Three Lines of Defense for FCPA Compliance: Lessons from a Holistic GRC Model

In a session at Compliance Week 2011 entitled, "*Implementing a Compliance Program in a Global Business Using a Holistic GRC Model*", the speakers, John Farrell and James Littley, both of KPMG and Robert Brewer, Chief Compliance Officer of Office Depot presented a model to consider for a Foreign Corrupt Practices Act (FCPA) compliance system. Overall it was an excellent session and they presented an interesting concept for the FCPA compliance practitioner under the general rubric of "A Holistic GRC (GoveranceRiskCompliance) Model to Drive Compliance Programs Effectiveness –Three Lines of Defense."

Their thesis was that a properly constructed compliance program, in any area, such as the FCPA, Export or Customs Control, Immigration Control or any similarly regulated area has three lines of defense to prevent a compliance incident. They identified the three lines of defense as (1) the Risk Content Owners line of defense; (2) the Risk Process Owners line of defense; and (3) the Risk Content and Content Monitoring Owners line of defense.

I. Risk Content Owners

This first line of defense is the business owners who are on the front lines for any company. Their roles include management of day-to-day business risks and to recommend actions to manage and treat that risk. This group also is tasked with complying with the company's risk management process. Where appropriate, this group will implement risk management processes where applicable and this group will execute risk assessments and identify emerging risk.

The key roles/responsibilities for this first line of defense are:

• The company's Enterprise Risk Management (ERM) Steering Committee should be made up of Vice Presidents who manage risks daily in their individual departments and Business Units.

• Each ERM Heat Map risk is assigned to the Executive Committee members who are either most impacted by the risk or who have the most opportunity to influence the risk.

• The ERM Steering Committee and Executive Committee are responsible for prioritizing risks and identifying emerging risks.

• The Board of Directors is responsible for oversight of how well management is managing the risks of the company.

II. Risk Process Owners

This second line of defense is typically the company legal department and compliance department. Not only are these the standard setters in an organization but they may also be charged with certain monitoring tasks. This group should establish policy and process for risk management. This group is the strategic link for a company in terms of risk. It should provide guidance and coordination among constituencies. It should identify enterprise trends, synergies,

and opportunities for change. This group should also initiate change, integration, operationalization of new compliance best practices. Typically this group is the liaison between third line of defense and first line of defense. Lastly this group will oversee certain risk areas and in terms of certain enterprise objectives such as compliance with regulations such as FCPA, Export Control, etc.

The key roles/responsibilities for this second line of defense are:

•The ERM Manager should establish quarterly cross-functional meetings and reporting processes to drive regular discussion of risks at the Vice President and Executive levels.

•There should be a linkage of ERM to the Company's Strategic Plan.

•There should be a linkage of ERM to Annual Audit Risk Assessment, development of the Audit Plan and resource to audit teams as they perform audits.

•The ERM Manager must keep abreast of current events, audit issues, SOX compliance, legal issues, loss prevention and data security issues and upcoming legislation in order to facilitate dialog on important topics at the ERM Steering Committee and Executive Committee.

III. Risk Content and Monitoring Owners

This third and final line of defense is generally thought of as the Assurance Providers and consists of senior management, Internal Audit and up to the Board of Directors. Its roles include either working with or through senior management and/ or the company's Board of Directors. This line of defense will is tasked to rationalize and systematize risk assessment and governance reporting so that it is not only transparent but useful and stored in a manner that can be retrieved if a regulator comes calling. It will provide oversight on risk management content/ processes, followed by second line of defense. Finally it will provide assurance that risk management processes are adequate and appropriate.

The key roles/responsibilities for this third line of defense are:

•All risk focused functions report up through the Chief Compliance Officer, therefore cooperation and leveraging of information between these groups must be robust. These functions include: Internal Audit, Loss Prevention, Enterprise Risk Management and Insurable Risk Management.

•The ERM Manager should aggregate & synthesize information gathered from across the organization and reports it up to the Executive Committee and the Audit Committee or Compliance Committee of the Board of Directors quarterly.

•Internal Audit should consider ERM risks related to each area under audit and tests mitigating controls when appropriate.

This tri-parte model is an excellent way for a company to not only think through how to design an overall GRC structure but an outline to assess how well it may be doing in any one specific compliance area such as the FCPA. The first line of defense should be driven down to the Business Unit level. This will allow, indeed require, the Business Unit to buy into the overall compliance program. The legal/compliance department is the key bridge that writes and leads implementation of the overall compliance training through training but also assesses whether the compliance program is effective and remains robust. The role of senior management is to provide overall leadership and deployment of resources throughout this entire process. We recommend that you consider integrating this type of analysis into your company or using it as an assessment tool.