FOLEY

FOLEY & LARDNER LLP

Enterprise Risk Management — Risk Intelligence and Anti-Fraud Controls

2007 NATIONAL DIRECTORS INSTITUTE

ENTERPRISE RISK MANAGEMENT — RISK INTELLIGENCE AND ANTI-FRAUD CONTROLS

In today's environment of intense scrutiny by regulators and stakeholders, investment in risk management is more important than ever. The stages of the risk assessment process include risk identification, categorization and prioritization, compliance risk assessment plans, risk ownership, implementation, and review.

Other countries, especially in the European Union, are developing stricter regulatory controls and, as a result, a far more litigation-friendly environment is emerging. Companies have to be creative in order to be able to address the constantly changing and developing risk environments in all jurisdictions in which they operate, not only to ensure compliance but also to take best advantage of growth opportunities.

At Foley's sixth annual National Directors Institute on March 8, 2007 in Chicago, Illinois, a panel entitled "Enterprise Risk Management — Risk Intelligence and Anti-Fraud Controls" was moderated by Brendan Sheehan, senior editor, *Corporate Secretary*, and featured John Gimpert, partner, Deloitte & Touche LLP; and Barry Franklin, managing principal, Aon Risk Consultants, Inc.

Overview

Regulatory compliance is generally viewed by corporations as a burden. However, the ultimate purpose of compliance is more effective management structures, and this is most likely to be achieved if compliance is considered as part of a risk management framework. There are more important reasons for getting compliance activities right than the fear of regulatory reprisals for failure. Compliance is a means to an end; not the ultimate goal.

Risk offers opportunities and downsides, and is not inherently a bad thing. Two types of risk exist — rewarded risks a company takes to achieve growth and increase profits, and unrewarded risk (e.g., the risk of noncompliance) that offers penalties rather than rewards as a possible result. Assessment of unrewarded risks is costly but necessary to enable the company to focus on rewarded risks. Risk assessment, which is known under a variety of names today, such as control rationalization, compliance sustainment, is really about the competitive positioning of the company.

Investment in risk management is more important today than ever. The trends are troubling: the costs of getting risk management wrong are increasing disproportionately; complexity and risk interdependencies of businesses are increasing; scrutiny, both by the regulators and by the stakeholders, is intense and increasing. On the other hand, the companies that manage risk smartly succeed. The conclusion is that companies need a game plan to react quickly and proactively to risk. At a minimum, they should create a list of their top five risks and put a plan in place to effectively deal with them. Enterprise risk management shows the companies how to focus energies and resources on risks of substance and significance to stakeholders and provides them with a game plan.

Risk Assessment Process

The risk assessment process consists of the following stages, as outlined in OCEG framework:

Risk Identification

- Identity and characterize key risks: this is best achieved through surveys and interviews
- Categorize risks according to functionality: operational, financial, technology, legal

Risk Prioritization

- Prioritize and score risks — frequency, severity, likelihood of occurrence
- Develop risk map detailing impacts of risks
- Establish risk ownership and assign by function or business unit. Risks can then be grouped into categories depending on magnitude (low, moderate and high)

Critical Risk Analysis

- Financial modeling of key risk issues using proprietary loss simulation models
- Evaluate risk/return of competing strategies
- Consider expected value and distribution of modeled key performance indicators. Results will assist in capital allocation decision process

Implementation

- Recommend risk mitigation strategies
- Implement and monitor mitigation activity
- Report results periodically to key stakeholders and review risk strategies to account for changes over time

Some of the critical factors that make a risk assessment plan and its implementation a success include:

- Top-of-the-house support. This endorsement is critical. Similarly, a "non-retaliation" culture is essential to foster the spirit of full disclosure
- Automation of the data management process which enables reporting and helps to sustain the process
- Integration of the risk assessment process into the day-to-day operations of the company

Financial Services Case Studies

In one case study, a large financial institution turned to Aon Risk Consultants, Inc. for enterprise risk management services. The primary goal was to identify and measure the primary risks, controls and control gaps related to compliance with global regulations.

Subsequent goals were to gain efficiency and to institutionalize the achievement of compliance.

The report produced by Aon identified 86 risks and listed the top five risks for each business unit. Everything was well-documented to ease institutionalization of compliance. A risk plan was promptly developed and successfully implemented. All goals were met.

In a second case study, a large financial institution turned to Deloitte & Touche for enterprise risk management services. The institution's challenges were unknown requirements across multiple geographies and jurisdictions, growing privacy and security requirements, inconsistent interpretations of requirements for similar processes and systems within the institution, and skyrocketing cost of managing multiple lists in silos.

Deloitte developed a risk-based common library that uses ISO (International Standards Organization) and AICPA (American Institute of Certified Public Accountants) recommended applications, has sources mapped, uses reference architectures for consistency, and produces integrated requirements. The sources of recommendations are regulatory requirements, industry standards, internal sources and common practice.

Deloitte's approach also worked well because it created a one-stop shop for requirements, de-conflicted privacy and security requirements, provided the business with full traceability, facilitated alignment between business risks and the operating environment through reference architectures, stopped the piling on of best practices without requirements, facilitated alignment between operations, engineering, operational risk and internal audit, and increased overall efficiency and cost-effectiveness of the financial institution.

Failing to Act

Companies who initiate risk assessments must be prepared to act upon the information they uncover. Having a written risk assessment report potentially leads to increased discoverability of this information and increased liability if intent or at least recklessness can be proven by the company's failure to correct the problem. At the same time, willful blindness is not a defense in court. The biggest issue in not taking steps to minimize the identified risk is that the risk would continue to fester. It is also very hard to tell at which point a company has satisfied the reasonableness requirement in connection with dealing with an identified risk, for the purposes of potential litigation. It is better to err on the side of caution in this area.

Cost

The expense of a risk evaluation, like so many other business expenses, depends upon the requested level of detail, and can run anywhere from $30,000 into the millions for large, complex corporations. When deciding whether a company can reasonably afford to conduct the evaluation, management also should consider the potential implications of not doing so.

Effects

Risk assessments need not infringe upon a company's strategic direction. A risk assessment does not directly change the company's strategies, but it can help the

company understand the risks associated with its current strategies and may suggest some changes that would minimize such risks. This may lead to a reassessment of the existing strategies and adoption of new ones. Several examples exist — including McDonald's and Merck — of companies that were able to use the findings of risk assessments or even formal investigations as a source of ideas for improvement of the company's efficiency or for new and improved strategies.

For More Information

For more information on this session or the sixth annual National Directors Institute, visit Foley.com/ndi2007 or contact the panelists directly.

Barry Franklin
Aon Risk Consultants, Inc.
barry_franklin@ars.aon.com

John Gimpert
Deloitte & Touche LLP
jgimpert@deloitte.com

Brendan Sheehan
Corporate Secretary
brendan.sheehan@thecrossbordergroup.com

2007 National Directors Institute Sponsors

Foley proudly recognizes the 2007 National Directors Institute sponsors: UBS, Aon, Korn/Ferry International, Deloitte, RR Donnelley, D. F. King, Ashton Partners, Boardroom Bound, Chicagoland Chamber of Commerce, NASDAQ, NYSE and Springboard Enterprises. The support we receive from our sponsors is crucial to the development of the program and we thank them for their efforts in once again making NDI a huge success.

Save the date! The 7th Annual National Directors Institute will be held on March 6, 2008 in Chicago. Learn more at Foley.com/ndi.