By Michael Power

Smart and Dumb Questions to Ask About Risk Management

There has been an avalanche of post-crisis reflections on risk management and its presumed deficiencies. And the wind in many countries is blowing firmly in one direction—namely, a need for better risk *oversight* and risk governance. For example, the U.K. Financial Services Authority has been explicit that the crisis has its roots in a failure of governance, and expectations about the oversight role of independent directors are increasing as a result.

There has been a great deal of wise commentary on the nature and meaning of "risk oversight," but it is worth restating the obvious. Despite a lack of clarity about the meaning of the term and related metaphors about "lines of defence," there is an expectation that directors, analysts, investors, regulators, auditors, and many others must be more challenging in the way they interrogate risk management and must hold management to account for its performance. Indeed, whereas risk management practice and its exponents were centre stage in the recent past, now it is the users, overseers, and governors of risk management who are in the spotlight.

Yet, despite the increased salience of risk oversight in every major jurisdiction, there is surprisingly little helpful guidance for an emerging population of overseers. Of course, there is no end of guidance and prescription per se. There has in fact been an explosion of risk management principles and codes of many different, but overlapping, kinds in the post-crisis period, and many existing codes have been revised. However, much of this material does not provide very practical help—being formulated more as conceptual frameworks and collections of generalities for the already-knowing practitioner, not as an aid for the oversight agent who may be less expert in risk management.

Good risk oversight requires overseers to exercise challenge by asking good questions about risk management. I suggest that the present mass of guidance does not help them to do this. Indeed, it leads to what I call "dumb" questions about risk management, questions that do not allow overseers to get at the realities of practice.

WHAT IS A DUMB QUESTION?

A dumb question is one that essentially lacks traction, and is relatively easy for a CEO or CRO to answer and deflect without revealing much of substance. Dumb questions allow executives to say something about due process, compliance, and the formal structure of risk management, but they don't allow overseers to grasp the living process. For many external parties seeking to exercise oversight, such as institutional investors, dumb questions waste their limited time. Dumb questions simply invite busy executives to rehearse risk management clichés.

So what are dumb questions more precisely?

An example of a dumb question could be "Do you have an embedded risk management system?" or "Do you have a strong risk culture?" There is nothing wrong with such questions themselves—their dumbness is not immediately evident, because they seem to feed naturally off the available guidance and current discourse. But dumb questions are much less likely to lead to an intelligent conversation. In structure, they lead back to a yes/no response rather than opening up the topic. Because dumb questions adopt the language and categories of existing abstract principles, they are also more likely to default into discussions about compliance, structure, and documents. Questioners may learn a lot about how risk management is structured and organized, but little about risk and how the business thinks about and deals with it.

SMART QUESTIONS

Smart questions are much more specific and focused than dumb questions and do not draw directly on existing principles of risk management. The specificity is not a weakness—on the contrary, it can be a most revealing point of entry for an outsider. Smart questions are also tailored to the role of the person being asked. In the case of a CEO, analysts might be tempted to ask a question like "Do you have a risk appetite policy that is well understood by every member of the organization?" Unless the questioner is very lucky, this is a dumb question. Smarter questions to ask the CEO might be:

- What are the processes by which you satisfy yourself that risk appetite is a real constraint on action?
- Is the organization good at stopping bad projects that have gained momentum?
- When was the last time something was stopped in the organization because it was considered too risky?
- How do you feel about meetings with the chief risk officer? Do you feel you talk to your chief risk officer enough?
- What are the three most important bits of management information that you use each day? What do they tell you, if anything, about risk?

Turning to the chief risk officer, it is also tempting to ask whether he or she has a fully operational enterprise risk management system or is planning to implement one, as many surveys of practice seem to do. Dumb questions. Smarter questions to ask a CRO might be:

- Have you ever been excluded from meetings that you felt you ought to attend? What did you do about it?
- Do you feel you have enough contact with the CEO?
- Can you envisage being able to veto developments? Did you ever try, and why?
- Are you involved in product development from the beginning? If not, why not?

As these examples suggest, smart questions will tend to be concrete and will elicit specific examples. They are hard to answer, but are also likely to lead to interesting discussions and reflections. Very specific questions will most likely yield specific answers, but these specific answers often tell a bigger story about how risk culture really is the "tune in the middle" rather than the "tone at the top."[1] Dumb questions lend themselves to impersonal surveys and tick box approaches, but they are also rather safe. Smart questions are uncomfortable and challenging, and may create tension for both the asker and the recipient—a productive tension, as good oversight ought to be. The answers to banks of dumb questions are more likely to be self-reinforcing and reveal little about the real risk management. They will tend to produce an illusion of control. Yet the manner in which even a single smart question gets answered will be highly informative about how risk management really works. Better still, smart questions are time efficient and enable those charged with oversight to learn whether executives are prepared to be open about how they manage risk. Dumb questions don't discriminate between executives who are candid and those who are not.

Outside parties who might exercise risk oversight have different time and cost constraints that are ignored by existing risk management guidance. As in all things, the "ideal" is the enemy of the "good enough." Dumb questions are often organized in suites that mirror existing frameworks and principles, and they are unfriendly to overseers for this very reason. In contrast, because smart questions open up a conversation about risk management, overseers can ask fewer questions—so smart questions are especially suited to those who are most pressed for time. Smart guidance for risk oversight should be designed with the five-minute overseer in mind and should provide the three questions that should be asked in order to exercise the best possible oversight given the constraint. Smart questions will vary, of course, from company to company and industry to industry, but one could imagine clusters of such questions as a resource for hard-pressed overseers such as non-executive directors. There needs to be a range of question types for agents with different time constraints.

More Smart Questions

Instead of a question such as "Describe the three lines of defence in your organization," why not ask the CRO, "How do you and your team avoid being dragged into doing the work of the business?" or "How do you manage the overlap between your team and the internal auditor?"

BEING SMART ABOUT RISK APPETITE

One area where it is particularly difficult—but important—to generate smart questions is risk appetite. One of the most conspicuous outcomes of post–financial crisis reflection has been the regulatory imperative that boards need to do a much better job of defining and enforcing their risk appetite. Boards of financial organizations are on notice that the risk appetite

policy design and implementation process will be subject to much greater scrutiny than ever before.

Yet for all this pressure, risk appetite is also a slippery idea with multiple "currencies" (capital, target credit ratings, acceptable loss, ethical boundaries) and attitudes to transgression. Many visual representations of risk management suggest an aspiration for a highly integrated pyramid or similar structure in which there is oversight from above and escalation from below. The aspirations embedded in such cubes, pyramids, and circles are the visual equivalent of looking for a single number for risk appetite. These representations embody an unrealistic, machine-like control model of organizations that is insensitive to the organizational realities of trade-offs.[2] They generate dumb questions, such as "What is the organizational risk appetite?" rather than asking how different values and appetites are mediated (e.g., growth versus control).

Dumb questions typically confuse aspiration with reality. The reality is that organizations are permeated by many different risk appetites, not all of which are commensurable and talk to each other. We don't like this idea because it violates enterprise risk management ideals of integration, but its realism is the basis for smart questions. So, rather than asking the CEO or CRO whether there is a risk appetite policy that is fully agreed on by the board, smart questions—in addition to those suggested above—might be:

- Which part of your organization is least sensitive to risk appetite policy and why? Where do you feel least in control of your organization?
- What are the key areas where you think the appetite for risk changed in the year? How did you find out and what did you do about it?
- Tell me why your risk appetite document is not just a piece of fiction.
- How do you incentivize for quality at point-of-sale/-service delivery?

There is no mystery about smart questions. Once one gets the point, it is easy to develop them. Robert Simons at Harvard has pointed to such questions in his famous risk scorecard.[3] The real mystery is that so many countries have developed a public narrative of risk management that inhibits and crowds out this kind of intelligent risk oversight, providing overseers with a battery of banal questions whose answers leave one no wiser.

CONCLUSION

To be completely fair, there are examples of efforts to develop smarter questions and aides-memoire. The Institute of Internal Auditors has developed guides in the form of 10 questions that directors should ask about various areas, such as internal audit and information technology. Furthermore, quite a bit of commentary and debate in recent years has been as much diagnostic as prescriptive, so it cannot be blamed for being unhelpful as guidance when it is not intended to be. But even taking this into account, there is nevertheless a deficit of useful guidance for time-constrained agents charged with risk oversight. Large guidance documents and statements of principles may create an aura of legitimacy around risk management practice, but in their design they contribute to a rational image of things being in control and controllable. As such, they don't provide support to those who need to figure out if the risk management in any specific organization is any good.

Finally, at the risk of being cast as a heretic, I suggest that the major driver of dumb questions is the widely accepted principles-based approach to risk management. Principles are, of course, very attractive to company executives and regulators for their flexibility in catering to different circumstances. They also help to make managers of risk look good and in control. But for risk oversight purposes, they are the wrong place to start. The drafters of such principles and guidance were no doubt so concerned with developing a coherent and consistent architecture for risk management that they forgot the needs of time-poor independent executives, analysts, and investors who are now feeling the heat. At a time when the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and related frameworks are under review, and are likely to be revised, it would be nice to think that their successors will provide a much better platform for smarter oversight. We shall see.

Michael Power*
Professor of Accounting and Director of the Centre for Analysis of Risk and Regulation at the London School of Economics

Michael Power *was educated at St. Edmund Hall, Oxford, and at Girton College, Cambridge. He is a fellow of the Institute of Chartered Accountants in England and Wales (ICAEW) and an associate member of the U.K. Chartered Institute of Taxation. He has held visiting fellowships at the Institute for Advanced Study, Berlin, and at All Souls College, Oxford. In 2009 he was awarded an Honorary Doctorate in Economics by the University of St. Gallen, Switzerland. His research and teaching focus on regulation, accounting, auditing, internal control, and risk management. He has authored The Audit Society: Rituals of Verification (Oxford, 1999); The Risk Management of Everything (Demos, 2004); and Organized Uncertainty: Designing a World of Risk Management (Oxford, 2007). Michael is also the Non-Executive Director of St. James's Place plc in the United Kingdom.*

1 See Tony Blunden and John Thirlwell, *Mastering Operational Risk* (London: Pearson Education Limited, 2010), 18.

2 Christopher Hood, "Where Extremes Meet: Sprat Versus Shark." In Christopher Hood and David K.C. Jones, eds., *Accident and Design: Contemporary Debates on Risk Management* (London: UCL, 1995), 208–27.

3 Robert Simons, "How Risky Is Your Company?" *Harvard Business Review* 77 (May–June 1999), 85–94.

** The opinions expressed in this article are solely those of the author.*