Never before has effective board oversight of corporate risk been more vital—yet boards remain stymied by company risk management programs that are poorly managed, complex and dispersed. Many companies need practical governance structures which can help the board monitor how well risk is being managed.

Over the past decade, corporate governance seems to be the story of boards of directors struggling to play catch-up. There almost seems to be a pattern. Something bad happens. Questions about board-level oversight come from all directions. Lawsuits are commenced. The SEC issues new regulations. Boards of directors are left struggling to fulfill new expectations.

The corporate battle against fraudulent financial reporting provides an illustration. The problem was a dramatic upsurge in reports of accounting fraud and earnings restatements. Criticisms of boards came from everywhere. Sarbanes-Oxley and new SEC regulations followed, and boards and their audit committees in particular found themselves trying to measure up against new responsibilities.

Now, the pattern seems ready to repeat itself. This time the issue is not accounting fraud. It is risk management. We are slowly and painfully emerging from the worst of the credit crisis. Criticisms of board-level attentiveness to the management of risk abound. Yet again, boards face heightened expectations of performance, while wondering how to fulfill them.

This is not an easy time to be a director. The discipline of risk management promises to pose all sorts of new challenges. Exactly what risks are we talking about? What should be the role of the board? What is the role of the CEO? Should there be a Chief Risk Officer? How should all of the corporate apparatus interact?

Coming up with the questions is much easier than coming up with the answers. At root, the challenge of risk management creates knotty issues of corporate governance, board oversight, independence, and assuring the needed expertise. Unfortunately, events have leapt forward in a way that does not give boards a great deal of time to find answers.

Board-level risk management is not the same as risk reduction. Not all risks will warrant meaningful oversight at the board level.

What is board-level risk management? A critical distinction here is that risk management is not a synonym for risk reduction. The starting point, rather, is recognition that risk management at the board level should accomplish three things.

The first of these is the identification of those areas of risk warranting board-level attention. The second is building capability so that acceptable levels of risk can be determined. The third is establishing a corporate governance mechanism that allows ongoing exposure to the risk to be managed. The overriding goal is risk management—not risk elimination.

None of this is easy, particularly since not all risks will warrant meaningful oversight at the level of the board of directors. At the same time, some risks can be debilitating and demand serious board-level attention. Which risks are ones the board would want to keep an eye on? That will largely depend on the business, but at many companies the following risks may be candidates for board-level attention:

- Credit risk—the potential loss arising from a counterparty’s failure to meet its obligations to the company when due.
- Liquidity risk—the consequences of the company’s inability to meet its own financial obligations to others when due.
- Accounting risk—failure of the financial reporting system to fairly capture and report the company’s financial results and position.

Michael R. Young is an attorney with the firm of Willkie Farr & Gallagher LLP. [www.willkie.com]
Market risk—the potential loss arising from adverse fluctuations in interest rates, foreign exchange rates, equity and commodity prices, or other aspects of financial markets.

Legal and compliance risk—failure to comply with legal or regulatory requirements.

Operational risk—the adverse consequences of inadequate or failed internal processes, people, or systems.

The breakdown into these areas of risk may at first seem a little random, but they share two characteristics. The first is the obvious emphasis on finance and the flow of money into, through, and out of the company. Credit risk addresses the company’s ability to collect money. Liquidity risk, the company’s ability to pay money. Accounting risk looks at the company’s ability to fairly report its financial performance and position. Market risk addresses threats to the financial position from adverse market shifts. The second characteristic is that each involves risks that, ineffectively managed, could bring down the company.

The CEO and the Chief Risk Officer. The key question now becomes: Exactly who within the organization is the best point person for effective management of all of these risks? Who will see to it that the quest for profitability is not out of sync with appropriate risk parameters?

As with every other aspect of corporate endeavor, the point person for acceptable risk will normally be the CEO. Some have questioned whether that should be the case. Perhaps the risk manager should be someone higher or lower, either on the board or in management. However, the more common view seems to be that, at its core, risk management is the balancing of risk and reward to maximize profitability. That is the essence of what being a CEO is all about.

Any sensible CEO will want to delegate as much as he or she reasonably can. This means that risk management in the first instance will almost always take place within the individual business units. For example, it would be counterproductive for a sales representative to sell lots of product to a customer who cannot pay the bills.

Yet there can be danger in over-reliance on business units for risk management. One is the perfectly natural inclination we all share to optimism. At the business-unit level, this can translate into disproportionate faith in the trustworthiness and financial strength of counterparties.

One danger is that separate business units will function as “silos,” and that corporate-wide concentrations of risk might grow undetected.

That inclination to optimism can become even more pronounced when the business unit’s success is measured by performance targets that emphasize shorter-term objectives (such as revenue) rather than problems that may take longer to surface. Significant parts of the corporate machinery, therefore, can bias the business unit against complete objectivity in evaluating risk.

Another problem can arise from excessive reliance on individual business units. It is possible that the separate business units will function as “silos” and that corporate-wide concentrations of risk might grow undetected.

One business unit might extend credit within a particular industry and think that the level of credit risk is acceptable. However, unbeknownst to the manager of that business unit, a separate unit may be extending significant credit within the same industry, or maybe a third. Each business unit may be approaching effective risk management in a completely sensible way. On an enterprise-wide basis, though, the company has inadvertently taken on a concentration of risk that is beyond its risk appetite.

Hence there is a trend in larger companies toward the installation of an enterprise-wide Chief Risk Officer (CRO). One of the main objectives of the Chief Risk Officer can be to seek information on risk across business units. The CRO can look for otherwise undetected concentrations of risk tucked away at various parts of the company (residential mortgage risk is a timely example), make informed judgments about competing risk objectives, and highlight risk concerns, encouraging enterprise-wide...
Increasingly, the CROs within companies are being supported by an enterprise-risk management capability known, naturally enough, as “enterprise risk management” or ERM. The theory is that ERM reaches into the critical aspects of corporate risk and does two things. One, it helps the business units understand the risks and take them into account, perhaps with more objectivity than if the business units were simply left to themselves. Two, ERM enables the collection of data for objective, and theoretically more disinterested, evaluation by the Chief Risk Officer.

That is not to say that ERM is purely a data-collecting and evaluation operation. Effective risk management can also involve the pre-establishment of bright-line constraints, and ERM can play a key role in putting such constraints in place. ERM may also play a role in determining when exceptions to pre-established constraints should be allowed.

Still, the entire risk apparatus will be, in a sense, a bureaucracy with a built-in bias toward conservatism. The risk professionals may get no particular reward if things go well. If things go badly, however, they will hear about it fast. The resulting temptation for ERM personnel, therefore, may not strike the optimum balance between risk and reward.

Often, it makes sense for acceptable parameters to be determined through discussion with the business leaders rather than through ERM dictates. If either side is left unsatisfied, they may turn to the CEO for additional input or, if that fails, to the board of directors. An important benefit is that the most difficult risk decisions can get escalated to the most senior levels.

It is at this point that one of the trickiest aspects of risk management comes to the fore. How should the board structure itself to optimize its oversight of risk? Should the entire board assume full responsibility for risk management? Should responsibility go to a particular committee, such as the audit committee? Should there be a special “risk committee” of the board? Or should some other corporate mechanism be put in place?

Right now, the thinking is all over the place. Some argue for the full board; some for the audit commit-
At the board level, risk management “best practices” have yet to be written. The problem involves shaping a workable system.

☐ Oversight by the board. This uncertainty on the best structure of board oversight of risk is understandable. The problem involves shaping a workable system of oversight that builds in sufficient accountability, expertise and manageability, while still covering the full spectrum of risks warranting board attention. That system requires sophistication that allows the board to understand the weaknesses and vulnerabilities of the system even when they are not volunteered by those at lower levels.

Ideally, a director would not need to do that at all. In a perfect structure, problems involving risk would naturally be identified by the various businesses. This information would then be packaged, presented to the CEO, and raised in the normal course with the board for its consideration and reaction.

Unfortunately, few corporate governance systems are flawless. Even well-meaning managers cannot always be counted upon to volunteer their own weaknesses or, for that matter, to fully appreciate what they are. Rather than candid reports by managers as to exactly what they are doing wrong, board members can often find themselves staring at PowerPoint presentations assuring them that “Everything Is Under Control.” Hence the need for some level of board skepticism and sophistication on risk management.

The need for board sophistication and expertise on risk cannot be taken lightly. Today, some of the most perilous risk management issues can involve the mind-numbing mathematics of modern-day risk analysis. How is this being handled at the board level today? Even outstanding boards are struggling. For some, the needs of the moment are being addressed by resort to the closest thing to a risk management committee already in place. At many companies, that means that broad areas of risk management are being turned over to the audit committee.

☐ Risk and the audit committee. How did the audit committee earn this privilege? In the aftermath of Enron, the law turned to audit committees to take on what was perceived to be the biggest risk of the moment—accounting risk. At the same time, some governance experts, sensitive to the need for risk management in non-accounting areas, defined audit committee responsibility with enough breadth that non-accounting risks were also swept in. The precise contours of these non-accounting risks, though, were not always clearly defined. Many audit committees thus found themselves with fuzzy responsibilities for risk management.

The rules of the New York Stock Exchange illustrate the fuzziness as well as anything. The rules and the accompanying commentary accept the core audit committee responsibility for oversight of financial reporting. However, they seek to expand that a bit by encouraging the committee to take on an undefined category of “major financial risk exposures.” True, the NYSE acknowledges that “the audit committee is not required to be the sole body responsible for risk assessment and management.” Nonetheless, it is to “discuss guidelines and policies to govern the process by which risk assessment and management is undertaken.” Precision in responsibility, and therefore accountability, is not apparent.

The right question is whether the audit committee is optimally situated to take on these additional risks. Many audit committee members could argue that they already have enough to do just to stay on top of the ever-increasing workload of financial reporting. Another consideration is that the expertise of a typical audit committee is directed, as a matter of law, to such things as debits, credits, and GAAP. If an audit committee has expertise in, say, the risks of international currency transactions, it will only be by coincidence.

☐ A separate risk management committee? That takes us to the idea of a committee similar to audit, but with a broader mandate—a “risk management” committee. The suggestion of such a committee on risk, as the board-level overseer of risk management, is increasingly coming into vogue.
Still, such a committee may lack the skills to cover the complete spectrum of risks needing board attention. A director with expertise in international currency transactions may not be able to ask the right questions about corporate credit risk models.

To remedy that shortcoming, some have proposed that the risk management committee hire its own risk experts. The thinking is that the committee could then field its own team on credit risk, liquidity risk, market risk, and so on. The committee, and therefore the board, could have both the expertise and the information to understand what is really going on.

Others question whether this additional bureaucracy is really the best approach. After all, the board theoretically already has a system for ready access to information and expertise—the management it has employed. That management may include a Chief Risk Officer and ERM.

If the goal is fostering a collaborative, transparent risk management system, a board risk committee with its own staff could send things in the opposite direction.

If the board is concerned that it is not getting reliable information, that is a management problem and probably best dealt with in other ways than the installation of a parallel bureaucracy. Additional problems could include the access of the board’s separate staff to risk management information. Fostering a collaborative and transparent effort to balance risks and rewards within the company should be the goal. A board committee armed with its own staff could send things in the opposite direction.

Another approach might be to deploy existing committees of the board, each with responsibility for the risk attendant to its own area. For example, a finance committee would have responsibility for credit and liquidity risk. The compensation committee would have responsibility for risks arising from pay. The audit committee would be responsible for accounting risk, and so on.

This seems logical, but it immediately encounters a different obstacle. One of the great hazards of risk management is the tendency for each group with responsibility for a particular area of risk to function in isolation from the others. The division of risk management across a spectrum of specialized committees, while perhaps maximizing the skills needed to ask the tough questions, runs the risk of recreating the “silo” effect, now at the board level. Which committee, for example, would have responsibility for the impact of compensation on commodity trading?

As another example, today everyone is preoccupied with liquidity risk. Many would point to liquidity risk as the cause of the failures of such companies as Bear Stearns and Lehman Brothers. In the aftermath, risk management is centering on a recalibration of pay to give employees greater incentive to care about the longevity of their companies. Thus, pay packages are including larger components of long-term stock.

While that may be an effective device to manage liquidity risk, however, it may exacerbate a completely different area—accounting risk. One of the lessons of the accounting scandals is that fraudulent financial reporting tends not to start with dishonesty, but with pressure for performance in order to sustain stock price. If stock ownership by employees becomes disproportionately large, that pressure could increase (particularly if employees have borrowed against their equity holdings to finance household cash flow).

Recall the pressure to sustain the stock price placed upon the subsequently-imprisoned CEO of WorldCom, who had borrowed more than $400 million collateralized by his company stock. In focusing so intently on liquidity risk, we may fall into the trap of being less attentive to other risks. Overall risk management would then suffer as a consequence.

There are other downsides to board-level decentralization of risk oversight through a “multi-committee” approach. The board of directors could become a “tower of Babel” with so many different committees that the whole thing collapses into confusion.

Another concern would be loss of accountability for risk management overall. No single committee assumes “ownership” of the risk management system. An important objective of the system should be to
create a culture of risk sensitivity, and, where necessary, to protect the independence and effectiveness of the CRO. Such a lack of accountability could dissipate the effectiveness of the entire risk capability.

So where does all this end up? Taking everything into account, those favoring a centralized “risk management committee” at many companies may have the better argument. A single, dedicated risk committee would serve as the focal point for risk management at the board level. There would be no dissipation of accountability. There would be a single spot if necessary for ultimate resolution of tough risk management issues.

Expertise and sophistication can be strengthened by having the Chief Risk Officer report directly to the risk committee as well as to the CEO. The committee would thereby gain access not only to the CRO’s views and analysis, but to the information of the entire ERM organization. CRO and ERM independence would be strengthened.

As a complement to a centralized committee on risk, separate board committees (compensation, audit, etc.) could continue to maintain responsibility for the risks falling within their respective areas. The CRO (and therefore the ERM apparatus) could report directly to these committees on their respective areas of risk.

However, we still have to address the issue of silos among the differing committees and the need for breadth of membership expertise. One approach to those problems might be to populate the risk management committee mostly with representatives of the other committees.

Thus, for example, the committee could include the chairs of the compensation committee, the audit committee, the finance committee, etc. In that way a pay decision that, say, increases accounting risk can be talked through before the final decision is made.

A downside is the cumbersomeness of such a network of committees and the need for efficient interaction so that key corporate decisions are not unduly delayed. Discipline would similarly be needed to keep the risk management committee to a manageable size. Nonetheless, such an approach might be the best way to capture the desired expertise and sophistication, while integrating information and perspectives.

Is there a one-size-fits-all approach for boards across the spectrum? Certainly not. Each board should be left to explore its own dynamics as to what may, or may not, work. Still, the SEC has already started rolling out new regulations on risk disclosure, and has established a new risk division. Lawsuits on risk management in the subprime crisis have already commenced. As has happened many times before, board-level oversight is in the crosshairs. It is time for the board to play catch-up once again.