

Balanced Scorecard Report

THE STRATEGY EXECUTION SOURCE

SEPTEMBER – OCTOBER 2011 : VOL 13 NO 5

Managing the Multiple Dimensions of Risk—Part II: The Office of Risk Management

By Anette Mikes, Assistant Professor, and Robert S. Kaplan, Baker Foundation Professor, Harvard Business School

In the second article of their two-part series, the authors explore the concept of an Office of Risk Management along with a case study of an innovative risk management function at JP Morgan Private Bank. They also look at the “softer” components of risk management, including a comparison of two different, equally effective risk officer styles and roles.

The 2010 BP Deepwater Horizon oil spill was spectacular not only in its magnitude but also in its irony. When Tony Hayward became CEO of BP in 2007 after a series of refinery explosions and major pipeline leaks, he vowed that safety would be his top priority. Among the safety rules he instituted were those requiring all employees to use lids on coffee cups while walking and prohibiting employees from texting while driving. Three years later, Hayward presided over one of the worst man-made disasters in history: the explosion of the leased \$560 million oil rig in the Gulf of Mexico. Eleven workers died, and more than 4 million barrels of oil spilled into the Gulf, endangering wildlife and plants, and disrupting lives and commerce all along the Gulf Coast. The cost of the cleanup alone will likely exceed \$40 billion, not counting the cost to BP’s reputation. The National Commission’s Report to the President attributed the disaster to significant management failure—failure that crippled “the ability of individuals involved to identify the risks they faced, and to properly evaluate, communicate, and address them.”¹ Even greater economic and social damages resulted from the global financial crisis of 2007–2009, another spectacular failure enabled by poor risk management at companies and regulators.

In Part I of this series, we introduced a multiple-category view of risk, arguing that organizations must tailor their risk management processes to the inherent nature and controllability of the different categories of risks they face. Building on this framework, we focus here on the roles of an internal risk management function. Multiple units in a company can be involved in risk management, including the finance and internal audit departments, and a formal risk management department headed by a new organizational executive, the chief risk officer (CRO). There is no one way to organize an enterprise’s risk management functions. Specific types of risk are best managed by

continued on the following page



ALSO IN THIS ISSUE:

- Designing a Sound Governance System to Drive Strategic Transformation at ADWEA 6
- Quantifying Value in Tax-Funded Tourism Marketing at the Canadian Tourism Commission 10
- Never Underestimate the Importance of Soft Skills in Executing Strategy 14

WHAT DOES IT TAKE TO BE A STRATEGY EXECUTION CHAMPION?

Learn how the 20 winners of the 2010 Palladium Balanced Scorecard Hall of Fame for Executing Strategy® achieved breakthrough results. Get your copy of Strategy Execution Champions: The Palladium Balanced Scorecard Hall of Fame Report 2011, available at www.strategyexecutions.com.

DON'T MISS A SINGLE ARTICLE. GET YOUR FREE BSR INDEX TODAY.

Download the latest compendium of the entire Balanced Scorecard Report archive—the nearly 350 articles published since BSR’s inception. It’s organized by more than two dozen topics, and it’s free at www.index2010.hbr.org.

JOIN US!

Register to join Kaplan and Norton’s Palladium Execution Premium Community (XPC), the premier online destination for strategy and performance management and Balanced Scorecard practitioners, and receive the free monthly BSC Online newsletter. Learn more and become a member at www.thepalladiumgroup.com/xpc.

¹ “Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling,” National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Report to the President (January 2011).

RISKS	RISK MITIGATION OBJECTIVE	CONTROL APPROACHES	RISK ASSESSMENT APPROACH	OFFICE OF RISK MANAGEMENT: CONTRIBUTION	OFFICE OF RISK MANAGEMENT: RELATIONSHIP WITH BUSINESS LINES
Category I Employee misconduct and misbehavior ("known knowns")	Drive incidence of occurrence to zero	Internal control; boundary systems; mission and value statements; internal audit	Control self-assessments; diagnostic controls; near-miss data collection; operational loss databases	Coordinate or oversee common controls with internal audit function	Independent overseers
Category II Strategy execution ("known unknowns")	Reduce likelihood and impact in cost-efficient way	Key risk indicator scorecards; risk mitigation initiatives; risk reviews at strategy review meetings	Risk maps with nominal scales; statistical risk estimation models (VaR, risk-adjusted capital, risk-based performance measures)	Run risk workshops and risk review meetings; help develop portfolio of risk initiatives; act as devil's advocates and integrators (systems thinking)	Independent overseers and/or embedded risk managers
Category III External, uncontrollable ("unknown unknowns")	Reduce impact should risk occur	Contingency planning; insurance and hedging programs (limited)	Risk envisionment; scenarios; war games; "tail-risk" assessments; mental models	Run scenario-planning and war-game exercises with management team; act as devil's advocates and integrators (systems thinking)	Embedded risk managers

■ FIGURE 1: THE OFFICE OF RISK MANAGEMENT—WHAT IS THE VALUE ADDED?

The ORM coordinates risk management across the enterprise. Whether it is independent or embedded depends on many factors; there is no one-size-fits-all approach.

specific staff functions that carry out critical risk management processes. The staff function that coordinates risk-management activities is the Office of Risk Management (ORM), which may be a virtual office if those activities are spread across multiple organizational units. Every ORM should follow these three principles:

1. Complement (rather than displace) existing internal audit and management control practices.
2. Promote business-relevant discussion and debate in the business lines.
3. Challenge business executives about the risks emanating from their strategies.

Risk management involves running or facilitating processes that help identify, assess, and control uncertainties in order to turn them into “manageable risks.” It involves periodically reviewing and, if necessary, revising risks and controls in light of new information and evolving objectives. Risk management also counters the organizational tendency to become inured to risks, accept deviances and near misses as the “new normal,” and override

controls. In short, risk management encompasses the formal processes through which an organization learns about, and attempts to prevent the forgetting and incubation of, risks.²

If existing functions performed all these risk management processes well, then an ORM would be redundant. However, the organizations we studied over the last 10 years concurred that an ORM adds value through two mechanisms. First, it promotes the continual questioning of existing controls: Are they fit-for-purpose in light of the organization’s underlying and evolving risk profile? Such an oversight role requires independence from the business lines. Second, the ORM helps businesses envision uncertainties and risks that are outside their day-to-day thinking but that, once identified, can be mitigated and managed and converted to controllable risks. In this second capacity, the ORM must demonstrate its understanding of and relevance to the business lines and their strategies in order to engage them in a constructive and ongoing dialogue on risk. The dual requirement on the ORM to deploy independent overseers as well as

embedded, business-savvy risk managers is a formidable structural and human resources challenge.

Thus, the ORM both strengthens existing compliance systems and serves as an internal devil’s advocate to elevate the awareness and discussion of enterprise risks. ORM staff must learn to balance their conflicting roles as independent compliance advocates and embedded and trusted business advisers.

Independent Risk Oversight

Internal controls have traditionally served as the first line of defense against losses from employee misbehavior—called Category 1 risks in our framework. (See Figure 1.) The independent internal audit function monitors and evaluates the effectiveness of these controls.³ Even for such known risks, the risk management function must be ever alert to changes in the organization’s strategy and the external environment that might create new challenges for compliance and controls. Consider the case of JP Morgan Private Bank (JMPB), one of the most successful global private banks, known for its award-winning service and innovation. JMPB offered clients investment opportunities in both internally managed and external funds. The company’s regulators, wary of the bank’s ample opportunities for self-dealing and conflicts of interest, required it to perform substantial due diligence not only on the external funds but also on the internally managed funds so that investment managers would not direct client assets internally when better external options existed. Thus, in addition to maintaining traditional internal controls—including routinely reviewing risks from inadequate documentation, clearing, and settlement or reporting—JMPB’s risk management function also had to ensure that all investment managers complied with external regulatory requirements. It subjected every internal and external investment product to strict due diligence. Those that passed this vetting process with high marks could be

2 A. Mikes, “Stepping into the Unknown: How Companies Learn Through Risk Management,” FS Focus, Vol. 50 (June 2011).

3 According to the internal control-integrated framework defined by the Committee of Sponsoring Organizations of the Treadway Commission (1992).

added to the private bank's investment offerings, but would still be reviewed regularly and could be removed from the platform at any time.

Starting in 2007, JMPB's independent risk management function became aware of new risks emerging from the deteriorating credit quality of counterparties that executed financial transactions for the bank's investing activities. In response, the risk management function bolstered its assessment of every counterparty's credit quality and instituted new compliance policies. These policies included a new internal process (and accountability) for rapidly seizing collateral in the event of a counterparty default, enhanced documentation to enable JMPB to take possession of such collateral, and documentation of the collateral's location. The increased scrutiny and stringent collateral requirements of these new policies served the bank well during the financial crisis, minimizing its counterparty losses.

Managing Strategy Execution Risks

Complex organizations may well know some of the risks associated with their strategies. But they also tend to be less sensitive to the new risks they take on when entering new strategic territories. For example, BP had decades of experience in hydrocarbon exploration and production, but drilled the Macondo well in an area where it had less knowledge of the underlying geology.⁴ Especially when operating under time and cost pressures, complex organizations have a tendency to forget and incubate risks they previously knew about by becoming selectively indifferent to them. A study of NASA's *Challenger* shuttle launch disaster documented the "normalization of deviance" and the acceptance of "routine non-conformity" to preestablished standards as major contributors to the disaster that took the lives of eight astronauts.⁵ At BP's Macondo well, numerous early warning

signs about the increased likelihood of a major risk event became evident to the drilling rig crew: gas bubbles appeared, fragments of rubber seals floated to the surface, concrete didn't seal the wellhead as expected, and instruments stopped working or signaled unusual conditions. But BP was paying roughly \$500,000 a day to lease the rig, which was already 43 days late for a new drilling job. As a review board concluded, "With the clock ticking, bad decisions went unchecked, warning signs went unheeded, and small lapses compounded."⁶

The goal of the risk management function is not to inhibit or stop risky projects. Strategies with high expected returns—whether drilling for oil in new and difficult places, sending unmanned missions across the solar system in search of the origins of life, investing in new securities that offer greater and apparently uncorrelated returns—generally come with higher risks. In fact, an effective risk management function should enable an organization to undertake higher expected-return projects, as it mitigates those higher risks to acceptable levels. The risk management function should not stifle risk; its role is to identify the risks that accompany the strategy and adopt cost-effective interventions to mitigate the most likely and consequential ones.

In Part I, we described the active and intrusive risk management process introduced by Gentry Lee, an expert in aerospace engineering and the chief systems engineer of NASA's Jet Propulsion Laboratory. For every project, Lee formed an independent risk review board that met periodically with the project team and performed the devil's advocate role, challenging and debating assumptions, requiring set-asides of funds and time reserves to mitigate the highest risks, and making recommendations to senior management about whether the project, and eventually the launch, should proceed. Lee's risk management process directly

affected the day-to-day business of project teams. Arguably, a similar process for each of BP's major deep-drilling oil exploration and production projects would have revealed the risks of a blowout, prompting the company to devote more resources to reduce its likelihood, such as through employee training and enhanced and more reliable instrumentation.

An alternative approach to risk management was led by John Fraser, the chief risk officer at Hydro One (another organization we discussed in Part I). Fraser, whose expertise lay in banking, not utilities, was a much less intrusive and hands-on risk manager than Lee. He had no formal qualifications to challenge Hydro One's engineers at risk assessment workshops and risk-based resource allocation meetings. Fraser was a facilitator, not a devil's advocate, at risk review meetings. His office collected and moved information about Hydro One's critical and material risks up, across, and down the organization.

Consider a third organizational approach to managing strategy execution risks instituted at JMPB in 2007. The chief investment officer of a major internal fund, Global Access, recruited a small group of market-oriented risk managers to work closely with him and his portfolio managers to think more deeply about the risks across positions, with the goal of improving overall returns and protecting the portfolios from major downside shocks.

Embedded risk manager Gregory Zhikarev explained his role:

My colleagues in independent [compliance] risk management who sit outside the Global Access team don't necessarily have the proximity and real time visibility of what trades and risks are being taken. So we want somebody on the inside looking out for everybody's interest, and that person is me. I serve as a close business partner to portfolio managers . . . responsible for keeping portfolios in alignment

4 Commission, *Report to the President*, *ibid.*, p. 89.

5 D. Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (University of Chicago Press, 1996); and D. Vaughan, "The Dark Side of Organizations: Mistake, Misconduct, and Disaster," *Annual Review of Sociology*, Vol. 25 (1999).

6 I. Urbina, "In Gulf, It Was Unclear Who Was in Charge of Rig," *The New York Times* (June 6, 2010).

Despite the efforts of risk-regulating authorities to issue standards and guidelines about how to conduct risk management, we are quite confident that “one size does not fit all.”

with both broad Private Bank-level policies ... as well as Global Access-specific, market-risk-related items such as trade approvals, portfolio risk analysis, positional concentrations, etc. ... [M]y role is to keep portfolio managers honest. ... I listen to their views so I can help them fine-tune what they should sell and buy in order to reflect their views in their portfolios.

JMPB's other embedded risk managers, like Zhikarev, continually asked “what if” questions, requiring portfolio managers to look at different scenarios and think through their implications for the bank's business. They challenged managers' assumptions and actions, and helped portfolio managers design trades prior to approval at investment committee meetings. For this, they had to help portfolio managers assess how proposed trades contributed to the risk of the entire investment portfolio—not only under normal circumstances but also under extreme stresses. For example, under conditions of market distress, the correlation of returns across different asset classes such as stocks and bonds increases dramatically. Stress testing helped investment managers estimate potential tail losses (for low probability events). Zhikarev explained that stress testing made managers consider system effects and the unintended consequences of their planned actions: “Portfolio managers come to me with three trades, and the model may say all three trades are adding to the same type of risk. Nine times out of 10 a manager will say, ‘No, that's not what I was trying to do.’ Then, we can sit down and redesign the trades.”

Mary Callahan Erdoes, CEO of JP Morgan Asset Management, reflected on the importance of the expert risk managers embedded within the Private Bank. “Things happened in 2008 that no one ever contemplated. You need these highly

sophisticated, highly savvy people who have market skills and who can think about the what ifs.”

Three companies, three different roles for managing strategic risks. In our assessment, each of the different risk management functions served their companies well. Lee, for Mars missions, and Zhikarev, for asset allocation decisions in turbulent market conditions, addressed high-risk technical problems. They needed domain expertise if they were to be credible when actively questioning the assumptions of project engineers and investment managers, and confident in their judgment about whether to accept or veto the decisions of the line managers they served. Fraser dealt with wide-ranging enterprise risks that included human resources issues, access rights across aboriginal-owned territories, governmental regulation of prices and service, ice storms, asset maintenance and reliability, and financing. This universe of risks was much wider than that faced by Lee and Zhikarev. For this reason, Fraser facilitated but did not make Hydro One's risk-based resource allocation decisions. He formed an alliance with the company's headquarters planning function, which consisted of former field and project engineers. This expert group actively engaged with project engineers during asset-planning and resource allocation processes to provide expertise and discipline to the risk-based resource allocation process.

From these case studies, we have tentatively concluded that effective risk management must be contingent on the scope of activities and strategy of the organization. Despite the efforts of risk-regulating authorities to issue standards and guidelines about how to conduct risk management, we are quite confident that one size does not fit all. In enterprises

that follow focused, often project-based, strategies, the greatest risks stem from execution-related issues, especially when line experts enter new territory. The discussion of these risks requires senior risk officers who are themselves experts. For firms like Hydro One that have complex and diverse operations but are not pushing the envelope into new territories, the risk management function does not need subject matter expertise in all the risk issues the enterprise faces. It would be impossible for the ORM or any senior risk officer to have or develop in-depth expertise across Hydro One's operating processes. In such cases, the ORM facilitates an active risk management process that channels diverse risk information to the relevant and appropriate decision-making echelons of the organization and increases the risk awareness of frontline employees.

Envisioning the “Unknown Unknowns”

People in all organizations find it particularly challenging to think about Category III risks that are not only external and uncontrollable but also outside the realm of their known experience. Indeed, it is hard to predict complex systems, and anyone who aspires to do so must bear in mind the warning of Nobel laureate economist Friedrich Hayek: “[W]ith essentially complex phenomena, the aspects of the events to be accounted for about which we can get quantitative data are necessarily limited and may not include the important ones.”⁷ But partial, qualitative, and fragmented information about such “unknown unknowns” often does exist in complex organizations, waiting to be pieced together by the creative imagination of those who look across organizational silos to envision unlikely events that could place the strategy, and possibly the entire enterprise, at risk.

We believe that formal envisioning exercises, such as war gaming, scenario analysis, and tail-risk stress testing, help uncover the enterprise's vulnerability to unexpected external events. Therefore

⁷ F. Hayek, “The Pretense of Knowledge,” Nobel Prize acceptance lecture, quoted in L.G. Crovitz, “Tsunamis of Information,” Wall Street Journal (March 21, 2011).

these exercises must be considered an integral part of any organization's risk management function. If an existing corporate department, such as strategic planning, already conducts such exercises, then the ORM need only monitor and help facilitate them. But if no current organizational unit currently has expertise or the responsibility to conduct envisioning exercises, then this role defaults to the ORM.

At JP Morgan Chase, the CEO, supported by the company's chief risk officer, chairs regular tail-risk committee meetings at which managers brainstorm about how to avoid or mitigate risks in extreme circumstances. As Barry Zubrow, the company's CRO, tells us, "Most of the events we discuss at these meetings never occur, thank God; but a few of them do happen, and we either have already mitigated their consequences or, because of our prior contingency planning, acted rapidly to minimize the damage."

The tripartite risk management role at JP Morgan Chase is a model that many enterprises have started to embrace within and outside the financial services sector. It consists of a strong, centralized compliance function for known risks; embedded risk managers who serve as risk advisers and coaches of business unit leaders; and an active, visible leadership team at the top that conducts regular scenario-planning exercises and tail-risk meetings.

Can Independent and Embedded Risk Managers Coexist?

The JMPB case raises an interesting organizational issue about the tension between centralized, independent risk managers and those embedded within business units as advisers and counselors to line managers. Independent risk managers are often seen only as compliance champions. As the controls and processes they operate are by nature bureaucratic, they struggle to gain recognition from the business lines. JP Morgan Asset Management's Erdoes remarks: "Risk management could very much be driven by an old-fashioned, backward-looking, check-the-box mentality." Risk managers' reliance on the "regulatory crutch" is a

common problem in companies that initially introduced risk management under the imperative of compliance with external rules. JP Morgan's answer to this concern was an active, visible leadership team at the top promoting the value added of risk management's role. As Zubrow told us, "I may have the title, but [CEO] Jamie Dimon is the chief risk officer of the company. He sets the tone at the top."

Embedded risk managers generate an opposite type of conflict and concern. As risk managers become members of the business team, they could "go native," reducing their vital devil's advocate role in challenging line managers' decisions and actions so that they can become accepted as value-added members of the inner circle. Some regulatory and corporate governance guidelines stress the importance of having an independent risk management function, which contradicts the idea of embedded risk managers. The ORM will ultimately have to choose, or strike a balance between maintaining independent oversight versus partnering with the business lines to embed risk management into operational and strategic decisions.

Risk Management and Strategy Execution: Separate or Integrated?

A final choice organizations must make is whether the Office of Strategy Management (OSM) should include the proposed new ORM. At a time when companies are trying to trim corporate staffs and reduce administrative overhead, introducing a new corporate function will not be met with enthusiasm. But managing risk is different from, and even opposed to, managing strategy execution. Strategy is about focus and specialization. Strategy should focus a company's resources—physical, financial, and human—on achieving competitive advantage in well-defined product, customer, and industry segments. It involves investing disproportionately in relatively few applications. Risk, in contrast, involves thinking about what can go wrong with even well-crafted and well-executed strategies. Often risk mitigation requires dispersing resources and diversifying investments—just the opposite of strategy execution.

Viewed in this way, risk management should be complementary and separate from strategy management, so that senior management gets exposed to both perspectives. As Zubrow's words imply, the CEO must simultaneously be the chief strategy execution officer and the chief risk officer, making the final decisions, with board oversight and approval, about the balance between return and risk. Embedding the risk management function within an OSM introduces the very real concern of subverting risk considerations to strategic priorities. Only by having a completely separate and independent function can the two competing viewpoints be developed fully and professionally, bringing the relevant information on strategies as well as their risks to the decision-making processes of the senior leadership team. ■



Anette Mikes is an Assistant Professor at Harvard Business School, where she teaches financial reporting and control. In 2010, she launched (with Robert Kaplan) the new executive education program Risk Management for Corporate Leaders. She holds a PhD from the London School of Economics.



Robert S. Kaplan, along with David P. Norton, created the Balanced Scorecard concept. The Baker Foundation Professor at Harvard Business School and Chairman of Professional Practice at Palladium Group, he also codeveloped activity-based costing. Kaplan has authored or coauthored 14 books (five of them with Norton), 20 Harvard Business Review articles (eight with Norton), more than 130 papers, and dozens of articles for BSR.

To learn more

See A. Mikes, C.S. Rose, and A. Sesia, "J.P. Morgan Private Bank: Risk Management During the Financial Crisis 2008–2009," Harvard Business School Case (2010: 311-003).

REPRINT #B1109A