The Need for Directors to take Charge of ERM

McKenna Long & Aldridge LLP
Attorneys at Law

FINANCIER WORLDWIDE
September 2006
BY THOMAS WARDELL

Though it has been on the horizon for several years, the topic of Enterprise Risk Management, or 'ERM', has suddenly emerged as a front and centre concern for directors. Although there really is no statutory mandate, the board's need to take responsibility for ERM is undoubtedly here to stay. Why now? The principal reasons are as follows.

Director liability, such as the contributions by directors from personal assets to the WorldCom and Enron settlements has clearly alarmed directors; the Disney case and its emphasis upon care and thoroughness on the part of directors has underscored this exposure. *Caremark* and its cousins make clear that in order to have the protection of the business judgement rule, directors must understand their company's business and its plan and have systems in place to monitor management's progress and effectiveness.

New York Stock Exchange listing standards provide that an audit committee must discuss policies and insist on guidelines for a process to assess and manage risk. This is a mushy standard, rather toothless, but embedded in the Listing Standards nonetheless.

US sentencing guidelines, revised in response to a Sarbanes requirement, have added and emphasised continuous risk assessment as an 'eighth' principle of a good compliance program. This risk management mandate focuses on violations of law.

The SEC continues to pressure public companies for expanded discussion of risk in MD&A and Risk Factors. This pressure takes two forms: first, to more carefully and thoroughly identify the real risks to the business, and secondly to explore and explain them thoroughly so that investors can understand them. So far, the SEC has principally used jawboning, employing comment letters and public statements as a way of pressuring companies to expand risk discussion.

The internal control process, mandated by Section 404 has for many companies bubbled to the surface some risks which need to be addressed, although technically speaking, the 404 process does not require risk assessment.

What is ERM?
The term itself comes from the Committee of Sponsoring Organizations, or COSO. ERM is an extension of the COSO control system framework, which was identified by the SEC as the first (and for most of the run-up to 404 compliance, the only) acceptable framework for internal control systems under Section 404. In its proposed 404 regulation, the SEC proposed to adopt the COSO framework in its entirety. In the final regulations, however, the SEC dropped the risk assessment component from the internal control framework. COSO, however, continued its work and in September 2004 released a risk management framework. And like its control framework, the COSO ERM framework is expressed as a cube (see below).

The COSO ERM framework is a good reference point, but for many boards and companies it represents far too complex a process. And there is a simpler one which nevertheless can measure up to COSO as the ultimate best practices model.

Where to begin
Directors should begin with a clear understanding of the expectation – what ERM is and what it is not. The focus for the board needs to be upon the principal or key risks faced by a company. For many companies the present state of risk management consists of a review of insurance coverage. That, of course, is not what is intended by the concept of ERM. But neither is a full-scale plunge into the jungle – entangling the board in all of those minor and everyday risks that come from operations. The directors' job is to understand and monitor their company's strategic and business plans and make decisions about

execution of those plans and the risks and opportunities entailed in them and in that process to assess and shape the company's appetite for risk.

How, then, to get there?

- Remember that the risks are the key or primary ones. Begin by asking senior management the first crudely framed question: "What are the principal uncertainties the company is facing?" Or maybe it is: "What are the five principal risks?" Or "What are all the principal risks?" And then: "What is management proposing to do about them?"
- • Assume that much of what you need is already going on within the company, although it may not have been bundled into an identifiable process or into systems that can be used to create reports. Often business plan aspects and the risks attendant in the business plan have been identified and organised, but the systems (and often IT systems) to monitor the progress of the business plan and develop early warning signals – both soft and hard controls – have not been installed or do not link efficiently or have gaps. An ERM system will pressure companies to put such things in place.
- • Don't outsource immediately and don't outsource everything. There are companies who have fully outsourced the ERM process only to discover that they have essentially bought an overlay system which does not in many ways tie into their existing operations and creates dysfunctional connections; this then requires them to reengineer the ERM system in order to accommodate their own operations. Had they begun with the premise that they were already, although perhaps inefficiently, 'managing' risk and put individual resources with consultation and some infusion of outside resources where gaps were identified, they would have developed an ERM system that was both more accurately framed to capture, manage and monitor the risks in their enterprise and to do so much less expensively.

Concepts to keep in mind

- • Using the term 'uncertainty' as opposed to 'risk' ('uncertainty' is a concept embedded in the COSO framework) is a good idea. 'Uncertainty' allows for recognising that risk management also entails seizing upside opportunity when it is presented. It also underscores the management function as opposed to the loss repair function suggested by the word 'risk'.
- • 'Alignment' is another concept to be held close – that is, alignment of systems, controls and monitoring processes with business planning and operations to the extent that those are not already present.
- • Assigning responsibility and accountability is an integral part of the design and management process. Individuals within the management structure must be responsible for particular operating and strategic risks/uncertainties and be accountable up the line for this responsibility.
- • Cut across silos. If the systems or processes under discussion or being installed do not cut across silos, the process has not gone far enough. Perhaps the single most significant difficulty encountered by most companies in designing and installing ERM is to find a way to connect the silos without interfering with operating efficiencies.
- • Look for aspects of ERM already at work in internal audit, corporate planning, strategy, compliance and the stronger operating units.
- • Inevitably, the ERM system attaches to the compliance system and should be connected to it. This will be an aspect of the monitoring/reporting system.

Measuring against the COSO model

A board can also measure its own ERM process against the COSO ERM framework. Instead of the eight elements of ERM that COSO identifies on the 'Risk' axis of the ERM cube as "internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & communication, and monitoring," cluster these as three concepts:

- • identification and assessment of uncertainties (after setting objectives – that is, the business plan);
- • response and control activities;
- • monitoring and reporting.

These can easily be understood and conceptually applied across the other dimensions of the ERM cube – from strategy through operations, reporting and compliance along one access and applied from subsidiaries up through business units and divisions to the entity – or enterprise – level along the third access.

Conclusion

Keep in mind that ultimately the goal is to have a process internally that manages the uncertainties of principal business strategies on an ongoing basis and allows meaningful summary reporting to the board so that their monitoring can be continuous. Uncertainties occur daily in business and some develop into major uncertainties. The board must have a system that reports changes regularly, thereby allowing full-blown discussion as soon as necessary. Good practice would be to insist upon some level of reporting at every board meeting and at least annually a full-dress discussion of all the uncertainties resident in the major drivers of the company's business plan. The result should be an extension of thinking to possible consequences and reactions to them, leading in turn to quicker, sounder responses and greater enterprise value.