HARVARD | BUSINESS | SCHOOL

Risk Management—the Revealing Hand

Robert S. Kaplan
Anette Mikes

Working Paper 16-102

Risk Management—the Revealing Hand

Robert S. Kaplan
Harvard Business School

Anette Mikes
HEC Lausanne

Working Paper 16-102

Risk Management—the Revealing Hand

Robert S. Kaplan, *Harvard Business School*, and Anette Mikes, *HEC Lausanne*

Abstract

Many believe that the recent emphasis on enterprise risk management function is misguided, especially after the failure of sophisticated quantitative risk models during the global financial crisis. The concern is that top-down risk management will inhibit innovation and entrepreneurial activities. We disagree and argue that risk management should function as a Revealing Hand to identify, assess, and mitigate risks in a cost–efficient manner. Done well, the Revealing Hand of risk management adds value to firms by allowing them to take on riskier projects and strategies. But risk management must overcome severe individual and organizational biases that prevent managers and employees from thinking deeply and analytically about their risk exposure. In this paper, we draw lessons from seven case studies about the multiple and contingent ways that a corporate risk function can foster highly interactive and intrusive dialogues to surface and prioritize risks, help to allocate resources to mitigate them, and bring clarity to the value trade-offs and moral dilemmas that lurk in those decisions.

Risk Management—the Revealing Hand

"In a well-functioning, truly enterprise-wide risk management system, all major risks would be identified, monitored, and managed on a continuous basis."

-- Rene Stulz[1]

The combination of financial reporting transgressions in the early 2000s and the failures of large financial services companies during the global financial crisis of 2007-2008 has led to legislation and regulations requiring an increased role for enterprise risk management. Some believe, however, that increasing the power and influence of risk management will have an adverse effect by inhibiting innovation and entrepreneurial activities. Such concerns are not unique to the current era; the developmental economist Albert Hirschman believed that too much concern about future threats can discourage people from undertaking bold new ventures. He introduced a principle, which he called "the Hiding Hand," that explicitly excused incomplete and inadequate risk assessment. Not dwelling on future threats, he claimed, "can serve as a stimulus to enterprise" by encouraging otherwise risk-averse managers to take on risky projects that in the bright light of thorough risk assessment would appear infeasible.[2]

We believe, to the contrary, that planning practices should be guided not by the Hiding Hand, but by a Revealing Hand that enables risks to be identified and then mitigated in a cost-effective manner. Risk management, as stated by veteran NASA systems engineer Gentry Lee, is "not a natural act for humans to perform." Well-documented psychological and sociological biases within organizations lead them to overlook important risks and to systematically underestimate and undermanage those they do identify.[3] When managers are overconfident about their strategies and projects, early identification and discussion of

[1]Rene Stulz, "Risk Management Failures: What Are They, and How Do They Happen?," *Journal of Applied Corporate Finance*, 2008, p. 44

[2] The infamous principle of the Hiding Hand has come to epitomize a particular view of entrepreneurship that sees each project accompanied by two sets of partially or wholly offsetting developments: first, a set of possible threats to its profitability and existence (in today's parlance: risks), and second, a set of unsuspected remedial actions that can be taken once the threats materialize. The logic is that committed to, and caught up in, a project that has encountered difficulties, the entrepreneur must mobilize all creative resources and problem-solving energy at her disposal. According to Hirschman, there is a dual fallacy that necessitates the Hiding Hand: first, planners tend to underestimate challenges and risks, and at the same time they also underestimate their organization's creative capacity to deal with those challenges. See Hirschman (1967: 15). (Full citations of all articles cited in the notes are provided in the References at the end of the article.)

[3] Kahneman (2011).

risks are required to discipline corporate risk-taking and to limit to acceptable levels the expected consequences from risk-taking behavior. Most policymakers, regulators, and academics—particularly those who work or specialize in the financial services sector—agree that greater internal clarity about and public disclosure of material risks are likely to lead to better decision-making. But there is far less agreement about how the Revealing Hand of risk management should go about this assignment.

Some risk management experts embrace a culture of "quantitative enthusiasm." They believe that the most important role of the corporate risk management function is to identify and then measure risks. Such risk "quants" rely on their ability to express risks in the form of statistical distributions, including the correlations among them, for use by corporate decision-makers when (1) comparing the expected outcomes of risky alternatives; (2) evaluating the effects of risky investments on the value and risk of the firm's entire "portfolio" of assets and businesses; and (3) benchmarking the firm's aggregate risk exposure against its risk appetite.

Nassim Taleb and others have provided a forceful critique of this quantitative approach to risk management. They note that almost all financial risk models failed during the global financial crisis, and in other recent bouts of market volatility, to signal the huge losses (labeled by Taleb as "Black Swan" events) that occurred with far greater frequency than expected.[4] The failures of the models led to severe loss of confidence in quantitative risk managers as an effective Revealing Hand mechanism. If statistical models fail to function when they are needed the most, risk management necessarily "changes from science to art."[5]

The decline of quantitative risk models, however, should not prevent us from recognizing the potential value from implementing an effective corporate risk management function. Indeed, admitting that risk management is more art than science helps to introduce some humility into the risk function—and to the standards that govern this function—that should enable a company's risk management function to become more reliable and more effective. Such humility begins by recognizing that, among the range of management disciplines, risk management is one where measurement is particularly difficult and, indeed, a source of problems in its own right. Measurement generally involves the attempt to quantify events or phenomena that have already occurred or that already exist. But risk management addresses events in the future, those that have not yet

[4] Taleb (2007).
[5] Stulz (2008: 43).

occurred and many that may never occur. In many if not most circumstances involving risk management, completely objective measurement is clearly not possible—and thus a large element of subjectivity inevitably enters, and often ends up, properly, dominating the analysis. Financial markets are a partial exception to this observation to the extent that the past behavior of asset prices can be a reliable predictor of future price behavior. Academic studies tell us that this is true in general, perhaps more than 99% of the time. But as already noted, all bets are off during major discontinuities, when the Black Swans make their appearance. During these times, past price distributions and correlations provide little guidance on the magnitude of risk exposure and how to mitigate it.

Since the global financial crisis, many quantitative skeptics, including some from within the financial services sector, have challenged the quantitative risk managers. The skeptics advocate that effective risk management must go beyond measurable risks to encompass qualitative approaches that will better help managers in thinking about how good projects and strategies might turn bad, and how their organizations would fare under different scenarios.[6]

In this article, we examine the scope, the processes, and the consequences of the quantitative and qualitative components of risk management. We begin with the premise that those seeking to find common ground to reconcile the two approaches can learn from cases, both inside and *outside* the financial services sector, of challenges faced by the Revealing Hand of risk management, and how these can be overcome. To advocates and practitioners of quantitative risk management, the world of current corporate practice appears messy, political, and gloomy. In an article published in this journal eight years ago titled "Risk Management Failures: What Are They and When Do They Happen?" Rene Stulz offered the following assessment:

> Once risk management moves away from established quantitative models, it becomes easily embroiled in intra-firm politics. At that point, the outcome depends much more on the firm's risk appetite and culture than its risk management models.[7]

In the pages that follow, we present a somewhat more optimistic view of risk management, one that does not abandon quantitative financial models, but does rely less

[6] Mikes (2009, 2011).
[7] Stulz (2008:43)

heavily upon them. But in providing this moderately optimistic view of risk management, we provide an emphatic caveat emptor: We have studied many man-made disasters, both in the public and private sectors, and what we have found repeatedly is this: Early warning signs and risk information were available to operators and decision makers in advance of the events, but behavioral biases and organizational barriers prevented the information from being acted on. Despite much talk of "unknown unknowns" and "black swan" events, risk identification appears to be the lesser of two challenges.[8] The principal challenge faced by organizations and their risk managers is their failure to act in the face of accumulating—albeit ambiguous and inconclusive—evidence of an imminent and catastrophic event. Accordingly, one of the major aims of this article is to explore the role, organization, and limitations of risk identification and risk management, especially in situations that are not amenable to quantitative risk modeling.[9]

We have conducted multiple studies of organizations whose risk management systems have been characterized by both (1) *longevity* (they had been in existence for at least five years) and (2) *credibility* (they had the active support of top management). We have tried to understand how risk management tools and processes functioned within the strategy and operating environment of each company. These examples have helped us understand when technology and quantitative models are likely to be productively employed in risk management, and when risk management processes require extensive discussions and highly interactive meetings as a substitute for objective risk measurement.

The Principle of the Revealing Hand

The Jet Propulsion Laboratory (JPL), a research and development center that manages capital-intensive, time-critical technological projects for the U.S. National Aeronautics and Space Administration's (NASA) unmanned space missions, experienced several costly and avoidable failures in the 1990s.[10] Post mortems revealed that JPL's risk assurance function, among its other shortcomings, was focused on checklists for quality

[8] Turner (1976); Pidgeon and O'Leary (2000).
[9] See Stulz (2015); Mikes and Kaplan (2015).
[10] The Mars Climate Orbiter disappeared, during orbit insertion on Sept. 23, 1999, due to a navigation error; analyses had been performed and communicated using English units (feet and pounds) rather than NASA-mandated metric units (meters and kilograms). The Mars Polar Lander disappeared as it neared the surface of Mars in December 1999. To save money, the Lander did not have telemetry during its descent to Mars and subsequent analysis suggested that the failure was probably due to a software fault that shut off the descent rocket too early, causing the spacecraft to fall the last 40 meters onto the surface.

control, while overlooking many risks—such as errors stemming from engineers working in English rather than Metric units—that had "incubated" for a long time in functional silos.

After the two spectacular failures in 1999, JPL hired veteran aerospace engineer Gentry Lee as chief system engineer—in effect the chief risk officer—to develop and implement a new risk management approach for its planetary and outer space missions. Lee defined his role as "minister without portfolio, the person who made sure everything worked the way it was supposed to on a global scale." He described how he thought about mission risks: "At the start of a project, try to write down everything you can that is risky. Then put together a plan for each of those risks, and watch how the plan evolves."

This conception of risk management, unusual at the time, flew in the face of the previous risk culture at NASA, which had been epitomized by the famous 1992 pronouncement of chief administrator Daniel Goldin: "Be bold—take risks. [A] project that's 20 for 20 isn't successful. It's proof that we're playing it too safe. If the gain is great, risk is warranted. Failure is OK, as long as it's on a project that's pushing the frontiers of technology."[11]

Goldin's pronouncement was clearly consistent with Hirschman's Hiding Hand principle. As Hirschman advocated,

> Since we necessarily underestimate our creativity, it is desirable that we underestimate to a roughly similar extent the difficulties of the tasks we face so as to be tricked by these two offsetting underestimates into undertaking tasks that we can, but otherwise would not dare, tackle.[12]

But Hirschman studied public sector officials who lacked confidence and were highly risk-averse. He wanted the Hidden Hand to instill an optimistic bias so that bold, high-value public investments could be identified and approved.

Lee recognized that JPL had exactly the opposite problem of Hirschman's risk-avoiding bureaucrats. Risk-taking at NASA and JPL was rampant, and culturally accepted. It was encouraged, and engrained in the new DNA of the organization, especially after Goldin's advocacy of "faster, better, cheaper" missions. Lee believed his principal challenge was to counter the overconfidence and optimistic bias of his technically very capable engineering colleagues by revealing to them the actual riskiness of their projects:

---

[11] Daniel Goldin, transcript of remarks and discussion at the 108th Space Studies Board Meeting, Irvine, CA, 18 November 1992; Daniel Goldin, "Toward the Next Millennium: A Vision for Spaceship Earth," speech delivered at the World Space Congress, 2 September 1992.

[12] Hirschman (1967): 13)

> JPL engineers graduate from top schools at the top of their class. They are used to being right in their design and engineering decisions. I have to get them comfortable thinking about all the things that can go wrong. … Innovation—looking forward—is absolutely essential, but innovation needs to be balanced with reflecting backwards, learning from experience about what can go wrong.

Many managers inside NASA, and in many other enterprises regarded risk management as the "business prevention department." Lee, a principal inspiration for our formulation of the Revealing Hand principle, believed strongly that risk management should not curtail innovation and risk-taking. Rather, rigorous risk management of innovative projects should *enhance* the organization's innovative capacity and its capability to accept risky projects, increasing their chance of success. Lee's disciplined approach to risk identification and mitigation was designed to overcome the overconfidence of innovative project leaders who had never experienced failure in their professional work.

Not a Natural Act for Humans to Perform…

As mentioned earlier, we now have extensive evidence of a general tendency of individuals, whether they face uncertainty alone or in large organizations, to place too much weight on recent events and experiences when forecasting the future. This leads them to grossly underestimate the range and adverse consequences of possible outcomes from risky situations.[13] Nobel laureate Daniel Kahneman contrasts what he calls "System 1 thinking," which proceeds rapidly and is driven by instinct, emotion, and extensive practice, with "System 2 thinking," which is deliberate, analytical, and based on evidence. This framework helps explain why risk identification is difficult. People, using their familiar and instinctive System 1 thinking, do not naturally activate the analytical and non-intuitive System 2 thinking required for effective risk management. Managers and employees, especially under budget and time pressure, become inured to gradually emerging risks and their System 1 thinking leads them to override existing controls and accept deviances and near misses as the "new normal"—a behavioral bias that has been given the wonderful name of "normalization of deviance."[14] By treating red flags as false alarms rather than early warnings of imminent danger, they end up tolerating unknowingly

[13] For studies providing evidence of biases such as "availability," "confirmation," "(over)confidence," and "anchoring," see Hammond, Keeney, and Raiffa (2006); Kahneman, Lovallo, and Sibony (2011); and Kahneman (2011).
[14] Vaughan (1999).

an increase in vulnerability to risk events. Companies also make the mistake of "staying on course" when they shouldn't. As events begin to deviate from expectations, managers instinctively escalate their commitment[15] to their prior beliefs, "throw good money after bad," and incubate even more risk.

In addition to these biases of individuals, organizational biases such as "groupthink" inhibit good thinking about risks. Groupthink arises when individuals, still in doubt about a course of action that the majority has approved, decide to keep quiet and go along. Groupthink is especially likely when the group is led by an overbearing, overconfident manager who wants to minimize conflict, delay, and challenges to his or her authority.

All these individual and group decision-making biases help explain why, in the years running up to the global financial crisis, so many organizations overlooked or misread ambiguous threats and failed to foresee the huge downside risks to their asset holdings and high leverage. Wall Street banks also hired the "best and the brightest," people with little if any past experience with failure. Their combination of brilliance, overconfidence, and impatience to succeed led to the creation of innovative, apparently highly profitable, but also highly risky securities in organizational cultures that celebrated and rewarded bold, short-term risk-taking. For example, during a decade of declining interest rates and macro-economic stability, Stanley O'Neal and Charles Prince, the CEOs of Merrill Lynch and Citigroup, respectively, pushed their companies to take on more risk to avoid being left behind in the race for trading profits.[16]

Especially in innovative, high-performing companies, it is hard for cost and profit-conscious managers to invest more resources in risk identification and risk mitigation, particularly when nothing appears to be broken.[17] Gentry Lee believed he would not have been given the authority or resources to install a risk management process at JPL unless and until a number of NASA's Mars and shuttle missions ended in catastrophic failures.

The Revealing Hand of risk management must be forceful and intrusive to allow individuals to activate "System 2" careful thinking about risk. It requires intrusive, interactive, and inquisitive processes to accomplish the following: (1) challenge existing assumptions about the world internal and external to the organization; (2) communicate risk information, aided by tools such as risk maps, stress tests, and scenarios; (3) and draw

[15] Staw (1981).
[16] Nocera (2008).
[17] Mikes (2008).

attention to and help close gaps in the control of risks that other control functions (such as internal audit and other boundary controls) leave unaddressed, thereby complementing—though without displacing—existing management control practices. As discussed later, the companies that we examined in our case studies deliberately introduced highly interactive and intrusive risk management processes to counter the individual and organizational biases that would otherwise inhibit constructive thinking about risk exposures. In short, they illustrated the Revealing Hand in action.

Limitations of Regulated and Standardized Risk Management

After the global financial crisis, consultants and policy makers reached the conclusion that, as articulated by Ernst & Young Partner Randall Miller, "companies with more mature risk management practices outperform their peers financially."[18] Consultants offered to show less risk-savvy companies how to reap the "likely profit margin increase" that has accrued to "risk management leaders… over the last three years"[19] and to achieve the spectacular EBITDA-differentials between the "top" and "bottom" of the risk management maturity scale.[20]

Despite such claims, academic studies have yet to confirm whether and how risk management practices add value.[21] We can also be skeptical of the universal and standardized procedures that consultants advocate as best risk management practices. Their surveys of contemporary practice document the widespread creation of risk management departments, risk committees and the hiring of specialized staff for these (not surprising given recent regulations and guidelines that mandate, or strongly recommend them). The surveys also provide evidence of widespread adoption of risk management tools such as risk ratings, KRIs, horizon scanning, scenario planning and stress testing.[22] But what these large sample surveys fail to provide is convincing evidence of the quality, depth, breadth, and impact of risk management in the adopting organizations.

For example, a company may have a risk management department run by a professional CRO who has the expressed backing of the CEO and board. But unless that CRO also has the resources, leadership, and support to reveal the company's strategy risks proactively and authoritatively, his or her department may be largely ineffective. Simple

[18] EY (,2012).
[19] PWC (2015).
[20] EY (2012).
[21] Mikes and Kaplan (2015)
[22] The most popular ones are documented by PWC (2015).

surveys of practice do not reveal how often risk professionals prevented high risk projects from going forward. Nor do the surveys offer much of a sense of the kind and value of the help CROs provide business managers when setting and trying to adhere to the firm's declared "risk appetite."[23] Not surprisingly, the surveys also document that mandated and codified risk management practices have not been embraced by corporate managers.[24] A survey of C-suite executives reported that fewer than half believed that their organization had an effective risk-management program.[25]

Risk Management Observed

Our bottom-up, inductive approach for understanding effective risk management programs sheds light on why risk management is difficult to codify and standardize. In Table 1, we list the case studies that we have studied in detail.

Table 1. Risk Management Observed: Cases and References

Case	Highlights – learnings
Hydro One Mikes A. (2008). Enterprise Risk Management at Hydro One (A). Harvard Business School Case	Role of risk function: *Independent facilitator* Scope and skillset of CRO ("the triumph of the humble CRO") Action-generation by +tools: risk maps and « bang for bucks » indices +processes: dialogue and workshops +risk-based resource allocation
LEGO Group Mikes A. & Hamel D. (2012). The LEGO Group: Envisioning Risks in Asia (A). *Harvard Business School Case*.	Role of risk function: *Independent facilitator* Scope and skillset of CRO (" the triumph of the humble CRO") Action-generation by +tools: scenarios +processes: dialogues and workshops +scenario planning linked to annual planning process
Jet Propulsion Laboratory Kaplan R. S. & Mikes A. (2010). Jet Propulsion Laboratory. Harvard Business School Case.	Role of risk function: *Business partner* Scope and skillset of CRO (expert, devil's advocate and decision maker) Action-generation by +tools: risk maps +processes: risk review workshop (gateway meetings) +culture of intellectual confrontation +time and cost reserves, tiger teams and humility

[23] Stulz (,2015).
[24] RIMS and Advisen (2013).
[25] KPMG (2013).

Private Bank Mikes A., Rose C. S. & Sesia A. (2010). J.P. Morgan Private Bank: Risk Management during the Financial Crisis 2008-2009. Harvard Business School Case.	Role of risk function: *Business partner and compliance champion* Scope and skillset of CRO (expert, devil's advocate but not decision maker) Action-generation by +tools: risk models and sensitivity analyses +processes: face-to-face meetings with traders, weekly asset allocation meetings +culture of individual autonomy in risk perception ("everyone must have a view") +dual risk function includes embedded (business partner) versus independent (compliance) risk managers
Corporate Bank ("Wellfleet", pseudonym) Mikes A. (2009). Risk Management at Wellfleet Bank: All That Glitters Is Not Gold. Harvard Business School Case.	Role of risk function: *Business partner and compliance champion* Scope and skillset of CRO (expert, devil's advocate but not decision maker; compliance champion) Action-generation by +tools: risk models and sensitivity analyses +processes: face-to-face meetings with relationship managers, credit approval chain, credit risk committee +culture of powerful risk voice +dual risk function includes embedded (business partner) versus independent (compliance) risk managers
Retail Bank ("Saxon Bank", pseudonym) Hall M., Mikes A. & Millo Y. (2015). How Do Risk Managers Become Influential? A Field Study of Toolmaking in Two Financial Institutions. Management Accounting Research, 26, 3-22.	Role of risk function: *Business partner and compliance champion* Scope and skillset of CRO (devil's advocate but not decision maker; compliance champion) Action-generation by +tools: scenario planning +processes: face-to-face, quarterly performance reviews +culture of individual responsibility for action-generation ("star chambers with CEO") +dual risk function combines embedded (business partner) and independent (compliance) risk managers

Investment Bank (Goldman Sachs) Authors' Interview with Chief Risk Officer Craig Brodercik and Chief Accounting Officer Sarah Smith in New York, 4 February, 2010	Role of risk function: *Business partner and compliance champion* Scope and skillset of CRO (devil's advocate but not decision maker; compliance champion) Action-generation by +tools: quantitative risk management enhanced by mark-to-market (fair value) accounting as an independent "window to risk"; expensive infrastructure (people and technology) +culture of respect for risk management, "challenge culture": controllers have final say on valuation, not traders + risk function works closely with accounting and asset management / traders

Many risk management departments operate as *independent overseers*, with an exclusive focus on compliance, internal controls, and risk prevention. This has been the traditional domain for risk management, particularly in highly regulated environment. Others, as can be seen in our sample, have moved beyond this to a *business partner* role. For example, JPL's risk function influences key strategic decisions, such as approval or veto of new projects, the quantity of resources dedicated to risk mitigation, and a final recommendation about whether to go forward with a planned mission launch. Risk management is effective at JPL because the personnel involved in the process have the domain expertise necessary to credibly challenge the risk-taking project engineers on their own turf and to interpret and react to changing conditions in and around JPL's projects.

In a third role, the *independent facilitator*, as practiced at Hydro One and the LEGO Group, the risk managers do not influence formal decision-making. Rather, they set the agenda for highly interactive risk management discussions and facilitate the communication of risk up, down, and across the organization. In this role, the CRO needs strong interpersonal and communication skills but not, necessarily, a high level of domain expertise. These CROs must operate with a degree of humility to stimulate broad and wide-ranging discussions that develop qualitative and subjective risk assessments.[26] Such assessments, in turn, help senior line managers set priorities among operational and strategy risks and allocate resources to mitigate them.

Working with limited formal authority and resources, this kind of humble, facilitating CRO builds an informal network of relationships with executives and business

[26] Mikes (forthcoming)

managers, with the aim of being neither reactive nor proactive while maintaining a careful balancing act between keeping one's distance and staying involved. Even without formal decision-making authority, the risk discussions facilitated by the humble risk manager are consequential; they identify, "map" and (to the extent possible) quantify risk exposures, and influence decisions and resource allocations by line managers who ultimately must execute risk management within their operations and authority.[27]

The apparent success of this independent facilitator model of risk management suggests that calls for increasing investments in risk management and for the formal inclusion of senior risk officers in the C-suite could be misguided. Many companies will be best served when the Revealing Hand of risk management occurs through the facilitation of risk talk and risk-based resource allocation—as opposed to top-down compliance enforcement and decision-making by the CRO. Our evidence suggests that this humble CRO role is most effective for companies incubating a wide array of risks, where neither regulatory compliance, nor any particular technical domain expertise, are required to stimulate System 2 analytic thinking and discussions about strategy risks among employees and line managers. Instead, the humble CRO brings together many different functions and market-facing units to share information and produce a common understanding of the diverse risks faced by the enterprise.

Finally, we identify a *dual or hybrid* role for risk management. As exemplified and practiced by the companies in our three financial services cases, the risk function balances compliance with business orientation by deploying separate groups of independent and embedded risk managers. It has been common in the financial services sector to lament the unreasonableness of regulators' demand for an independent risk management function.[28] One CRO we interviewed (Saxon Bank) claimed that too much independence led to less impact: "When I came [to the role], the risk management function was… so independent as to be totally irrelevant. They wrote histories of risk after the fact, they wrote criticisms of what the business did. My first question to them was, 'Where were you, honeybun, when all this happened?'"[29] The CROs in our financial services cases were critical of efforts to make their role entirely about independence *or* all about business partnering. They recognized the tension and built separate organizations to handle both types of demands. A central risk function performed the role of compliance champion and independent risk

[27] Mikes (forthcoming)
[28] Hall et al. (2015); Stulz (2015).
[29] Hall et al. (2015): 10)

overseer. At the same time, they introduced a separate, experienced cadre of embedded risk managers, with considerable domain expertise, who worked closely within the line organization to continuously advise business decision-makers about changes in their real-time risk exposure.

The diverse case studies summarized in Table 1 suggest that any observed set of risk-management practices (the ERM mix) should be unpacked into a set of fundamental components. These components (and their determinants) include at least the following:

Processes for identifying, assessing, and prioritizing risks. Risk identification can take place face to face (as was the practice in all our cases) or through self-assessments prompted remotely by a centralized database or risk register.[30] Face-to-face meetings can be intensive, interactive meetings between the risk expert and the line managers, as practiced at JPL and our three financial-services cases. Or they can involve open discussions among employees from different functions, and hierarchical levels, as practiced at Hydro One and the LEGO Group. Risk discussions can be confined to senior line managers and staff, or they can be decentralized by engaging front-line, support, and administrative staff as well. Further research is required to explicate contextual factors that influence the appropriate risk identification processes to be deployed, but the extent and kind of *interdependencies* in the task environment will likely be the dominant influence.[31] For example, the reciprocal interdependencies across JPL's design teams and across the LEGO Group's core functions—product design, supply chain, and customer relationship management—required that their risk organization needed to have a broad span of influence if it was to conduct cross-functional risk discussions. By contrast, at Hydro One and in the financial-services cases, the organizational and project units performed separate functions. In these cases, the risk workshops could be focused on the project, department, business unit or portfolio at hand, and the range of participation in risk identification was determined by the diversity of functions involved within each of these organizational units.

Frequency of risk meetings. JPL's project engineers had to make trade-offs between a mission's scientific goals and the immutable laws of physics. The risks associated with a particular mission were largely known by the end of the initial project meeting, and the laws of physics would not be changing during the course of the project. The formal review meetings at which progress on risk mitigation were actively discussed could be done annually or even bi-annually. By contrast, Hydro One's risks continually evolved from

[30] Mikes, Tufano, Werker, and De Neve (2009).
[31] Thompson (1967)

changes in demand, regulation, interest rates, and equipment. Consequently, its CRO led risk workshops among employees and managers throughout the year, did face-to-face risk assessments semi-annually with each member of the senior executive team, and conducted (risk-based) resource allocation meetings annually. The LEGO Group, similarly experiencing continually evolving and diverse risks—from changes in children's play preferences to the availability of retail partners across the world—linked its scenario workshops about risk identification and their prioritization to the annual planning process. At the Private Bank (asset management) division of a universal bank, and at the Investment Bank, risks changed hourly, or even from one trade to the next. At the Corporate Bank and the Retail Bank, risk shifted frequently enough to require continual monitoring and assessment by risk managers with strong domain expertise, embedded in the line organization. From these observations, we conclude that the frequency of risk identification and assessment processes must match the *velocity of risk evolution*, a bit of common sense that nevertheless tends to be lost in "one size fits all" compliance frameworks.

Risk tools. Most companies summarize risks with multidimensional visualizations, such as risk maps, that subjectively quantify risks according to their expected likelihood, impact, and controllability. Hydro One and JPL conducted regular assessments and reviews of their subjectively ranked "top-10" risks. Financial services companies, with extensive historical data on asset pricing, covariance, and risk events, also used risk map summaries, but they added data- and analysis-intensive statistical assessments, such as value-at-risk calculations and stress tests.

The choice of risk tools, which ranged from qualitative descriptions and scenarios to complex calculations of expected loss and exposure, appears to be conditioned by (1) the availability of data and knowledge about a particular risk (loss) and (2) how relevant and reliable the available risk tools are in the eyes of risk experts (*calculative cultures*) and everyone else using the tools. Quantitative risk management becomes impossible when historical predictive data are unavailable or have lost their ability to predict because of a paradigm-shifting discontinuity. As Rene Stulz commented about the subprime crisis:

> It was not possible to obtain a distribution of losses associated with a sharp downturn in real estate by using only historical data.… A risk manager would have needed to understand both the likelihood of a decrease in real estate prices, and the expected effect of such a decrease on the prices of those securities.[32]

[32] Stulz, (2008: 43)

But even such extreme conditions should not stop the Revealing Hand of risk management from functioning effectively, as long as risk managers recognize the novelty of the situation and are willing to temporarily abandon their now-irrelevant quantitative models. For example, Goldman Sachs stopped relying on value-at-risk modeling when it became clear that the frequency of losses far exceeded the models' predictions. It emphasized instead its proprietary daily marks-to-market across its entire subprime portfolio to assess risk exposure. At Retail Bank, risk managers co-opted the economist staff function to create scenarios that enabled them to gauge the evolution and possible severity of the financial crisis as it unfolded—again, extending the Revealing Hand by the use of alternative quantitative modeling.

Even among just the seven cases we examined in detail, effective risk managers functioned in a diversity of ways. A quest for universal prescriptions in risk management seems at best dubious, and at worst harmful—especially if it prevents companies from finding their way among the multiple dimensions of risk management to an approach customized and tailored to their specific situation.

What Can Risk Managers Learn from Man-Made Disasters?

As already noted, risk managers are currently riding a favorable tide as regulators, standard setters, and professional associations advocate the establishment of a strong risk management function. The conditions for the healthy growth of the risk management industry are highly favorable. Yet organizational disasters continue, and with growing visibility (among the most recent is Volkswagen's cheating-software scandal). Consultants have pointed to the capability gaps between increasing risks on the demand side and existing risk management programs on the supply side.[33]

> As a former CRO of the Indian IT services company Infosys commented to us:
>
> Everyone does risk management in bad times. The strong test of risk management is whether it works in good times. Will top management stand behind the risk managers, avoiding temptation, and saying no to things that put the enterprise at risk?

Managerial attention and resource allocation—in effect, active deployment of the Revealing Hand—are easy to sustain while the memory of a recent disaster or crisis is fresh. But attention can lag after a period of normality and stability. Also, new risks, such

[33] PWC (2015).

as cyber-terrorism and cyber-security, can emerge slowly and with limited visibility. Risk management practices will always lag innovation. They operate in a catch-up mode, which is why even with extensive regulation, future financial crises remain likely.

In this section we draw on the literature on man-made disasters and conclude that mere enhancement of the Revealing Hand of risk management will not alone solve the bigger problem of management inertia and inaction.

In his pioneering book about man-made disasters published in 1978, British organizational sociologist Barry Turner argued that an *incubation period*, which includes communication breakdowns and unheeded warnings, precedes all man-made disasters. A chain, or several chains, of puzzling events, near-misses, errors, and partially understood occurrences develop in a way that is at odds with existing beliefs and norms about likely sources of risk. Disaster studies reveal that at least one person in a line management role typically has crucial, risk-relevant information that (in retrospect) could have triggered actions to prevent man-made disasters from occurring.[34] Researchers have also identified a *recovery window*, a period after the emergence of a clear threat, in which constructive action is feasible before the major accident occurs.[35] For example, in NASA's Challenger and Columbia disasters, crucial, although ambiguous, risk-relevant information reached decision-makers who conducted a discussion but failed to act.[36]

We recognize that hindsight, which is of course unavailable to actual decision-makers at the crucial time, has 20-20 vision about the relevance of risk information. But even when functioning in real time and with information gaps, good risk management should have the capability to interpret and evaluate the potential downside implications from ambiguous signals—in effect, to activate System 2 thinking rather than respond instinctively and without challenging existing beliefs. Turner himself recognized this problem early on when he wrote:

> The central difficulty therefore lies in discovering which aspects of the current set of problems facing an organization are prudent to ignore and which should be attended to, and how an acceptable level of safety can be established as a criterion in carrying out this exercise.[37]

[34] Pidgeon (,1997); Vaughan (1999); Edmondson et al. (2005); Watkins and Bazerman (2003).
[35] Roberto et al. (2006)
[36] Vaughan (1996); Edmondson et al. (2005).
[37] Turner (1976:379)

Indeed, one might go so far as to argue, as another scholar did 20 years after Turner, that "Organizations are defined by what they ignore."[38]

But when multiple organizational actors have different perceptions about the risks at hand or even which risks are most important to the organization, merely increasing the visibility of risks can lead to dissonance among them. In such a conflicting situation, they will rely on their intuitive System 1 reasoning, which can ignore and incubate even visible risks. The logical consequence is no action, followed by disaster. Under novel circumstances, a firm's normally compatible strategic objectives and values come into conflict with each other and trade-offs must be made. For example, when the first actors sensed that "the music had stopped" in the CDO market, several sold large portfolios of about-to-be worthless assets to not-yet suspecting trading partners. They made a trade-off, perhaps implicitly and without conscious thought, to put their long-developed client relationships at risk so that they could sustain an alternative and now conflicting stakeholder value, to avoid large write-downs and losses. Before reaching such moments of truth, organizations should ideally be reviewing and renegotiating a consensus about the priorities of objectives and values that are most important to them. Such a consensus can then explicitly guide decision-making and trade-offs when unexpected conflicts arise.

A Three-Part Solution

In fact, coming to an agreement about the company's belief system, about its objectives, values and priorities, is the first—and in some ways the most important—of the three parts of developing an effective risk management system. The second is to formulate the firm's "risk appetite" about how much and what kind of risk can be tolerated. And third is the continuous monitoring and benchmarking of a firm's risk-taking behavior against its risk appetite.

The firm's risk appetite should clarify what risks can be accepted and left unattended, and what risks need immediate attention and action. It starts with the company leadership team reaffirming its mission and values. Consider the situation faced by the Merck executive team when the first clinical-trial evidence emerged that its blockbuster drug Vioxx was associated with an increase in cardiac incidents for patients who used it for more than 18 months.[39] Merck decided immediately to withdraw the drug from the market, following the mandate of its core value, "Merck puts patients first." Every decision

[38] Weick (1998: 74). We thank HEC student Jeannine Jeinitzer for this reference.
[39] Simons (2009, 2010).

and action Merck took, before and during the event, was consistent with this core belief that elevated a standard of patient safety above short-term profits as the corporate pre-eminent goal. Merck's CEO Raymond Gilmartin subsequently decided to litigate, not settle, every single private law suit brought against the company. He was confident—based on Merck's strong culture and value system—that even under the extraordinarily intrusive discovery rules during litigation, no Merck employee would be found to have ignored or suppressed scientific information suggesting that Vioxx put its patients at risk. Merck ended up winning all of the litigation, either at trial or upon appeal.

The FDA regulatory agency subsequently judged that Vioxx could be returned to the marketplace, reflecting the ambiguous nature of the evidence and the ability of consumers to make personal judgments between immediate and sustainable pain relief versus a modest increase in cardiac risk. But Merck refused to reissue the drug because putting patients first was such a core value.[40]

Companies under pressure and facing ambiguous threats should rely upon strong belief and boundary systems, especially their core values, to determine "whose interests come first when difficult trade-offs must be made."[41] This was precisely the situation faced by the groups NASA empowered to make decisions for the Challenger and Columbia missions. Firms reveal their actual risk appetite not by boiler plate statements, but by acting upon their underlying value priorities in truly testing situations under circumstances that force them to make trade-offs among their multiple stakeholder groups.

Some companies use a so-called radar or spider chart to stimulate discussions and clarify beliefs about their risk appetite.[42] For each of the company's key stakeholders—including customers, employees, suppliers, and regulators—a risk radar chart identifies a set of objectives and a targeted confidence level associated with meeting each of those objectives. Second, the management team chooses a target risk appetite for each of the company's major stakeholders on an ordinal scale that is designed to be comparable across all dimensions. The managers acknowledge the reality that they cannot maintain equal risk exposure across their diverse constituents. They must make trade-offs in time and resource commitments among goals such as deliver high return-on-investment for shareholders,

[40] Merck's chief competitor, Pfizer, with a very similar drug, Celebrex, and facing similarly ambiguous evidence, left it on the market after adding a black-box warning. By so doing, "Pfizer shareholders thus avoided losing billions of dollars in profits," as the Pfizer executives maintained their primary commitment to shareholder value (Simons, 2010: 4).
[41] Simons (2010: 4).
[42] Quail (2012).

retain and develop employees, build long-term customer relationships, become an excellent corporate citizen in local communities, and reduce the environmental footprint, beyond what is mandated to comply with regulations.

Hydro One's "risk appetite scale" and radar chart shown in Figure 1 provide the visual representation of these trade-offs.

----------INSERT FIGURE 1 HERE: both risk appetite scale and radar chart----------

The *risk appetite scale* enables managers and board members to discuss their willingness to compromise on any particular objective, should a trade-off become necessary, expressing the strength of commitment and priority attributed to the value or stakeholder group associated with that objective. The radar chart provides the mechanism for managers to discuss and agree to adaptations of the firm's risk appetite, as circumstances evolve, making clear the firm's choices—as proposed by management and ratified by the board. At periodic risk review meetings, managers can compare their actual decisions to those espoused in their risk radar chart. In this way, the chart enables managers to monitor—and then decide to either tighten or relax—its risk exposure among multiple constituents.

We return to the case of the financial firm selling CDOs during the financial crisis. Suppose that its decision-makers had an active mental model (a "mental risk radar chart") that visualized the firm's core values and stakeholder objectives. Then, when it had become clear that "the music had stopped," the decision to sell soon-to-be-worthless CDOs would have triggered a discussion of the trade-offs about to be made, and its implications in the short term and beyond. Following the decision, the mental or explicit risk radar chart of the firm's actual risk appetite would be updated to show a greater willingness to put long-term trading-partner relationships at risk relative to the firm's risk appetite for financial performance and, perhaps, survival. The decision to quickly exit the CDO asset class before the anticipated market decline revealed that the value of corporate survival superseded the value of long-term client relationships. Other firms decided not to merely exit or hedge their subprime risk exposure but rather to place a major bet by shorting the subprime market. After the financial crisis, these firms were widely criticized and litigated. But these examples illustrate the difficult choices firms can face; they are complex dilemmas that bring tension among the firm's commitment to serve its multiple and diverse stakeholders, including its own financial interests.

No Wall Street firm, to our knowledge, explicitly documented such trade-offs, nor would we expect them to have done this. But we believe that the Revealing Hand of risk management should make decision-makers aware of the potential conflicts of interests and moral dilemmas that are inherent in their most difficult decisions and actions. The Revealing Hand should also prepare decision-makers for the inevitable backlash that follows such "defining moments"[43] and give them the confidence to defend those actions, as illustrated by the actions of Merck's CEO at the time of the Vioxx scandal. Creating such awareness and confidence requires intrusive, interactive and intensive debates about the organization's multiple values and stakeholders, the decision-makers' attachment to each of them, and the potential long-term consequences from a difficult decision made at a defining moment. The risk radar chart provides a summary of the conclusions from such debates and serves as a continuous guide for management decisions about the long-run consequences from difficult decisions.

Conclusion

The widespread failure of quantitative risk management during the financial crisis should not be the death knell for quantitative risk-management models. Value-at-risk, sensitivity analyses, risk maps, scenario planning, and risk appetite radar charts are important components within a firm's risk-management practices. The models, however, should not be the sole—and rarely the most important—basis for decision-making. They cannot replace management judgment. They are best used to trigger in-depth, analytical, and rigorous discussions among managers and employees about the different types of risks faced by the firm, and about the dilemmas (financial and moral) involved in responding to them. Used in this way, firms avoid the artificial choice between quantitative and qualitative risk management, allowing both to play important roles in surfacing and assessing risks, and then to make decisions and allocate resources to mitigate the risks in a cost-efficient and moral manner.

Robert Kaplan is Senior Fellow and Marvin Bower Professor of Leadership Development, Emeritus at the Harvard Business School.

Anette Mikes is Professor of Accounting and Control at the University of Lausanne (HEC).

[43] Badaracco (2003)

References

Badaracco, J. L., Jr. (1997) Defining Moments: When Managers Must Choose between Right and Right. Boston: Harvard Business School Press, 1997.

Brunsson (1982). The Irrationality of Action and Action Rationality: Decisions, Ideologies and Organizational Actions. *Journal of Management Studies*, Vol. 19, No. 1. 29-44.

EY (2012) *Turning Risk Into Results – How Leading Companies Use Risk Management to Fuel Better Performance*.

Edmondson, A. Roberto, M.A., Bohmer, M.J., Ferlins, E.M. and Feldman, L.R. (2005). The Recovery Window: Organizational Learning Following Ambiguous Threats. In: Starbuck, W.H. and Farjoun, M. (eds.) Organization at the Limit: Lessons from the Columbia Disaster. Blackwell. 220-246.

Hall M., Mikes A. & Millo Y. (2015). How Do Risk Managers Become Influential? A Field Study of Toolmaking in Two Financial Institutions. *Management Accounting Research*, 26, 3-22.

Hammond, J. S., Keeney, R.L. and Raiffa, H. (2006). The hidden traps in decision making. *Harvard Business Review* 84 (1): 118–126.

Hirschman, A.O. (1967) *Development Projects Observed*, 1967. The Brookings Institution.

Kahneman, D. (2011). *Thinking Fast and Slow*. Farrar, Straus and Giroux.

Kahneman, D., Lovallo, D. and Sibony, O. (2011). Before you make that big decision... *Harvard Business Review* 89 (6): 50–60.

KPMG. (2013). Expectations of Risk Management Outpacing Capabilities – It's Time For Action, May 2013.

Mikes, A. Risk management and calculative cultures (2009). *Management Accounting Research* 20 (1): 18–40.

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society* 36 (4-5): 226–245.

Mikes, A. (2008). Chief risk officers at crunch time: Compliance champions or business partners? *Journal of Risk Management in Financial Institutions* 2 (1): 7–25.

Mikes, A. and Kaplan, R. S. (2015). When One Size Doesn't Fit All: Evolving Directions in the Research and Practice of Enterprise Risk Management. *Journal of Applied Corporate Finance*. Vol. 27, No. 1. Winter. 37-41.

Mikes, A, P. Tufano, Werker, E.D., and De Neve, J-E. (2009). *The world food programme during the global food crisis (A).* HBS No. 9-809-024. Boston, MA: Harvard Business School Publishing.

Mikes, A. and Migdal, A. (2014). *Learning from the* Kursk *Submarine Rescue Failure*. Harvard Business School Working Paper.

Mikes, A. (forthcoming). The Triumph of the Humble CRO. In: Power, M.K. (ed.) *Riskwork.* Oxford.

Nocera, J. (2009). *Risk Management*. New York Times, Jan 2, 2009.

Taleb, N.N. (2007). *The Black Swan*, Penguin Allen Lane.

RIMS and Advisen Ltd. (2013). *RIMS Enterprise Risk Management (ERM) Survey*, August 2013.

Simons, R. "Stress-Test Your Strategy: The 7 Questions to Ask." *Harvard Business Review* 88, no. 11 (November 2010) Reprint R1011G: 1-9.

Simons, R., Rosenberg, K. and Kindred, N. (2009). *Merck: Managing Vioxx (A).* Harvard Business School Case.

Staw, B. M. (1981). The Escalation of Commitment to a Course of Action. Academy of Management Review. Vol. 6, No. 4. 577-587.

Stulz, R. (2008). Risk Management Failures: What Are They and When Do They Happen? *Journal of Applied Corporate Finance*. Vol. 20, No. 4. Fall 2008. 39-49.

Stulz, R. (2015). Risk-Taking and Risk Management by Banks. *Journal of Applied Corporate Finance*. Vol. 27, No. 1. Winter 2015. 8-19.

PWC. (2015). *Risk in Review – Decoding Uncertainty, Delivering Value*. April 2015.

Quail, R. (2012). Defining Your Taste for Risk. *Corporate Risk Canada.* Spring 2012. 24-30.

Roberto, Michael A., Richard M.J. Bohmer, and Amy C. Edmondson (2006). "Facing Ambiguous Threats." Harvard Business Review 84, no. 11 (November).

Thompson, J.D. 1967. *Organizations in Action.* Transaction Publishers: New Brunswick (USA) and London (UK)

Turner, B.A. (1976). The Organisational and Interorganisational Development of Disasters. *Administrative Science Quarterly*, Vol.21, 378-397.

Turner, B.A. (1978) Man-Made Disasters. Wykeham Science Press, London.

Pidgeon, N. and O'Leary, M. (2000) Man-Made Disasters: Why Technology and Organisations (Sometimes) Fail. Safety Science, Vol. 34, 15-30.

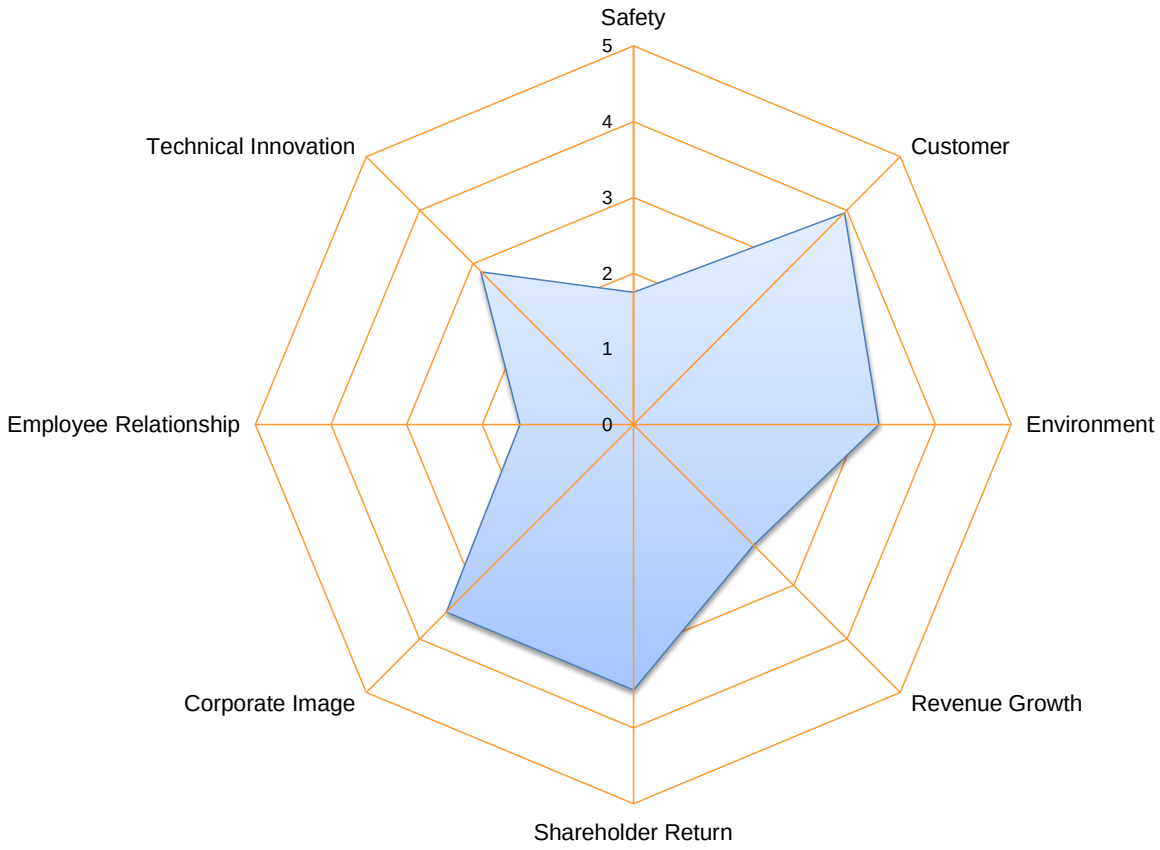
Vaughan, D. (1996) The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. Chicago.

Vaughan, D. (1999) The Dark Side of Organizations: Mistake, Misconduct and Disasters. *Annual Review of Sociology*, Vol. 25, 271-305.

Watkins, M.D. and M. H. Bazerman (2003). Predictable Surprises: The Disasters You Should Have Seen Coming. *Harvard Business Review* March;81(3):72-80, 140.

Weick, K. (1998) Foresights of Failure: An Appreciation of Barry Turner. Journal of Contingencies and Crisis Management. Vol. 6, No. 2. 72-75.

Figure 1: Target Risk Appetite



Source: Quail R. "Defining Your Taste for Risk." *Corporate Risk Canada*. Spring 2012: 24-30.

1

Risk Appetite Scale

Rating	Philosophy	Tolerance for Uncertainty	Choice	Trade-off
	Overall risk-taking philosophy	**Willingness to accept uncertain outcomes or period-to-period variation**	**When faced with multiple options, willingness to select an option that puts objectives at risk**	**Willingness to trade off 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 impact	Willing under right 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 possiblity/extent of failure	With extreme reluctance
1 **Averse**	"Sacred" Avoidance of risk is a core objective	Extremely low	Will select the lower risk option, alwars	Never

Source: Quail R. "Defining Your Taste for Risk." *Corporate Risk Canada*. Spring 2012: 24-30.