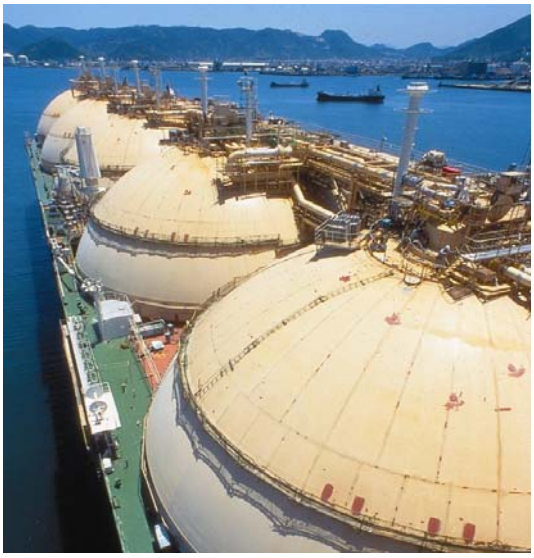
MANAGEMENT PERSPECTIVE

Implementing ERM - 1: The Importance of Perspective

David Wood
David A. Wood & Associates
Lincoln, UK

Scott Randall
Det Norske Veritas Consulting
Houston, TX



Corporate-governance requirements of the Sarbanes-Oxley Act of 2002 (SOX) have put strong pressure on oil and gas companies to implement enterprise risk-management (ERM) programs. The act requires principal executives and financial officers to certify information in periodic filings with the Securities and Exchange Commission (SEC) and dictates how managers assess internal controls and auditing standards. Facing new personal liabilities assigned by SOX, executives are turning to ERM as a way to identify and analyze risk from a company-wide perspective.

So far, the drive to establish compliance with SOX has been led by the financial, information-technology (IT), and legal-services sectors. Senior corporate managers typically embrace the effort as a means of limiting their personal liabilities and of plugging gaps in their risk-management strategies.

This powerful trend in the management of oil and gas companies raises four questions for seasoned risk managers:

- In view of the sectors leading it, is the current drive to implement an ERM framework too poorly targeted to achieve substantial improvements in corporate performance?
- Does the effort to implement an ERM framework fail to adequately emphasize the fundamental importance of, first, assessing and understanding the broad spectrum of technical and operational risks at the front line of each project and, second, progressively integrating that initial assessment into a broader corporate-wide, portfolio-focused, and strategically driven integrated risk assessments from which evolve responses to mitigate specific risks and exploit specific opportunities?
- Do the financial, IT, and legal consulting sectors possess the broad technical, operational, and management skills, experience, and industry knowledge necessary to direct the implementation of ERM in a highly technical and uncertain industry?
- Can the industry prosper if a risk-averse corporate risk-management culture is imposed upon it by well-meaning statutes and accountants without in-depth operational knowledge?

Our issue is with the implementation of ERM, not its principles. We contend that the simple answers to the above four questions are: yes, yes, no, and no. We therefore propose a more comprehensive approach to implementation of ERM.

Audit-Driven?

The misguided appeal to corporate officers of layering in a top-down, transparent, corporate-wide risk management process that can be audited or even driven by independent financial-services consultants, much as a financial audit, is that it may prevent them from being sued by disgruntled stakeholders in the event of disastrous outcomes from projects they have sanctioned. The reality is that such an approach is unlikely on its own to improve performance in terms of strategically driven, risked-value targets.

ERM must be controlled from within an organization—bottom-up and laterally as well as top-down. It must focus systematically and quantitatively, where possible, on project-specific risks and opportunities. Assessments of these risks and opportunities should be integrated with portfolio, corporate, and financial perspectives. They then should be incorporated and documented in operational decisions and options strategies, ultimately leading to specific mitigation or exploitation actions.

Part 1 of a series originally published in the March 21, 2005 edition of the **OIL & GAS JOURNAL**

"It is surprising how many oil and gas companies have yet to employ comprehensive, integrated, and systematic approaches to risk management…"

Assessment and planning of risk-management strategies require in-depth knowledge spanning technical, operational, supply-chain, geopolitics, security, fiscal, and financial issues specific to the industry. These needs are best illustrated by the nature of international upstream and midstream oil and gas projects that currently receive major capital investment. Deepwater field developments in difficult international locations, gas liquefaction and LNG receiving terminals, gas-to-liquids (GTL) facilities, and intercontinental pipelines with multiple or strategically difficult cross-border connections all require large capital investments phased over many years with long payback periods.

Financial-services, IT, and legal consultants are unlikely to be equipped collectively with the insight into such complex projects necessary to evaluate risks, advise on decisions, construct and weight comprehensive risk analysis systems, or recognize market opportunities. Such insight has to come from within experienced operating organizations pooling together multidiscipline skills, drawing on—but not driven by—specialist advice from external consultants. For these sectors of the industry, broader skill sets in operational risk have more to offer in the implementation of ERM systems than do the accounting, IT, and legal-consulting firms now attempting to dominate the field. To be successful, ERM must embrace expertise in geological and engineering attributes of properties, plant, equipment, health, safety, security, environmental, business, financial, and technology management.

Evolving Obligations

It is surprising how many oil and gas companies have yet to employ comprehensive, integrated, and systematic approaches to risk management, particularly as the industry is widely quoted as the textbook example of one operating in an environment of high uncertainty and subject to a diverse spectrum of risks and opportunities. Many oil and gas companies, upstream and downstream, acknowledge the risks but still chose to make decisions without adopting well-established, quantitative risk-analysis techniques or risk-management processes designed to optimize performance.

As companies diversify their operations internationally, the need for a structured approach to risk and opportunity analysis intensifies, as does the need for comprehensive market-entry and new-venture analysis. These requirements exist independently of the need for a risk-managed approach to corporate governance to prevent corporate mismanagement and fraud. The two should not be confused, and putting in place a mechanism to address the latter is not likely to satisfactorily address the former.

Another factor that might explain much of the industry's ambivalence to developing robust risk-management systems is the prevailing buoyancy of energy markets, underpinned by a sustained period of high oil and gas prices with financial institutions keen to lend to energy projects. In such an environment many projects and acquisitions that underperform due to the impact of unforeseen risk (such as lack of appropriate evaluation and planning) are to some extent being rescued by better-than-forecast commodity prices, which obscure the underlying problems. Companies (and their shareholders) that take this short-term view could perform better and are likely to pay a high price in the longer term for such complacency.

The 2002 SOX is organized into eleven titles, although Sections 302, 404, 401, 409, 802, and 906 are the most significant with respect to compliance. In the wake of major corporate scandals, Sections 302 and 404 have refocused US public companies on corporate governance and drawn attention to the need for ERM. Section 302 addresses personal liabilities associated with the signing of representation letters to the SEC. Section 404 requires companies to establish internal financial risk-management controls and dictates management assessment of internal controls and auditing standards. While these sections of SOX do not specifically require companies to establish systematic risk-assessment processes, they have raised awareness among corporate officers of their personal liabilities that indirectly pertain to the quality and transparency of risk-assessment systems.

SOX has increased pressure on executive and nonexecutive board members to look behind and verify information that managers provide them. Restoring trust after the mass deceptions at Enron Corp. was rightly the top priority for major businesses and legislators, and SOX represents the first step in that direction. But external rules are only the beginning; positive, visible action by corporations had to follow. Such actions need to be set by example and implemented from the top. BP PLC has been a leader in this area.[1]

Tightening of regulations by the US Securities and Exchange Commission (SEC) and similar authorities in other countries focused on the petroleum industry make clear the responsibility of a publicly traded company and its officers for oil and gas reserves and related disclosures. Some authorities have mandated the involvement of independent, qualified reserves auditors. Canada, for example, has done so with rules known as N1-51-101.

Part 1 of a series originally published in the March 21, 2005 edition of the **OIL & GAS JOURNAL**

Indeed, it was the introduction of such rules that forced Royal Dutch/Shell Group to finally admit to its erroneous historic reserves disclosures in January 2004 and subsequent reserves adjustments in January 2005. Two US pension funds filed suit in June 2004 against 27 directors and officers of Shell and their accounting and audit firms, PricewaterhouseCoopers International and KPMG International. That action followed financial losses and scandal associated with Shell's cutting its proved oil and natural gas reserves four times from January 2004 for a total downgrade of 4.47 billion boe for 2002 reserves—23% of its proved reserves as stated Dec. 31, 2002—and 500 million boe for 2003. The suit claims that future cash flows were overstated by more than $100 billion.

The reserves debacle exposed an underlying industry-wide disclosure and compliance problem in reserves booking that many companies are now being forced to address.[2] Compliance with SOX (and the SEC) means much more than the timely filing of petroleum reserves information by upstream companies. A clear system of control, responsibility, policy, procedure, culture, ERM, and reporting is preferable to ensure compliance with all of the reporting requirements of the SEC.

Enthusiasm for ERM

In response to external regulation by SOX, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) selected PricewaterhouseCoopers in January 2002 to develop a framework for ERM, which was issued in draft form in July 2003 and in final form in September 2004.[3 4]

The aims of this framework are laudable. "ERM helps an entity achieve its performance and profitability targets and prevent loss of resources," COSO says, defining ERM as "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The framework provides detailed application guidelines for managing and assessing appropriate levels of risk across an organization relative to the value it tries to create and for communicating its risk policy to stakeholders. COSO recognizes that uncertainty, "emanating from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes," underpins the need for ERM.

ERM relates to corporate governance by providing information to the board of directors on the most significant risks and how they are being managed. COSO, in order to address the lack of a unified approach, summarized its framework for ERM succinctly in the July 2003 draft in the form of a three-dimensional matrix (Fig. 1).

The framework includes:

- Eight interrelated component categories relating to the management process (rows).
- Four objectives categories (front to back columns).
- Four organization units of the corporate entity (left to right columns).

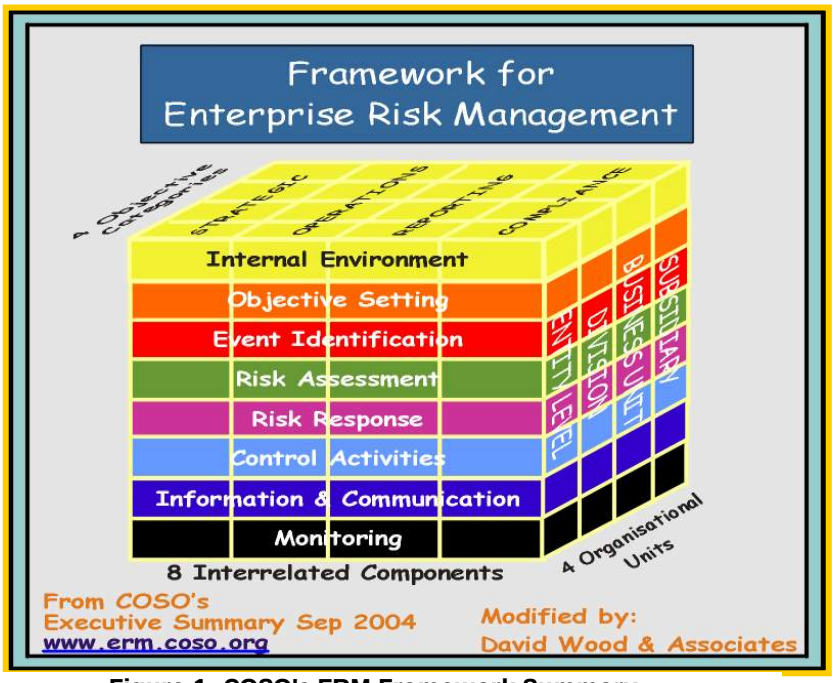


Figure 1: COSO's ERM Framework Summary

We believe that the ERM framework principles are adequately illustrated by COSO's three-dimensional matrix of components, organizational units, and functional objectives. We further believe, however, that a more effective perspective incorporates the interactions required to successfully implement ERM, as illustrated in the trapezoidal matrix in Fig. 2.

In this representation, event identification, risk assessment and risk response is conducted by asset teams and forms the operational foundation of the ERM system at the individual project level.

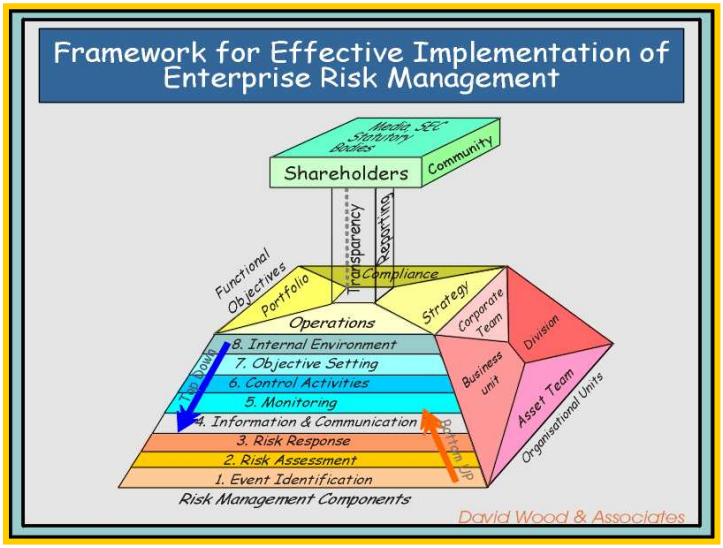


Figure 2: Trapezoidal Representation of ERM Framework for Effective Implementation

Complementing this operational foundation is the organizational superstructure of the ERM system, orchestrated at the corporate level, to establish the internal environment, objective-setting, control, and strategic portfolio management with monitoring, reporting, and compliance mechanisms implemented on an entity-wide basis by top-down directives. The foundation and superstructure of this implementation-oriented ERM framework overlap, welded together by appropriate, transparent multi-directional communication systems facilitating efficient reporting and documentation. Reporting and transparency also underpin information flow to stakeholders outside the management of the organization, such as shareholders, statutory bodies, communities, and the media—all key to effective compliance.

Performance-driven enterprises must look beyond tactical responses to SOX compliance by implementing transparent ERM systems tailored to their businesses. They should look for synergies in process, improvements in risk assessment, and response strategies by continuously calibrating historic assessments and strategies with actual outcomes. Appointing a chief risk officer, chief process improvement officer, or similar position to administer an active compliance framework based on ERM may achieve satisfactory compliance. But it is unlikely to improve risk and opportunity management.

From a cursory comparison of Figs. 1 and 2, we believe that it is clear which one was constructed with implementation, operations, and performance in mind.

Reporting and Control

The ERM framework draft focuses heavily on reporting and control issues rather than detailed assessment and implementation. To be deemed effective, COSO states that all eight components must be present and functioning. We go further and suggest that they should also be integrated with clear direction from the top down and assessment from the bottom up.

SOX and ERM are connected through use of the phrase “safeguarding of assets,” one of the three pillars of SOX Section 404 and 302. The other pillars are recording and reporting controls over financial statements.

During 2004 many corporations reacted to the requirements of SOX by frantically attempting to implement ERM systems. Corporate officers are preoccupied with what, in the absence of specific guidance from SOX or COSO, exactly lies within the scope of “safeguarding of assets” and how they might ensure that they have covered it in their evolving ERM systems. Companies are scrambling to create extensive documentation of internal controls and developing documentation and reporting systems that can cope with the expansion. However, it is clearly easier to initiate systems to document procedures for recording and statutory reporting purposes than it is to demonstrate that their systems and controls are adequately safeguarding corporate assets. As an example, Figure 3 below, illustrates various "contexts" or perspectives from which one can view Safeguarding of Assets.

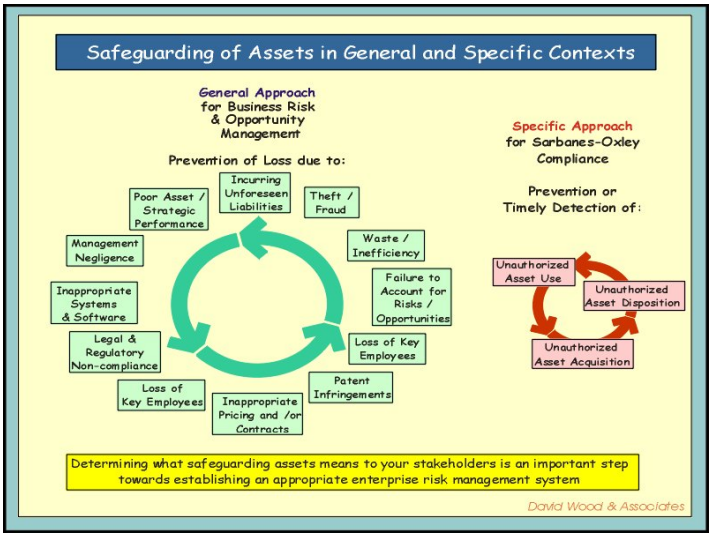


Figure 3

What "safeguarding of assets" means, does indeed depend upon your perspective. From a *statutory compliance* perspective it may simply be complying with the terms of the SOX Act and broader SEC regulations and auditing standards. From the *corporate governance* perspective the focus is broadened to consider implications and accountability to all stakeholders- internal and external to the corporation. From the *general business risk management* perspective safeguarding takes on a new meaning entirely, and must integrate the full spectrum of corporate, financial and operational issues relevant to asset management. Note that the approach taken by Det Norske Veritas, as embodied in its corporate motto, of "safeguarding life, property and the environment", is perhaps the broadest and most all encompassing of all.

In any case, it may be that defining what safeguarding means to its own organization is the most significant strategic risk decision that a board of directors can make.

Transparent Cultures

We contend that, in implementing ERM systems simply from compliance and financial-management perspectives, corporations are missing opportunities to implement comprehensive risk-management systems able to improve performance, limit liabilities, and comply with corporate-governance regulations. If compliance with SOX is viewed purely as a paper-signing certification exercise, as some companies appear to see it, the effort is unlikely to raise standards and performance or promote integrity.[5]

Compliance is expensive. When companies spend large sums to establish acceptable ERM systems, they must look beyond compliance requirements and seek systems able also to improve performance and make compliance and control worth the costs.

In order to restore their flagging public images in recent years, many of the major petroleum companies have established new performance benchmarks incorporating environmental and social-impact assessments, renewable-energy divisions, and ethics policies and have embraced long-term energy sustainability strategies.[6] However, more than 95% of their earnings continue to come from traditional oil and gas operations, and most of their exposures to risks and opportunities too. However, public concern remains high about corporate corruption, despite provisions of the Foreign Corrupt Practices Act applicable to US companies and non-US companies trading on US stock exchanges.

In the absence of a transparent, integrated ERM system, positive publicity-generating initiatives are unlikely to improve performance or public perception of that performance in the longer term. Many people see such initiatives as lip service rather than solutions to the underlying problems—and perception is reality to many investors.

"…it may be that defining what safeguarding means to its own organization is the most significant strategic risk decision that a board of directors can make."

Companies are rightly quick to display their social-responsibility credentials in efforts to impress institutional investors, which increasingly attaches merit to such credentials. Attesting to that trend is the proliferation of mutual funds and stock indexes geared to social values, such as the Dow Jones Sustainability Index. The ability of corporations to implement transparent ERM systems should carry similar weight and be driven by the business sectors where the main risks and opportunities reside.

Risk Profiles, Preferences

Corporate governance issues in the wake of SOX, the willingness of the SEC to pursue corporate officers through the US Department of Justice for wrongful disclosures, disclosure scandals, and higher international security risks have raised the risk profile for oil and gas companies from corporate liability and insurance perspectives.[7]

SOX mandates an independent audit committee with outside accountants and legal counsel. This increases the potential for conflict between corporate managers and nonexecutive directors. An ERM system too strongly influenced by conservative external financial and legal advisers can make a company unrealistically risk-averse. Turning down every deal, just like accepting deals without attempting to fully understand risks, is unlikely to be in the best interest of shareholders. Companies therefore need to take care when establishing ERM systems not to inadvertently shift their risk preferences toward overly cautious positions.

References

1. Browne, J., "BP's Browne: Transparency key to restoring trust," OGJ, Oct. 28, 2002, p. 34.

2. Demirmen, F., "Shell's reserves revision: A critical look," OGJ, Apr. 5, 2004, p. 43.

3. Tippee, B., "Corporate governance, risk management," Oil & Gas Financial Journal, Second Quarter 2004, p. 4).

4. Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management—Integrated Framework," summary available at www.erm.coso.org.

5. Fletcher, S., "Halliburton executive blasts Sarbanes-Oxley Act," OGJ, June 9, 2003, p. 26.

6. Fletcher, S., "Sarbanes-Oxley concerns dominate US corporate governance issues," OGJ, Oct. 13, 2003, p. 22.

7. Fletcher, S., "Liability insurance a growing concern for energy company directors, officers," OGJ, Oct. 13, 2003, p. 24.

The Authors

David Wood is an international energy consultant specializing in the integration of technical, economic, risk, and strategic portfolio evaluation and management. He received a BSc in geology from Leicester University (UK) and a PhD from Imperial College, London. Research and training concerning economics, portfolio, and risk analysis are key parts of his work. He is based in Lincoln, UK, but operates worldwide. His maintains a web site at www.dwasolutions.com and can be contacted by e-mail at woodda@compuserve.com.

Scott Randall is principal consultant in the enterprise risk management service area of DNV Consulting, Houston. He received a BSc in civil engineering from Michigan Technological University and an MBA in International Management from Thunderbird. He has over 20 years of experience in international market intelligence, energy risk management, strategic planning, and infrastructure project development. His e-mail address is scott.randall@dnv.com.

Part 1 of a series originally published in the March 21, 2005 edition of the **OIL & GAS JOURNAL**