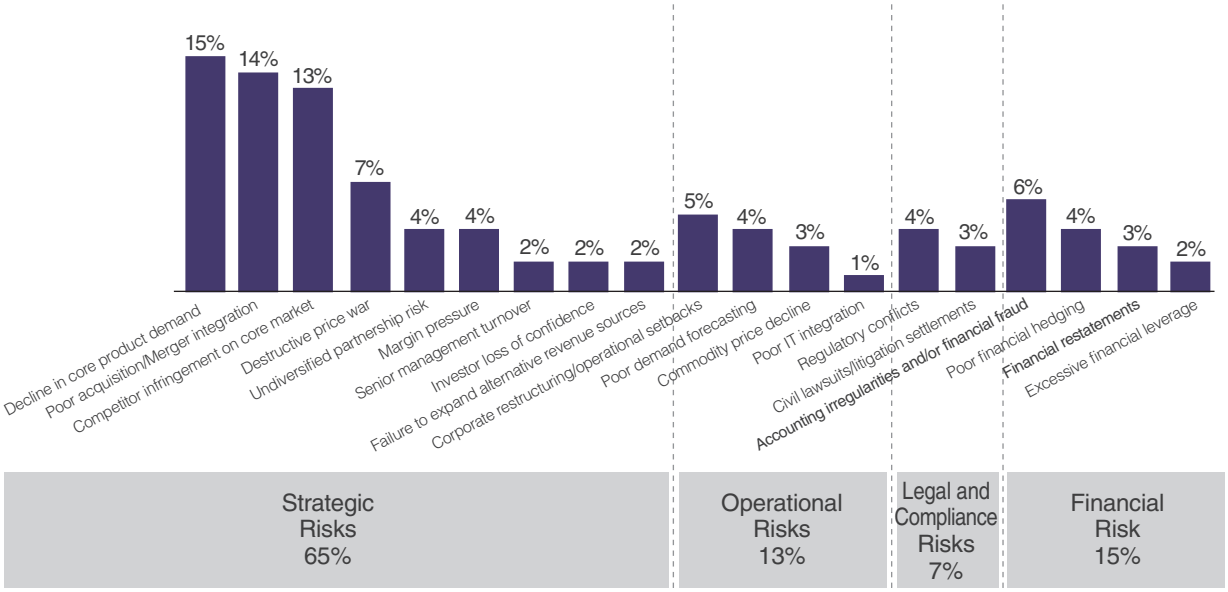
Connect Risk and Strategic Planning

The biggest difference about ERM today is that more companies are making an explicit link between their ERM programs and how they make strategic decisions and measure performance. The objective is to "connect all the dots, test assurances, ensure capitalization is in alignment with risk exposure and strategy and risk owners have the right tolerances and can be kept accountable," said Gary Bierc. Bierc sees ERM as a new form of business intelligence: the critical link between strategic planning and performance management.

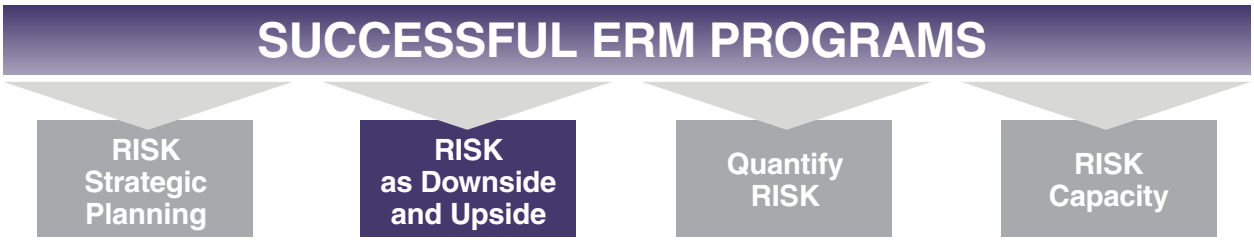
There's good reason to focus on strategic risk. According to James Lam, research studies show that for most organizations strategic risks account for about 60 percent of the risk universe, followed by operational risk (30 percent) and financial risk (about 10 percent). That means ERM needs to be a key element in strategic decisions. "At the board level, that may mean incorporating ERM into capital structure and strategic decisions," said Lam. "At the executive level it is about how ERM is integrated into business planning, for example, resource allocation and investment decisions. At the business unit level, ERM should impact pricing, because that's where you actually get rewarded for the risks that you take. The key challenge is to be able to integrate ERM into business decisions at all levels of the organization."

According to Deloitte's Ristuccia, "Progressive companies engage the board and senior leadership to build scenario planning into decision-making. They communicate that through their people and culture," he said. "Our mission is X. Our risk tolerance is Z. Our risk factors are 1-5 or 1-10 and are grounded in business strategy," Ristuccia explained. "That gives the organization a better chance to have ERM in the DNA of the organization and better transparency to connect the dots and advise senior managers," he said.

Figure 3: Market Capitalization Decline Drivers Top 20% of Fortune 1,000 (1998-2002)



Source: Corporate Executive Board



Think About Risk Downside and Upside

Connecting risk and strategy is where ERM is headed. "That's the future of the discipline," said Sedgwick's Mandel. "The [companies] that I see gaining the most traction are the ones that are making that connection. That link is critical not only to avoiding risk but as important to successfully taking risk in order to grow the business," he said.

> For companies in risky businesses, ERM is not just a necessity, it's a competitive advantage.

At Johnson Controls (JCI), a risk tolerance map allows management to identify areas where actual risk is below its target level, as well as the other way around. In the future, JCI expects to be able to measure leadership performance based on how it closes these gaps. For companies in risky businesses like IAMGOLD, ERM is not just a necessity, it's a competitive advantage. According to its ERM team, "If you do not have that supportive culture and an excellent program you are at a competitive disadvantage."

According to Zurich USA CRO Barry Franklin, "One of the reasons we have the processes we do and rely on financial metrics and risk-based decision-making is to help identify opportunities. If we have a choice of growing in a line of business vs. another, they [sic] may have similar loss ratios and may look like they would produce similar results. But when you look at return on risk capital, one may be a better opportunity," he explained. "We're using the tools we have to make better decisions to build a risk portfolio that is value added."

This kind of thinking is relatively new, according to Mandel. "Five years ago, no one talked about it. However, that's where the value is: learning to use risk information to drive the top line, whereas traditional risk is more focused on protecting the bottom line," Mandel said.

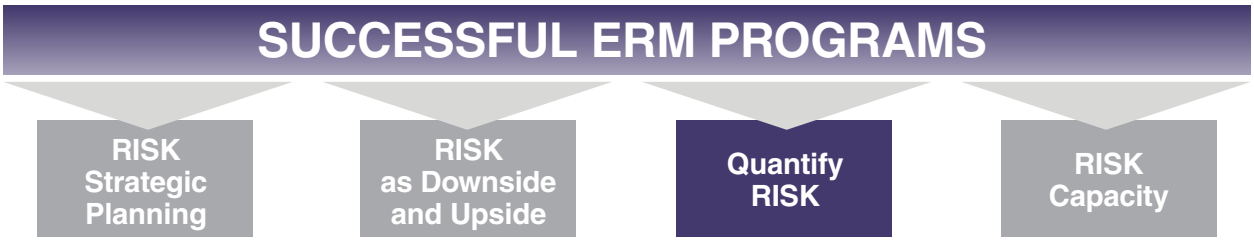
"This thinking is already present at different levels in some industries, for example natural resources," said Martin Pergler, Senior Risk Expert at McKinsey & Co. "There are living examples of companies that have started using good-quality ERM as a strategic advantage to increase value. When one industry does it, it creates a snowball effect as others look at the payoff," he said. But before companies can get there, they must take care of the basics. "When you're just getting the risk basics right, it's dangerous to take on greater risk to generate value. And if the risk culture is not under control, it may bring you down," said Pergler.

S&P's ERM Focus

When Standard & Poor's (S&P) began to extend its ERM thinking from banks and insurers to non-financial companies, "we found that management, investors and even analysts were not making the connection from relatively new ERM practices to the credit rating," said Managing Director Steve Dreyer. "It's very difficult to draw a bright line between good ERM practices and the ability of a company to repay its financial obligation over the next few years," he explained. "It turns out that many of the benefits of good ERM practices have much longer-term benefits, because they have to do with changing culture, practices and behaviors," he said. "If you take insurers, when they change the way they look at risk, the result of how it impacted their decision making are not known for many years," he said. "It's the same for non-financial corporations."

S&P's thinking about ERM has evolved over the last few years, "to talk in a different language," said Dreyer. Two years ago, the agency began to tie its risk management assessment more directly to credit risk, culminating in a Management and Governance score which is composed of four areas: Governance, Strategy Risk, Management, Organizational Effectiveness. Risk management is only one of those components, "which is where most of the work we've done on ERM ended up," Dreyer explained.

Dreyer is careful to note that a credit rating is only an opinion of the ability to meet financial obligations over the next few years (and for low-rated companies that's an even shorter horizon). For managements, that should be only part of the equation. "Management has its own objectives. I would like to think that long term profit maximization is one of them, which may lead to different decisions than what would result from looking ahead only three to four years from now." For example, a company may decide it can live with a lower rating in the near term in order to be able to expand and grow long term. "The practical constraint is that our time horizon is not 10 or more years out."



Put Numbers Around Risk

Being able to measure and demonstrate the value of ERM "is the next step in the evolution," according to Steve Dreyer, a managing director at Standard & Poor's (S&P) and the agency's ERM expert. "The first phase was to find out what could kill the company and stay away from that." While that's better than ignoring risk altogether, that's only the start. "The second is the recognition that it's bad to under-risk the company," Dreyer said. "It may not be as bad as over-risking it, but the idea should be a tradeoff along a continuum of risk and return," he said.

By quantifying risk, companies have a more reliable way to measure how each function or project contributes to the management of each risk that affects performance, according to Mandel of Sedgwick. "It's about measurement and showing value proposition and return on investment dollars," he said. That sort of thinking is best illustrated within the context of a risk-free environment. That sounds purely theoretical but it doesn't have to be. The methodology Mandel developed in collaboration with Gary Bierc is not rocket science. "It's a variation on forensic accounting that some people have likened to periodic business review. You look at the P&L and analyze what units are not performing and tie risk to that," he said (see sidebar on page 10).

By quantifying risk, companies have a more reliable way to measure how each function or project contributes to the management of each risk that affects performance.

Risk measurement doesn't have to mean complex financial modeling. "Compared to a decade ago, risk managers are more humble and they've learned to appreciate the softer elements of risk management," McKinsey's Pergler said. The original approach, "that risk management can be turned into a math and engineering problem, has created a backlash," he said, not least because of the financial crisis. That doesn't mean those concepts are not useful. "We've come back to a realization that in terms of 'business as usual' risk, you have to do some engineering and math, and create the risk culture to manage well," he said. "Where math is not helpful is in predicting tail events; there shouldn't be a wholesale move away from analytics. The important thing is to develop a better sense of the boundaries of where data and analytics can be helpful."

According to PwC's Peter Frank, "Best practice today involves analyzing your financials at risk; it's the analysis of the strategic plan developed by FP&A and sensitivity to key assumptions." These assumptions are linked to the company's biggest risk. "Financial risk analysis is about understanding how assumptions and objectives work together," he said. A lot of companies still look internally to come up with those scenarios, but they shouldn't stop there. "Look at big macro economic factors."

Companies like IAMGOLD, JCI and HCA are ranking their key risks, based on increasingly sophisticated formulas, that sometimes take into account more than just probability and severity, but also velocity and the mitigating impact of risk controls (see case studies). In the case of JCI, the ranking is handled by a simple web app that allows participants to assign a specific numbers. Those scores are fed through a formula that is displayed in a simple way that captures risks visually and intuitively (see Case Study 4: Johnson Controls on page 22).

Measuring Enterprise Total Cost of Risk™

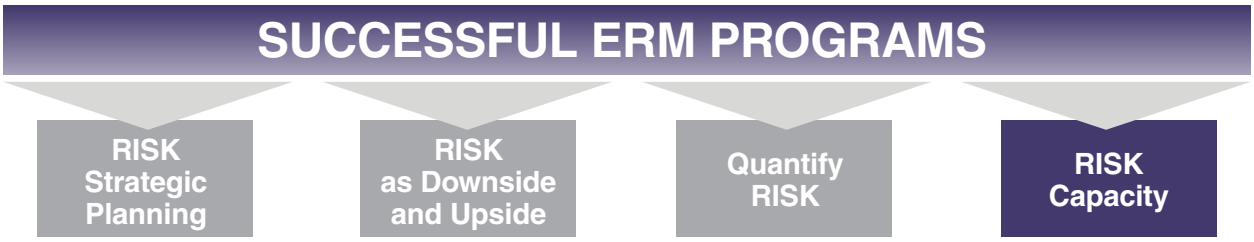
Back in the 1990s, Gary Bierc – now CEO of rPM3 Solutions LLC – built what was then called an Holistic or Integrated Risk Management program as an assistant treasurer and risk director at Moore, then a Toronto-based midsize business forms company that has since been acquired. The program had some quick successes. In 15 months, it took Moore's lowest performing business unit and turned a loss into an operating profit. "The ERM strategy is why we were doing better," Bierc said. But while that made intuitive sense to Moore's board, the board wanted a way to quantify it. That's what sparked Bierc's initial interest in putting numbers around ERM's value.

By 2010, Bierc won a patent for a new methodology to create what he calls the "fifth financial statement." It is essentially an expansion of the four traditional statements which focuses on risk; it strips out the cost of risk from the cost of doing business and makes it possible to incorporate real metrics at the outset – when making decisions – and at the end, to measure business and program performance based on the Enterprise Total Cost of Risk™ or ETCOR™.

"There's core business spending and there's risk spending," said Bierc. The core cost of business is the cost of business in a risk-free environment. The cost of risk is any cost added because risk exists. "We can measure the cost or risk signature on a business every single period. More importantly we can tie risk assessment work and proactive risk management activity, and meld that into the forecast," he said. At the other end, performance can be tracked based on risk investment.

Bierc's company's software tool, called ARQ Technology™ (or Aggregate Risk Quantification™), allows companies to "plug in" their trial balance or GL information and get a view into the variance between "risk-free" and "risk-loaded" performance and view it in real time. They can also use ARQ Technology™ to make proactive decisions, and look at historical trends to assess past performance.

While he concedes this approach requires a true shift in how many companies think about decision-making and performance, Bierc has seen increased interest from some big potential clients. "We're not asking you to replace but add to what you're doing," he said. Otherwise, "You're not getting a complete picture of performance."



Think in Terms of Risk Capacity

Tying risk to capital is one place where concrete measurements can come into play. It's an area that's near and dear to treasurers who are often the "keepers" of the capital structure. Several of the companies highlighted in this guide – Zurich the most obvious example – link risk-return tradeoffs to impact on capital capacity (see sidebar on page 8). That's especially true for leveraged companies or companies that are borderline or even below investment grade where credit access is a key driver of business success, e.g., IAMGOLD and JCI, or a company like Zurich that must maintain a high credit rating in order to write business.

"Capital management relates primarily to a target debt-rating equivalent, which is a common approach," said Zurich's Franklin. For Zurich, that means maintaining a target capital level that's consistent with an AA rating, which in turn implies a 99.95 percent likelihood of remaining financially solvent over a one- year horizon, a type of VaR measure. Based on capital model output and analysis, Zurich establishes target monetary tolerance levels which also take into account correlations among different risk types, geographies and lines of business. Franklin acknowledges that financial organizations have the advantage of being able to more easily to quantify risk in terms of quantitative models. "Financial managers in non-financial organizations still need to have a way to allocate capital and to ensure everybody is looking at return on capital. But it's more challenging. It's not quite as apparent," he said.

Professor Beasley points to S&P's May 13, 2013 decision to publicly disclose top and bottom Governance and Management scores, which include an ERM score. "When they (S&P) started in 2007, the effort got the attention of treasurers. Now they're seeing a financial incentive to do this," he explained, by protecting their credit rating and their cost of capital. There's data to show ERM pays off. Analysis of insurance companies shows that those that ranked high in their ERM scores survived the crisis much better than those who did not, according to Beasley.

Treasury can often play an active role in driving ERM initiatives, in particular in instilling a measurement culture, because that's what finance executives do every day.

In companies like JCI and IAMGOLD, treasury can often play an active role in driving ERM initiatives, in particular in instilling a measurement culture, because that's what finance executives do every day, according to Gary Bierc, who started his ERM career in treasury. That's very obvious in decisions treasurers make about insurance, risk tolerance, premiums and risk retention, as well as setting up captives and other forms of risk finance. However, by bringing ERM into the equation, "you can have a financing strategy that goes beyond the traditional insurance," Beirc said. "Because you're tracking events and consequences of events, you can begin to align your capital resources." Indeed, he said, "financial sourcing for the organization is where it all starts to connect: treasury work, ERM and risk metrics. Everything is about optimizing shareholder value."

Conclusion: Success Tips

There's clear evidence that (1) more companies are re-thinking their ERM approach and (2) that some companies are moving in the right direction. Why aren't more companies following this path? According to PwC's Peter Frank, that's primarily a mindset issue. And there are three things that really stand in the way:

1. Executive management often discounts large external risks because they feel that they cannot control them; plus they think that their industry peers are facing similar risks.
2. There's a spoken or unspoken belief that as CEO, business unit leader or CFO, "managing risks is what I get paid to do, and I already do it daily. So I don't need a formal process," Frank said.
3. Finally, while they may not admit it, many companies manage their performance for quarterly or yearly results. "It's a rare company that truly makes decisions for the long term when it comes to managing risk," Frank said. "That short-term view is a barrier to seeing some of the benefits of effective risk management."

What companies can do

The first thing to realize is that there's no single way of doing this. "What I've seen is that there are few people who are doing it the same way," said HCA's David Hughes. Companies that are successful "have figured what works best in their environment and their company and have had great success and their programs are growing. Some things work for others and not us," he said. Ultimately, "it's got a lot to do with management vision and the company's culture. "

However, here's what seems to work for the five companies highlighted in this guide as well as according to experts.

Buy-in from the top

"That's the key thing I would suggest for any ERM program," according to the IAMGOLD team. "Without it [ERM] is going to be an ineffective process. That's what companies can leverage," he said. "If executive management is not on board, the first thing would be for them to understand how this can add value to the business," he added, "from an investment, compliance and operational perspective." (See sidebar on page 5.)

Have a well-articulated process that makes logical sense to everyone. What was most striking about each case study conversation was how fluid the ERM practitioners were in their processes. They were able to easily, off the top of their heads, outline a sensible and well-articulated approach that was connected at the top and designed to reach out into the organization, linking the process to how the company makes decisions and talks about risk. That fluency reflects the fact that each of these companies has developed a very sensible, organized approach. They didn't have to memorize rhetoric or go through checklists.

> "Don't do [ERM] once and put it away," advised the IAMGOLD team. "It needs to be a living, breathing process as your business develops."

Keep it fresh

"Don't do it once and put it away," advised the IAMGOLD team. "It needs to be a living, breathing process as your business develops," they said. This message was echoed by an assistant treasurer at a high end retailer that's been evolving its programs over the years. And every year his company takes a look back at what it did last time, how its actions influenced risk levels and what else it needed to do.

Get the right champion

Interestingly, in each case, the "owner" of the company's ERM process had a different title. There's a very good lesson in that. The choice of owner reflects the organization's view on where the ERM process fits and sometimes a legacy of where ERM started. It's equally a reflection of leadership decisions about the more specific qualities of the particular executive. According to PwC's Bernstein and Hooper, the person leading the effort needs to have the personality and management acumen to mandate things getting done. North Carolina States' Professor Beasley suggested that effective ERM leaders have two key qualities: "That individual needs to really understand the business and how it ticks. And, he or she needs to be a good leader and diplomat."

Select the right spot on the complexity continuum.

Effective ERM programs are not necessarily very complicated. In fact, one of the failings of some more detailed, bottoms-up programs "is that they tend to get lost in the weeds," said PwC's Frank. "The bottoms-up approach tends to identify risks that are internal or operational in nature, and that the company already puts a lot of effort into managing," he said. However, "those bottoms-up approaches can sometimes fail to identify the big strategic things that could kill the company. Companies should focus on both."

Set up the right ERM structure

It's very important to establish the ERM function in the right way. For non-financial companies, ERM is typically not a full-time occupation. So even though Barry Franklin is CRO at Zurich, among non-financial companies the CRO title is rare: AFP data show only six percent of companies have CROs at the head of their ERM structure. That doesn't mean risk is no one's responsibility. For each case study in this guide, the company's ERM program includes a set of very clear ERM assignments to the business and senior staff functions. If it's everyone's responsibility then it's really no one's," Franklin said.

Condense the information

From a very operational standpoint, ERM practitioners recommend that the program's output needs to fit with the company's overall culture of information. At JCI, the ERM group produces an extensive report. But at HCA, the outcome is a one-pager. "Think about your audience, and what the result is going to be so there's not too much detail," HCA's Hughes said.

Learn from others

What was true for every one of the companies examined for this report is that their ERM champions had a keen interest in both sharing what they do and finding out what other companies are doing. They see this benchmarking – informal and formal – as the best way to learn how to do things better. "Look at what others are doing to get ideas," HCA's Hughes said. That's why HCA participates in Professor Beasley's ERM program and attends and presents at roundtables. Added Zurich's Franklin, "It's your decision and you own it. There are consultants who have wonderful knowledge and tools, but at end of the day they're trying to sell you services. You need to think long and hard about what you want to get out of ERM before engaging a consultant for ERM implementation services. And it may be a good idea to engage an experienced business consultant to assist with just that portion of the exercise before proceeding. Better to learn from somebody else's successes and mistakes."

A good ERM program takes time to evolve. Almost all of the companies in this guide have been at this for years, and several have embarked on an ERM "makeover" at some point, learning from earlier mistakes.

Be realistic about timing

Finally, a good program takes time to evolve. Almost all of the companies in this guide have been at this for years, and several have embarked on an ERM "makeover" at some point, learning from earlier mistakes. Sometimes the impetus was new management. Sometimes it's an event that refocuses the board's attention on risk or a change in market conditions. In each case, the program has been improved. "There's a life cycle to implementing these programs," Franklin said. So that top-level support "helps you get started." But it needs to be sustained so that management "supports the process to make it through the time period it takes to embed the process and tools in the organization, because that can take a number of years."

Case Studies

Case Study 1: The ERM Pivot

This fast-growing, $6.6 billion industrial equipment multinational has embarked on a journey to revamp its ERM program this year, starting with hiring an ERM professional. The first step was to identify the value driving the program. Next the new ERM Vice President is putting together a roadmap including an assessment of the organization's current risk culture to determine key focus areas for the program, and to improve the risk culture throughout the organization.

At many companies, the impetus for a new or improved ERM program is rooted in either an internal or external event that focuses the board and management on risk management. At this organization, the impetus for change was a challenging ERP implementation. That event and the current trend of implementing better risk-management practices in an organization brought greater attention to the existing ERM program, which resulted in the hiring of a senior ERM professional.

"I've never seen anybody implement ERM in the same way," said the ERM chief of an industrial equipment multinational. "But most successful organizations have an owner who drives it, has a vision and can relay that to the organization."

Having worked as a consultant, the new ERM chief noted that having a risk champion is critical to the success of the program. "There are so many different ways to implement ERM," he said. "I've never seen anybody implement it in the same way. But most successful organizations have an owner who drives it, has a vision and can relay that to the organization," he said. While the company has had an ERM process owner for several years, the position experienced a lot of turnover. The result was inconsistent practice and process. "If you get that type of turnover, the program often loses its way," he said.

Moving toward the "end state"

The company already had an ERM program in place from which to build from. Currently, it develops a risk register, driven by each region. There's also a quarterly conference call involving those at the top level of the organization to discuss potential and emerging risks. Risks are scored based on likelihood and impact, and the ERM team is charged with consolidating the incoming risk registers from the regions and reporting to management and the board on a quarterly basis. The new ERM chief is working on various initiatives to improve the current processes.

Figure out the "end state." One of the issues companies often struggle with is an understanding of the value of ERM and what that "end state" looks like, according to this ERM professional. In the first 90 days in his role, he looked at the potential value-drivers of ERM in his organization. "Once you get through initial risk assessment, it's often not clear where you going to take it and what you're going to get out of the program," he said. He outlined nine areas of potential value:

- Developing better reporting to board and executives on top global risks
- Identifying key risk indicators around core risks, or those risks that the company faces regardless of the environment
- Being more proactive on risk
- Delivering better outcomes for the organization
- Improving scenario planning
- Helping better decision-making at every level
- Articulating better understanding for risk appetite
- Improving the risk culture

- Creating the ability to take risk sensibly and feeling more confident that the organization is "in control"

"These are all things you could achieve out of the program," he said. "From our perspective, the emphasis is going to be on being more proactive about risk. That's where we're driving the program." Of course before you can get to that level, "you have to have all the foundational things," this risk professional said, e.g., a common language, common rating scales, etc. "That's what we're focused on right now. Down the road, I'd like to broaden out [the program] to include leading risk indicators around our core risks. That's where we want to take it."

Creating a roadmap

The next step on his list this year is developing and sending out a survey to explore the company's existing risk culture and to better identify how it should target its ERM resources and efforts. "That's a good way to go, by getting a sense various elements of our risk management; for example, how people communicate and feel about raising risks in the organization," said this practitioner. The results of the survey will be important input into the roadmap for the program, designed to help people make better risk-based decisions. "To tailor the ERM program, you need to understand the existing culture."

Creating global standards

While the ERM program dates back five to six years, "practices have gotten disjointed and the company has not always been following good practice," says this ERM expert. While there's a process in place, there's lack of standardization and common risk language. "Right now the process is driven at the regional level," reported the head of ERM at this fast growing multinational. "In order to work well, it has to follow a standard approach. That's the current focus."

Expanding ERM's reach

Part of this ERM professional's evolving roadmap includes taking steps to expand the reach of the risk identification and communication effort. Currently, "there's a lot of reliance on the executive level to make sure they're connecting with their teams about what risks the organization is facing. The new process will have an ability to reach deeper," he said. There's value in looking at risk at a high level, but there's also value in getting deeper into the organization. "The question is where you see that value of the deeper effort and that often depends on the type business and environment you're in including, what you're trying to do with the information," he said. In his view, "if what you're trying to do is to improve decision-making and risk culture, you need to go deeper with ERM."

Linking risk to decision-making

A risk cultural survey will help the company make decisions about where to spend resources and how to touch the broader organization. But this risk professional is cognizant that simply collecting risk information is not enough. "There's a lot of data. Depending on how you tabulate it, you can make it a useful component to help guide the organization to be successful so you can pick a strategy and have a robust discussion around key risks," he said. "That's what I see as the risk department's role: Taking all the data, deciding how far down you need to go. Then being able to consolidate, analyze and present it in a way that feeds executive management and the board so they can use it as actionable data in their strategy.

"A lot of companies create the data and don't have the resources to manage it," he said. "That's where a lot of organizations fail." The problem, according to this ex-consultant, is that "you can generate the data relatively quickly and without too much effort. But getting it in to the right format and doing the right analysis is much more difficult," he said. "There are a lot of organizations that underestimate the resources necessary to make sense of the information."

The ultimate end state is to have ERM embedded into the culture and driving decisions across the organization. But it may take time to get there. "We're on a journey," said this ERM expert.

Case Study 2: IAMGOLD Corporation

This mid-size Canadian gold-mining company has a deeply rooted risk culture, which it recently formalized into a four-step process. It treats Enterprise Risk Management as a living/breathing process as the company continues to refine its approach, and views successful risk management as a competitive advantage.

The mining business is inherently risky. It involves large capital investment, significant operating commitments, and costly exploration programs in countries that may suffer political and social instability. It's no surprise then that IAMGOLD professes to have had a strong ERM program long before it made revisions to its policies and procedures in 2012, according to the ERM team comprised of senior executives: EVP and CFO Carol Banducci; Aun Ali Khokhawala, Director of Internal Audit and Risk Management; SVP of Corporate Affairs Benjamin Little and Treasurer Alberto Nunez. The ERM team discussed the company's program during an interview in May 2013.

"In the mining sector, there's already a heightened awareness [of] how risk can impact operations and local communities," said one executive on IAMGOLD's ERM team. "Every time we look at our business plan and strategy, we go through a risk assessment."

"In the mining sector, there's already a heightened awareness [of] how risk can impact operations and local communities," said one executive. "It's embedded into our culture. Every time we look at our business plan and strategy, we go through a risk assessment," the executive explained. "Mining is risky and it is important for the business to understand the nature of those risks and how to deal with them."

According to these senior leaders, "ERM is not a one-time program, it's a process. There's always been a form of ERM displayed in the way the business is managed. A year ago we put more clarity around the framework about how to assess, quantify measure and report risks." However, according to the risk-management team, while the risk culture has been prevalent, there has certainly been more recent emphasis from the financial community and the board to instill more rigor around it. "Having the process more formalized helps with the communication with the directors and the investment community," according to one senior executive.

For companies in the mining industry such as IAMGOLD, risk management is not only a necessity; it can be a powerful competitive advantage. "If you do not have that supportive culture and an excellent program you are at a competitive disadvantage," one participant said.

The four-phase process

The team said the ERM program is something the company takes seriously and is fundamental to how the business is managed. The program has four phases:

1. **Risk identification and assessment.** Define the risk universe with input from across the organization. Risks are assessed within a two-dimensional model of impact and likelihood broken into four broad categories: strategic, operational, financial and compliance, with an accompanying structure of accountability both at the corporate level and at the various sites.
2. **Risk mitigation and reporting.** Define rules, responsibilities, control activities and processes to mitigate and monitor those risks.

Board and management level buy-in is critical to the running of the ERM program. "You're setting the tone at the top," said one IAMGOLD executive.

3. **Risk policy.** Document the risk policy and processes, including reporting and communications, and how ERM is integrated into the business planning process.
4. **Risk infrastructure.** Document the company's appetite for risk and implement technology tools to track the risks that impact the business and strategic plan. The company is currently at this stage.

The ERM framework was initially designed by Internal Audit/Risk Management (IARM). "IARM supports management in reporting to the board and Audit Committee [about] how we are doing versus our risk framework," the executives said. "We sit down with the Executive Leadership Team and review risks in terms of both a short- and long-term horizon and in relation to our business and strategic plans." That overview is then captured within key areas including compliance, financial, strategic and operational risks.

"We get input from all functional and site leadership," reported one executive. "We do functional, site management and executive level reviews, and based on the collective input we come up with the most significant risks to us."

The IAMGOLD team noted that ERM is an important, comprehensive and proactive undertaking that is used to assess and manage the company's key risks. "It's an evolving program. Wherever there is a potential risk, we identify it, address it and update our risk universe," they said, adding that while the key risks will get the most attention, all risks are continuously on the radar screen.

IARM is the ERM process owner in terms of developing, monitoring and reporting protocols and their respective action items. Execution is handled by the functional and business unit executives. Specific risks are assigned to specific individuals. IARM pulls that together and reports to the board through the oversight of the Audit Committee on a quarterly basis and more frequently if necessary.

Such board and management level buy-in is critical to the running of the program. "The engagement from those levels is absolutely necessary. You're setting the tone at the top," said one executive. "The time, effort and rigor at the top cascade through the rest of the organization. If there is not buy-in from top management, it becomes a corporate or compliance exercise. This is not the case here. The CEO is visibly engaged and spends a considerable amount of time on ERM, supported by the board and the chair of the Audit Committee." In fact, risk management is defined as one of everyone's key objectives, which is critical to creating a culture of accountability.

ERM in practice

The risks the company identifies through its process are integrated into the highest level of management decisions as well as day-to-day operations at the site level. "We look at risks to the business and the strategic plan. We identify mitigating activities for any risk that might prevent us from achieving those plans," the executives explained. "We go through this level of rigor at the project level. It gives us insight into risk management not just at the corporate level. ERM goes into every aspect of the business including managing our balance sheet and capital structure," they said.

"Risk management plays a significant role in the work we do with communities and governments where we operate," the ERM team said. The relationships the company builds with various local constituents help stabilize its presence and avoid potential dangers. The company refers to its work with the governments and communities as its social license to operate in that country or region. "It drives a detailed framework that involves all political elements and stakeholders," the executives said.

To highlight how critical this area is to the business, IAMGOLD designed a very specific risk management framework to help address risks related to the government dimension of the business. "It is a very robust program that affects the operational and strategic plans and ties to compliance," the executives said. "We have

to operate within the legal mining framework within these countries."

The corporate affairs effort is best viewed as a subset of ERM. What sets it apart is "the degree of systemization and disciplined implementation," one participant explained. There's a process by which risks in each jurisdiction are identified, and an active program is put in place to mitigate each one. The program is run out of the corporate affairs office in Canada, but managed jointly with the country leads. It's effective because of "the significant amount of time that our most senior people spend engaged with governments in host jurisdictions," he said. "The program captures various facets of government risk, from elections, when you want to avoid becoming politicized, to a high degree of engagement with local media, opposition and incumbents, to communicating the total contribution that we make to the economy."

Added one executive: "I have seen it work negatively at companies that do not have that level of engagement. We identify periods when risk is elevated, for example budget times." In each jurisdiction, the company identifies risks and sources of leverage, which are very specific to the location. "You want to be able to look at influences on outcomes, and make sure you understand how it works."

Commodity price exposure was identified as a key risk in the industry. The company runs through scenario analyses based on different price assumptions and establishes appropriate alternate action plans for each scenario. "In our industry the price of gold is not something we are able to control," they said. "We must have well-developed plans to adjust our business and operational plans and, if needed, we must be prepared to implement those plans. Price impacts can be material, so you have to think this through ahead of time."

Evolving program

This year, IARM is working to create a more robust, detailed risk policy and document the company's risk appetite and tolerance level. That does not mean there is not one now. The work the team did defining the process already gave rise to a substantial amount of documentation. "There is a common definition and clarity around how things are defined," explained one executive. "It is important to ensure that we define risks in a consistent way so there is a constructive conversation. There is a lot of work that has already been done in standardizing the nomenclature." The team added: "We have a lot of information and insight about the process, risk impact and the policy. As we discuss it, we continue to refine it."

Advice for others

The IAMGOLD executives offered this collective advice to their peers, in terms of key ERM success factors:

1. **Buy-in from the top.** "This is the key item for success that [we] would suggest for any ERM program. Without it, it is going to be a much less effective process. It is important to understand how this can add value to the business, from an investment, compliance and operational perspective."
2. **A robust process.** Next in line is having a rigorous process. According to these ERM pros, the company's four-phase approach lends structure to the process.
3. **Keep it fresh.** "Don't do it once and put it away," they advised. "It needs to be a living, breathing process as your business develops."
4. **Get the right people in the room.** Finally, according to these ERM veterans, it is important to get the right people to assess the right set of risk areas.

Case Study 3: HCA Holdings, Inc.

This hospital giant's ERM program had a surreptitious beginning in 2000. It has evolved over the years to provide management and the board with a view on the top-10 risks in the organization, while keeping ERM presentations at a high level and providing "digestible" information for each audience.

HCA Holdings, Inc. is a $33 billion hospital and healthcare provider, with 162 hospitals and 113 freestanding surgery centers in 20 states and England. The company was founded in 1968 and has since grown considerably into one of the nation's leading healthcare providers with over 200,000 employees.

According to David Hughes, HCA's Assistant Vice President, Enterprise Risk Management and Business Continuity Planning, there's no single way to do ERM. "What I've seen is that there are few people who are doing it the same way," Hughes said. Companies that are successful "have figured what works best in their environment and their company and have had great success and their programs are growing. Some things work for others and not us," he said. Ultimately, "it's got a lot to do with management vision and the company's culture."

Taking incremental steps

Hughes believes HCA's program has been successful because it started small and grew over time. While some new ERM technologies and tools are coming on line, Hughes is not sure such systems would necessarily add value. "Most are too detailed. Many have tried to take SOX tools and make them into ERM tools, and drill down really deep into risks related to certain processes," he offered. "That's not what ERM is about. Too many people try to do that out of the gate," he added. "They try to look at risk at too granular a level. You can always drill down later. Start at the top level and work on communication.

"In our company, ERM is a tool for executive management," Hughes explained. "If it's too detailed and drills down too deeply, you can lose that connection and it doesn't really translate into executive management decision-making," he said. "You can always get more detailed later. It's easier to start at a high level and get some early successes. That's how we started."

There was not much discussion about ERM when HCA began its ERM program in 2000. Prior to moving to HCA, Hughes worked in Internal Audit (IA) at a different organization. At the time he joined HCA, the company's management was interested in implementing a more risk-based audit culture. "We started down that path from an audit perspective," he said. "We decided to interview the management team to see what the risks were for the company's strategy and how IA could possibly facilitate that strategy."

After conducting all of the interviews, "We had all this information and we decided to create a presentation based on some of the risk information to share with the company's CEO. The CEO embraced it and thought it was fantastic," Hughes said. "He liked hearing about the different risks and what people said about each risk. (All of the interviews were kept confidential to allow participants to speak freely about the risks.) I think he was surprised by a few of the comments, but liked the information."

Those discussions elicited an impromptu reaction on the CEO's part; they convinced him that the company needed do more to manage risk. Subsequently, the CEO shared this new intelligence with the company's division presidents. He asked each of them to write down what he or she saw as the company's top three risks. Hughes' team summarized all the notes and then fed it back to all the participants. "We got the information out to the businesses and they thought it was powerful," Hughes said. "It wasn't planned but that's how it started."

Over the 13 years since that original visionary CEO, HCA has had two new CEOs. "Each questioned the importance of ERM [but] after learning more about the program [they] discovered they wanted to keep it and expand it. The CEOs have seen value in it and that is the way we've grown," Hughes explained. Indeed, "Each year we've grown a little more."

Collecting risk information

Hughes is quick to note HCA's process is far from perfect. "I'd like to see us collect more detailed objective data than we currently do," he said. "But it works for us." Over the years, the effort expanded from gathering the views of only the most senior management team and the board to those of divisional leadership and other members of management, as well eventually including a sample of survey interviews with hospital and other business unit management.

Participation expanded and so has the risk identification process. "Now we slice and dice it," Hughes said. The process involves conducting interviews with all the participants (and the interview "sample" of hospitals and other business units changes) once a year. Hughes conducts the interviews in conjunction with the Chief Audit Executive. "We tag-team the interviews because the information also helps [the audit executive] risk-base the audit effort." Last year Hughes and his team conducted 94 interviews: 52 with executive management, 30 with division leadership and 12 with board members. They also surveyed 180 people from the field. "We rotate our sample selections, have a good geographic coverage and include both large and small hospitals."

Each person is asked to name their top three risks. Hughes then compares the top 10 lists from each group to identify how well they are aligned and to identify any significant differences. "We try to identify whether the differences are because of a communication or a perspective difference." By expanding participation, HCA has been able to identify new and emerging risks. "When we first started surveying hospital management, some risks popped up that weren't on the radar that probably should have been. They were early warning signals," he said.

To prioritize the top 10, they employ a 10-point scale ranking system (Number 1 risk gets five points. Number 2 risk gets three points and the third risk gets two points) that scores each risk on the basis of the answers to the following three questions:

1. What are the top three business risks that the company faces over the next two years that could have a significant adverse effect on the company's ability to achieve its strategic and /or financial objectives?
2. What are some of the things the company is doing to help manage/mitigate these risks?
3. In your opinion, are these risk mitigation strategies effective? "That in itself is valuable information," Hughes explained. "Some interviewees may think we're not doing enough or the right things, and sometimes those voices are not being heard. Capturing that information and feeding it back can be very important."

Both scores and related comments are tabulated. "We add up all the points to get to our top 10," said Hughes.

Based on his analysis of the risk lists, Hughes creates a one-page "risk universe" document that includes all the company's significant risks. The document follows the four-quadrant COSO framework (strategic, operations, reporting and compliance risk categories) as well as input he receives from other companies. "We've used the risk universe for the past four to five years." This represents the known risks to the company at that point in time. We review and update it several times each year as new risk information becomes available. This simple view of the company's risks has been favorably received.

From a management standpoint, "Our focus is on identifying the risk and what is being done to manage them? Who owns the risk? What's the mitigation strategy. Is it adequate?" These same 10 items are disclosed to investors in the Risk Factors section of the Form 10-K and discussed by senior leadership and the board on a rotating basis as topics on the Board's agenda.

"We give the board the risk universe before we interview them. After the process is completed, we present the top 10 list and discuss the comments," said Hughes. They like the one-page risk universe and it also shows how we're thinking about risk," he explained. While the board gets less detail than management, "we present the top 10 risks along with some of management's quotes and information on how they're being managed and mitigated," he said. "They put those risks on the board's agenda so those risks are part of board meeting conversations.

"Our role is to facilitate the process for the CEO," Hughes explained. "The board should provide risk oversight, but the CEO should own the process. It's up to the business owners (management) to address the risk." For HCA, the facilitation process fits nicely under

the umbrella of IA. So Hughes reports to Audit, but he is not actually part of it in order to maintain his independence. Within HCA, "IA has a very good reputation."

Hughes' team is fairly thinly staffed. "My responsibility is ERM, business continuity and SOX …That covers strategic, operational, and financial and compliance risk. Most of the staff works on the BCP planning. Given the nature of the business, "that's a big risk for us." Some of the hospitals are in risky weather zones. And as the healthcare system went digital, BCP has also meant robust system recovery plans. During crunch time, when the company needs to consolidate all the survey data and comments and put together presentations, Hughes temporarily pulls some staff from IA. "It's not a full-time role."

The ERM benefits

According to Hughes, there have been several big benefits to the program. Not all were entirely expected.

Strategic planning. While the ERM program focuses on risk identification and mitigation, risk is not viewed as a one-sided thing: there's an upside and a downside. From a management decision-making standpoint, this means "we may decide we're not taking enough strategic risk, or managing it too closely," Hughes explained. If so, "there's an opportunity with change to be pursuing those operations or take a more entrepreneurial approach to the business," he said. "We try to look at how we can manage this risk to an acceptable level."

There's been a change in the organizational mindset and risk management has become intertwined with strategic planning. "People start thinking about risk differently," he said. Initially, risk was viewed as a way to say 'no'. "Now it has evolved into people considering risk as we start new initiatives. You don't always want to be the one in the room saying it's too risky when someone comes in with new business case," Hughes said. "This has made it okay to think about what our risks are within the strategy and how to mitigate and manage those risks, so we can make sure the strategy is successful," he said. "People aren't afraid to talk about risk. It's encouraged. So rather than being the 'nay sayers,' it's more about 'have you thought through this? What if this assumption is incorrect? What's our action plan if it doesn't work? That's a huge advantage."

Better alignment. One of the "biggest advantages that I didn't really foresee, is it that ERM has improved communication up and down the line," Hughes said. "During the first couple of years, there were differences in the risk view between the top and the bottom. For the last few years [those views] have been very similar. It's a tool to help ensure people are working toward similar goals and objectives."

Board communication. Another big side benefit has been an improvement in board education. HCA was public, then private, and now public again, so it has gone through various board regimes. The ERM program provided a context that allowed the board to quickly understand risks as viewed by management. "They [sic] really embraced ERM as a way for them to better understand the business," Hughes said. "We got good feedback from the board on the process. They enjoy it," Hughes said. "I talked to companies that don't interview the board. Some tried and the board said no. I'm not sure why that is. Our board has been very open to that."

Success factors

Hughes offered the following advice to ERM newcomers:

1. **Sell it to the top.** "It's got to be something the CEO wants and drives, or you won't get the management involvement you need." said Hughes.
2. **Don't overdo it.** If you start too big you may never finish. Get some quick wins and the key to that is not getting too detailed too fast.
3. **Get to the right people.** Involve the people who are involved in the strategy and understand the business.
4. **Condense the information.** Hughes also recommended that companies keep their visual presentations and reporting at a high level. "Think about your audience, and what the result is going to be so there's not too much detail," he said.
5. **Benchmark.** Finally, he said, "look at what others are doing to get ideas." That's why he attends the North Carolina State University Poole School of Business ERM initiative. "We've met with other companies. Sharing best practices helps strengthen everyone's program. That's why I really like the ERM Roundtables held at the North Carolina State University twice a year."

Case Study 4: Johnson Controls

Since 2007, Johnson Controls has been implementing a disciplined ERM program that tightly connects risk identification, assessment and mitigation to core business processes. Driven from the very top, the ERM effort is "baked into" the strategic planning process, and includes clear policies as well as frequent communication with the company's board.

Johnson Controls (JCI) is a $42 billion diversified company in the building and automotive industries. Incorporated in 1885, JCI's operating income is split nearly evenly among its three main business segments as are its revenues globally, among Europe, the U.S. and other markets. It has a long track record of profitability, with earnings growth recorded in all but one of the past 21 years.

Getting started

ERM emerged on JCI's senior management's radar screen in 2007. "The impetus was from the board," recalled John Sibson, VP of Strategy. "My program is easy to run because I set the tone at the top, starting with the board telling the CEO that this [ERM] is a priority. Ergo, it's a priority for the CEO," said Sibson. To back up the rhetoric, the CEO has never missed a risk committee meeting. "I have perfect attendance from the CEO,' said Sibson. "The tone from the top is a very big deal."

A team of high-potential individuals was assigned to the project and it spent nine months studying the topic, including benchmarking other best-in-class companies. The team developed a risk assessment process, conducted the initial enterprise-wide risk assessment and proposed a risk management implementation plan. "This was post-Enron, post-WorldCom and there was growing attention on risk management," Sibson said.

The team came back with a set of recommendations:

- Process led by VP/Corporate Strategy - incorporated in the planning process
- Risk horizon should be linked to the 10-Year Marker (JCI's long-term vision document)
- Annual validation of corporate and business unit risk universes (top 50 risks each)
- Workshops (4 – Corp, AE, BE, PS) will generate risk heat maps (2 dimensions)
- Corporate will review businesses risk priorities
- Risk mitigation planning will be the responsibility of the businesses
- Review of risk mitigation will occur as part of the strategy process

"What was unique about the recommendation was the suggestion that corporate strategy should own that [ERM] activity," Sibson said. That recommendation was interesting inasmuch as studies by groups like the Corporate Executive Board (CEB) have found that less than 10 percent of companies have placed ERM in strategy, while the majority placed it as part of Internal Audit or Legal. Yet the CEB data support the idea of placing ERM in the strategy function. While ERM is often in Internal Audit or Compliance, those risks are generally not the ones that bring down companies. "The real drivers are basic strategic issues," Sibson explained, "like people stop buying your product, poor post-M&A integration, competition, and price wars, which supported the concept of strategic planning ownership."

Getting the process in place

When the initial team came back with its recommendations, JCI identified 86 distinct risks and organized them into six categories: strategic, external, operational, people, financial and legal and compliance. By 2013, the universe has expanded to 106 risks. Many were added in 2009, according to Sibson, as the financial crisis revealed some risks that no one had anticipated.

The original recommendation to create a two-dimensional mapping tool has since been transformed. When the first two dimensions – likelihood and impact – were considered, there was immediate confusion regarding scoring whether current mitigation activity should be considered. The decision was made to add a third, current effectiveness dimension. More recently, JCI has added a fourth dimension: the velocity of risk, or how

quickly it may "hit" the organization. The four are incorporated into a simple, intuitive online tool that's called the Johnson Controls Solution Risk Navigator ™.

Each November-December, the ERM risk universe is refreshed. Each business unit chooses the most relevant top-50 risks from the universe of 106 and then creates a link to the web tool and that link is pushed out to all the program participants – around 350 senior executives. Then the participants map each of the 50 risks in four dimensions. The data from the five mapping exercises are consolidated across the corporation by the strategy group. Business unit leaders are responsible for managing and mitigating their own top 10 list as well as any additional risks that "touch them" from the corporate consolidated list, "so they typically manage around 15 or 16 risks," Sibson said.

Initially, the process involved only the 50 most senior executives in the organization – the senior corporate staff and the business unit presidents and their direct reports. But over time, that group has expanded six-fold. But Sibson doesn't see it expanding much further. "At some point, it [ERM] requires a broad breadth of exposure to the business. You go much deeper and people's focus tends to be much narrower. We have a good participation level."

From day-one, the ERM program ran concurrent to the JCI's strategic planning schedule and a September 30 fiscal year-end. The business unit plans support the accomplishment of JCI's 10-year "marker," or where the company wants to be in 10 years. Each year, corporate leadership and the business unit presidents review where things are vis-à-vis that marker, what changed since the last review and what new risks need to be considered when refreshing the plan. That process coincides with the verification of the risk universe during November and December. Next, the company devises "where we need to be and what needs to happen to get there," Sibson explained. "The consideration of the risk environment is critical," he said. Again, the timing fits. Key risks are first presented to corporate management in March, which gives business leaders several months to incorporate them into their plans. The plans are presented to the Board in May and the risk mapping output is reported to the board in a July Risk Narrative report. The strategic plan and profit plan is approved by the board in September and the plans are communicated to the broader organization in October. And that's where the entire process begins again.

In addition to the annual reporting, the top risks are also organized into one-page dashboards that describe the risk/problem statement, the mitigation plans including who's responsible and what metrics are used. Those dashboards are updated twice a year and shared with senior leadership and the board. (This is only a small part of the full scale risk communication "touch points" for the board; see below.)

To make the risk map a useful tool, "we wanted a visual map with color schemes and shapes, but a four dimensional tool, proved problematic," remembered Sibson. "People were focusing on the top right quadrant." Management was concerned it was creating blind spots. For example, risks of lesser impact that are much more likely but not residing in the upper right quadrant were being overlooked.

To ensure such risks are properly monitored, Sibson created a straightforward formula that takes the average of the risk's likelihood and impact, minus the current effectiveness score plus the velocity to arrive at a total risk score. The formula required some tweaking because low probability and low impact risks with a high velocity would get pushed to the forefront. And just because a risk is moving fast doesn't mean it's very material. The resulting score is used to rank the risks and chart them on a map. Another potential blind spot is created by the effectiveness score: To ensure effectively managed risks are still being tracked, ERM highlights the highest scoring ones and suggests that Internal Audit devote a small percentage of their audit activity to verifying actual performance vs. leadership perception.

Identifying risk ownership

Of course, 106 risks are too many for any single person to manage. In fact, Sibson stressed, "there are no dedicated risk professionals at JCI (not counting insurance). ERM is managed by strategic planning and select other members of the Risk Committee. In each business unit, responsibility for monitoring the entire risk universe is divided among the business unit presidents' direct reports and, for corporate, among the functional staff reporting to the CEO. The business unit head

of human resources, for example, would have all the people-related risks. "This enables the BU president to have a staff meeting a week or so in advance of each Risk Committee meeting where emerging risk concerns are shared and made available to the risk lead," said Sibson. The risk lead represents the business unit at the Risk Committee.

The Risk Committee wasn't part of the original risk governance organization. It was established in 2009, in response to a board request that JCI leadership re-assess the adequacy of the company's ERM efforts. "If you think about all that was happening during the financial melt-down in 2009, the board felt it was appropriate to question whether we were doing enough," according to Sibson. That year, four out of five webinars held by the National Association of Corporate Directors was on risk management. "The board asked the CEO to have me to reassess what best-in-class ERM looked like at other companies." Sibson turned to the Corporate Executive Board for help. "CEB said our program in its current form would qualify for second quartile performance. I asked what it would take to get us to the top quartile," he recalled. The answer: JCI needed a process to identify emerging risks, as well as clearly identify the company's risk appetite and improve overall communication with senior management and the board.

To address these issues, JCI did three things:

1. It revamped the risk organizational structure
2. It created a process to identify emerging risks and set risk appetite
3. It increased its "touch points" with the Board

Step 1: The Risk Committee

JCI's Risk Committee initially included eight members but has expanded to 10. It includes the CEO, the CFO, head of HR, the General Counsel and the VP of Strategy (John Sibson). The Executive Director of Risk and Insurance was added in 2012. The Committee also includes the four business risk leads who are appointed by the segment presidents and selected from the global leadership team. "The assignment serves as a developmental opportunity for future leaders of the company" Sibson explained.

The committee meets quarterly and communicates to the board via detailed minutes. Each meeting includes a prepared agenda that "bubbles up" from the various "pillars" that make up the company's overall enterprise risk effort. The total risk management effort includes Sibson's ERM program, Insurance Health and Safety, Legal/Compliance, Enterprise Security and Internal Audit. During the Committee sessions, Sibson ensures there are at least 30 minutes of open, roundtable discussion designed to help surface emerging risks that may not have made the list of top items identified in the mapping activity. Recent examples include the border safety with Mexico, where the company has significant operations and political risks in Argentina and Venezuela.

Step 2: Defining a risk appetite

In 2010, JCI deployed a CEB benchmark process for establishing risk appetite. At the time, the approach involved establishing a list of statements around risk appetite that defined the company's willingness to take on risk in different areas. For JCI, that meant coming up with 30 different statements covering 10 different focus areas. "Some of the statements were very quantitative and very clear," Sibson said. For example, the company established a minimum desirable credit rating of BBB+ for long-term debt and A2/P2 for short-term debt, which guaranteed access to the commercial paper market and meant any initiatives "would not jeopardize this credit rating," Sibson explained. Others were much more qualitative. "The problem was there were too many of them and a lot of them were qualitative, for example statements about diversification levels, or about maintaining a balance between business units share of invested capital and share of operating profit," Sibson said. What JCI found is that the statements were very subjective. "It wasn't a dynamic document that drove more informed decision making," Sibson said.

As risk-appetite thinking evolved, JCI revised its approach. "Nine months ago, we began to leverage a process highlighted by Canadian utility Hydro One in a document by the CEB," Sibson said (see Figure 4). Hydro's approach was to identify a series of simplified strategic objectives and then identify the company's existing and desirable risk tolerance against those objectives. Hydro pinpointed five strategic objectives: sustainability, safety, profitability, revenue growth and reliability. It then ranked each risk based on the answers to three simple

Figure 4: Ask Three Questions to Set Risk Appetite
Hydro One's Qualitative Risk Appetite Rating Scale

hydro one

Three Powerful Questions
- Only three questions are needed to get a good sense of executives' risk appetite.
- Asked in sequence, these questions help register a real understanding of committing to a risk appetite.

Rating	Risk Taking Philosophy	1 Tolerance for Uncertainty How willing are you to accept uncertain outcomes?	2 Choice When faced with multiple options, how willing are you to select an option that puts this objective at risk?	3 Trade-Off How willing are you to trade-off this objective against achievement of other objectives?
5-Open	Will take justified risks	Fully anticipated	Will choose option with highest return, accept possibility of failure	Willing
4-Flexible	Will take strongly justified risks	Expect some	Will choose to put at risk, but will manage the impact	Willing under certain conditions
3-Cautious	Preference for safe delivery	Limited	Will accept if limited, and heavily out weighed by benefits	Prefer to avoid
2-Minimalist	Extremely conservative	Low	Will accept only if essential,and limited possibility/extent of failure	With extreme reluctance
1-Averse	"Sacred" risk avoidance is a core objective	Extremely Low	Will select the lowest risk option, always	Never

Source: Corporate Executive Board

questions, scored them and used the average ranking to express theoretical risk tolerance. The questions were:

1. How willing are you to accept uncertain outcomes?
2. When faced with multiple options, how willing are you to select an option that puts this objective at risk?
3. How willing are you to trade off this objective against achievement of other objectives?

JCI went through a similar exercise. It identified 26 objectives, financial, operational and strategic. "We take those three questions and consolidate the result and for each we have a bar chart that shows theoretical risk appetite for a collection of risks." Then, "you use the concept of risk appetite to set your strategic vision and deliver that vision," Sibson explained. For example, the company had to rank its concern about maintaining the BBB+ rating against its financial and strategic objectives. "Our risk appetite on some of these factors is set by strategic priorities," said Sibson

For some objectives there's little or no risk appetite (i.e., a score of 1), for example around ethics, integrity and financial reporting. However, while safety is ranked at a very low risk tolerance, it's not a 1. That's because in some cases, tradeoffs need to be made. JCI's biggest customers are automakers. They rely on just-in-time (JIT) delivery to their plants. If the plant is in a potentially risky jurisdiction, JCI still needs to have a local presence. "We do everything to protect the safety of our employees," said Sibson. But it in order to maintain its business, not locating the plant at a nearby site is not an option. "You go back to those three questions, and there are cases where you accept a choice only if you have to, and make the tradeoff with extreme reluctance," he explained.

JCI assessed actual practice to desired state. There are some cases where the desired risk tolerance differs from the actual risk tolerance. Those help management identify areas where the company needs to take more or less risk. "We eventually plan to measure our leadership's ability to close the gap," said Sibson.

The measure of success is translating all these risk indicators into action. The company has proven it can do that. For example, a couple of years ago, JCI identified

technological breakthrough as one of its risks. Sibson referred to Michael Porter's Five Forces model which posits that companies typically do a good job understanding their current customers, suppliers and current competitors. When they fail, it's often because they didn't see a new competitor or substitute product coming to market. (Think of Kodak vs. Sony or Netflix vs. Blockbuster). "It's often the new entrants and the substitutes," Sibson said "that kill companies." The key to success is anticipating those forces.

To this end, JCI developed a disciplined process by which it monitors the market for potential competition, new technologies, new players as well as potential technology acquisitions. It has increased its work with universities and national labs and came up with a clear action plan to mitigate risk in this critical area mitigation. It expanded its focus and activities to more external forces to better prepare for emerging technologies. That involved a better understanding of developing technologies and in a couple of cases even investing in venture capital funds.

Step 3: Improved communication to the board

Finally, JCI increased its level of communication with its board. The board receives the Risk Committee's detailed minutes every quarter. In January, the company provides a dedicated Risk presentation to the board that highlights key risk topics. In addition, in July, Sibson provides a 50-page narrative about the ERM program which identifies the process, the top risks from the annual mapping output, progress on management and mitigation plans in the business units (dashboard updates) and other significant areas of risk discussion. That document goes to the board but is also distributed to senior management and team leaders who are involved in ERM activities. In addition, Internal Audit creates its own narrative every January, including their activities, audit plan and risk areas. "We're touching the board in more places," Sibson said. In fact, on average, so aspect of ERM is before the board 10 times a year.

The reception across all these communication lines has been very positive. Emerging during the second week of May 2013 from JCI's annual risk and strategic plan meetings with the board, Sibson said: "Just yesterday a director told me he appreciates the clarity and depth of the meeting minutes. They appreciate the level of detail and candor."

Lessons learned

Based on his six-year journey, Sibson advised his peers to consider the following key success factors:

1. **Set the tone at the top.** In the three and a half years of the Risk Committee's existence, the CEO has never missed a meeting, establishing through his actions that ERM is critical to the company's strategic efforts. Meanwhile, "It's critical that the board drives ERM from their level," he said.
2. **See risk as the flipside of opportunity.** Sibson said it's important that risk management stands for risk mitigation, not "risk minimization."
3. **Come up with a program that fits the organization.** For JCI, that did not mean setting up a group of dedicated professionals. "Had we hired a CRO with a $10 million budget, 30 people and a mountain of incremental administration it would have been a disaster," said Sibson. It's important to assign risk responsibility. Risk sits at the business levels and needs to be owned primarily by the business units. There's not necessarily a need for a standalone ERM apparatus.
4. **Broaden the scope.** ERM doesn't start and stop with an ERM program. It should have a broad view of risk, to include other areas such as safety and audit.
5. **Involve management in identifying risks.** "That senior leaders are part of the scanning apparatus is important," said Sibson.
6. **Make it easy.** "The tools we've created are simple and enable us to increase participation without adding administrative burden," he said.
7. **Increase communication.** Finally, report to the senior leadership and the board often, he advised. "The board appreciates the frequency and substance of this information."

Case Study 5: Zurich in North America

The U.S. operation of an insurance company headquartered in Switzerland has had a long tradition of embedding risk management into its culture, so that ERM informs every aspect of financial and capital management and is part of everyday business processes.

At Zurich, "ERM is first and foremost about effectively managing capital," said the company's Chief Risk Officer, Barry Franklin, "so you are financially capable of delivering on your promises to stakeholders, customers and investors."

While financial institutions are often perceived as being at the forefront of ERM, that's not necessarily the case with every single one. "A lot of companies haven't quiet mastered it yet," said Barry Franklin, CRO of Zurich in North America. "Even within the insurance context, there's still a wide array of ERM practices and companies at different points along the maturity curve," he said. However, "at the ones that are fairly mature and have been doing it for a very long time, ERM is well established and has worked its way into the culture." At Zurich, "when you talk about ERM, people have a pretty good idea what you're referring to," he said. Many of the risk management practices that Zurich has implemented may not be identified as ERM "because they have become so much a part of what we do. Risk management is embedded into normal processes," he said.

The three pillars of ERM

"When I look at the foundation for a company such as us, you have to have a mature program that rests on the company's entire financial management and capital management discipline," Franklin explained. At Zurich, "ERM is first and foremost about effectively managing capital. Second, it's about encouraging and supporting risk based-decision making. And third, it's about supporting and encouraging a risk-aware culture."

Capital management

ERM within the capital management context is about protecting the company's capital base, "so you are financially capable of delivering on your promises to stakeholders, customers and investors." To do this, Zurich employs an economic capital discipline, and establishes risk tolerance levels for business areas. "The process is very objective and analytical but incorporates some qualitative considerations as well," Franklin said.

At the group level, Zurich operates in about 170 countries and multiple lines of business across many legal entities. "Capital management for the Zurich Group relates primarily to a target debt-rating equivalent, which is a common approach." For Zurich that means maintaining a target capital level that's consistent with an AA rating, which in turn implies a 99.95 percent likelihood of remaining financially solvent over a one year horizon, a type of VaR measure. Based on capital model output and analysis, Zurich establishes target monetary tolerance levels, which also take into account correlations among different risk types, geographies and lines of business.

Reflecting correlations and dependencies brings complexity to the model, but "it's important because a large diversified insurance company needs less risk capital on proportional basis for the same level of perceived security, than does a similarly sized company operating in a single line or geography," Franklin explained. "This broad diversification is a key aspect of Zurich's strategy, and our approach to capital modeling helps us ensure our capital management practices remain aligned with that strategy." There's a process to reconcile the model and analysis to make sure we're allocating that diversification effect appropriately, to take into consideration the overall group desired risk tolerance level as well as quantify the diversification. "When we discuss the model, diversification and capital allocation it's important to remember we're talking about economic capital, which represents a theoretical number or the level you should have," Franklin said.

"Theoretical capital should reflect your forward-looking business strategy, which suggests a certain level of capital to support future business activity." Then there's real capital, or what an insurer must hold for regulatory purposes. "There's not necessarily a mathematical connection between the two," he said. "One is based on economics. The other varies by regulator and jurisdiction." While the economic capital (should) drive their business decisions insurers have to comply with regulatory capital requirements.

Franklin acknowledges that financial organizations have the advantage of being able to more easily quantify risk in terms of quantitative models. "Financial managers in non-financial organizations still need to have a way to analyze and allocate capital and to ensure everybody is looking at Return on Capital at some level. But it's more challenging. It's not quite as apparent to those outside of the Finance area why that type of capital focus is necessary, and the underlying data might not be as readily available," he said.

"Very few non-financial companies use sophisticated capital models to drive decisions at lower levels, e.g., pricing. They'll get there over time," Zurich's Barry Franklin predicted. "When you do, it's quite powerful."

Risk-based decisions

The way ERM is worked into decision-making is by trying to make risk-adjusted return decisions. Zurich uses capital-intensity ratios by product line or region to make sure the business it is writing is priced appropriately to achieve the desired overall return on capital, according to Franklin. "That also helps guide decisions on the make-up of the risk portfolio," he said. The sophistication of models used to drive those decisions depends on a company's maturity level. "Very few non-financial companies use sophisticated capital models to drive decisions at lower levels, e.g., pricing. They'll get there over time," he predicted.

"When you do, it's quite powerful. People start thinking about things in terms of risk metrics. Everybody is using the same set of ratios and metrics to guide decisions such as how much business to write or whether to invest a certain amount in a project or acquisition," Franklin said. "It brings things together under a common framework." That sort of approach has been widely adopted in insurance because it's a natural way to make business decisions.

"There are metrics people have used for a long time around pricing in our industry," Franklin said. "We can now take risk metrics and translate them into the more traditional ratios for a particular operating entity or line of business in order to achieve a target return on risk capital under the current return environment." Of course such disciplined thinking is not applied to every decision, for example the decision to procure pencils or copier paper.

Culture and governance

The final pillar of ERM is setting up a governance process that explicitly recognizes risk. At Zurich, there are risk committees at all relevant levels of the organization – beginning with the risk committee of the board – with clear responsibility and process for engaging risk in the business. "People understand what to expect from the risk area," Franklin said. "We have a very robust risk policy that is adopted and signed off at the highest level and is refreshed regularly. Everybody in a decision-making role is aware of that policy. Within each entity, owners are assigned for every risk process and every year they must attest that in they're in compliance with applicable provisions of the policy," Franklin said. The risk management group administers that process.

There's also an iterative process designed for evaluating exceptions and developing action plans to achieve compliance. That's because it's impossible to come up with a single policy that works in every case. "We have one group policy that's applied by thousands of people in hundreds of countries. It's impossible to have a 'one-size-fits-all' policy," he said. "We have the policy and then we deal with exception as one-offs to make sure that appropriate factors are taken into consideration." When an exception is made, it's revisited each year. As markets and operating environments change, the policy

can be revised accordingly, with agreement by the risk committee of the board," Franklin said.

Zurich also has a very well-developed governance structure for ERM that is headed by the global CRO who is a member of the group executive committee and the risk committee of the board. This individual has held a number of senior positions and is well known and very visible. Reporting to him are segment CROs. And each of them has a structure beneath them that covers the business on a regional basis and within that, by country or sub-region depending on scale and complexity. "I report to the CRO for general insurance business globally and I'm responsible for North America," Franklin said. "My team here is viewed as supporting the North American business units while at the same time providing independent assurance.

We talk about our governance approach as fitting within a three lines of defense model, which comes back to reinforcing the culture."

1. The first line of defense is the business management, the people making day-to-day business decisions like underwriting decisions.
2. The second is compliance and risk management. "Compliance looks at regulatory concerns, i.e., playing by the rules in the various states, provinces and countries within which we do business," Franklin said. "Risk management is making sure we're applying appropriate risk guidance and providing tools and frameworks to manage decisions. We coordinate very closely with both compliance and legal"
3. The third line is the independent internal audit function.

Lessons learned

Support from the top

"It's critically important that the most senior level of the organization supports and communicates the ERM program," Franklin said. "If people don't see leadership supporting the process and actively engaging in the process, they're not going to think it's important," he said. "I've seen examples where companies decided to implement an ERM program and the CEO might assign responsibility to the CFO who assigns it to the Treasurer who then assigns it to the Assistant Treasurer, and it becomes a one-time project that's done at mid-level and never sees the light of day," he cautioned. "If there's not an expectation created at the board or executive committee level that they're going to see something different as a result of implementing ERM, then in all likelihood the ERM effort will fail."

It takes time

"There's a life cycle to implementing these programs," Franklin said. So that top-level support "helps you get started." But it needs to be sustained so that management supports the process to make it through the time period it takes to embed the process and tools in the organization, because that can take a number of years."

Identify a champion

The best organizational structure will depend on the company size and culture. "For a mid-size organization, it may not make sense to set up a separate risk function; there's not going to be enough to do," Franklin said. "But there ought to be some dedicated resources where it's clearly part of individuals' objectives to execute this. If it's everyone's responsibility then it's really no one's," he said. "There has to be somebody leading the charge who has support and visibility within the organization to get things done. That may or may not be a full time CRO position."

Think of risk as being two-sided

"If risk management is viewed as 'the people who say no,' then we're not doing our job," Franklin said. "One of the reasons we have the processes we do and rely on financial metrics and risk-based decision-making is to help identify opportunities. If we have a choice of growing in a line of business vs. another, they [sic] may have similar loss ratios and may look like they would produce similar results, but when you look at return on risk capital, one may be a better opportunity," he explained. "We're using the tools we have to make better decisions to build a risk portfolio that is value added. While ERM is there to protect the capital base, "that satisfies one set of stakeholders: customers and regulators. However, you also need to look after the interests of the other stakeholders such as investors and employees. That requires you to take advantage of opportunities as well."

Some companies confuse operational with business risk. "We get paid to take business risk, but investors don't pay us to take operational risk," Franklin said. That's true for almost any company. "Many companies outside of the insurance industry get compensated to take risk – by developing new products, expanding into new markets overseas and so on," said Franklin.

Operational risks are "those areas that you do want to avoid or minimize. They cost money when you don't control them well but don't necessarily add value when you do control them well. You need to identify operational risks and address them, because they really have no 'upside' opportunity associated with them." That's why Six Sigma approaches tend to be implemented in organizations with little or no tolerance for downside risk.

"I encourage companies to consider what it is they want to get out of ERM," added Franklin. "If they just want to pursue a one-time project to say they've done it then they shouldn't even bother. It's not a project. It's a way of doing business." To succeed, "set expectations for what you intend to get out of it over the long term."

He recommended practitioners talk to peers within and outside their industry to find out what others are already doing. "You can learn a lot from consultants as well, and consultants can bring great value once you've determined where you want to go with ERM" he said. "But it's your decision and you own it. There are consultants who have wonderful knowledge and tools, but at end of the day they're trying to sell you services. You need to think long and hard about what you want to get out of ERM before engaging a consultant for ERM implementation services, and it may be a good idea to engage an experienced business consultant to assist with just that portion of the exercise before proceeding. Better to learn from somebody else's success and mistakes."

About the Author

Nilly Essaides is Director of Practitioner Content Development at the Association for Financial Professionals. Nilly has over 20 years of experience in research, writing and meeting facilitation in the global treasury arena. She is a thought leader and the author of multiple in-depth AFP Guides on treasury topics as well as monthly articles in AFP Exchange, the AFP's flagship publication. Nilly was managing director at the NeuGroup and co-led the company's successful peer group business. Nilly also co-authored a book about knowledge management and how to transfer best practices with the American Productivity and Quality Center (APQC).

CORPORATE TREASURERS *Council*®

Corporate Treasurers Council

The Corporate Treasurers Council is the executive-level membership of AFP. The CTC features tailor-made products, events and exclusive networking opportunities all year long for treasury and finance executives that address the latest industry insights, trends and best practices and will provide guidance, practical tools and the validation needed to move forward in making critical decisions.

When you join AFP and have the title of *corporate treasurer, assistant treasurer, chief financial officer, vice president of finance or controller,* you are automatically enrolled in the Corporate Treasurers Council (CTC) and have access to CTC products and events. For more information go to www.corporatetreasurers.org

Association for Financial Professionals®

About the Association for Financial Professionals

The Association for Financial Professionals (AFP) headquartered in Bethesda, Maryland, supports more than 16,000 individual members from a wide range of industries throughout all stages of their careers in various aspects of treasury and financial management. AFP is the preferred resource for financial professionals for continuing education, financial tools and publications, career development, certifications, research, representation to legislators and regulators, and the development of industry standards.

General Inquiries	AFP@AFPonline.org
Web Site	www.AFPonline.org
Phone	301.907.2862

The bricks to build something of value

Quality, honesty, integrity and trust are critical to every successful business. With these important elements as your foundation, you can begin to build real value.

Through our global network of firms with more than 180,000 people in 158 countries we provide quality advisory, assurance and tax services to many of the world's most successful companies. For more information about how we can support your strategic risk management needs, contact:

Eric Cohen
Principal
(646) 471 8476

Peter Frank
Principal
(646) 471 2787

pwc