ACC Association of Corporate Counsel
The in-house bar association.SM 25TH ANNIVERSARY
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036-5425

Tel 202.293.4103
Fax 202.293.4701

www.acc.com

ACC's CLO THINKTANK EXECUTIVE REPORT

"ENTERPRISE RISK MANAGEMENT FOR THE INSURANCE INDUSTRY"

This Executive Report provides an overview of discussion results from ACC's CLO ThinkTank session titled "Enterprise Risk Management for the Insurance Industry" held in Washington, D.C. on May 4, 2007. ACC's CLO ThinkTank sessions are designed to provide a forum for CLOs who wish to exert greater leadership at the bar, in the courts, and in the halls of government on emerging issues of greatest concern. Following is summary information on key topics and takeaways and discussion point highlights identified by these CLO thought leaders.

ThinkTank participants included the following legal leaders:

- Tom Bogart, Executive Vice President and Chief Legal Officer, Sun Life Financial Inc.
- Bill Casazza, Executive Vice President, Chief Legal and Governance Officer, Aetna Inc.
- Pat Hatler, Executive Vice President, Chief Legal and Governance Officer, Nationwide Mutual Insurance Company
- Mick McCabe, Senior Vice President & Chief Legal Officer, Allstate Insurance Company
- Carol Ann Petren, Executive Vice President & General Counsel, CIGNA
- Dana Proulx, Vice President & General Counsel, GEICO
- Karen Schaff, Executive Vice President & General Counsel, The Principal Financial Group

KEY TOPICS

Below is a list of key topics discussed during this CLO ThinkTank session:

- **Enterprise Risk Management (ERM) –Organizational Structure**
- **Board's Role in Risk Management**
- **Electronic Communications/Information Technology Considerations**
- **Anticipating Trends/Business Practice Review Process**
- **Miscellaneous (Governance Issues, Outside Counsel Management, Compensation Committee Role, Auditor Issues, Metrics)**

KEY TAKEAWAYS

Thought leaders participating in this session described a number of ideas and practices. Listed below are some top themes and takeaways. Ideas on additional issues are described in the Discussion Highlights section below.

- **No risk management experts within the law department; all in-house lawyers provide legal support on risk management issues.** Participants described how there is no one person on point for providing legal support on risk management; risk management touches everyone's work, and all lawyers need expertise to help support these considerations.
- **Dashboard approach to mapping and assessing risks is common.** Participants discussed various practices for identifying and evaluating risks, and actions to address risks. Several participants implemented a dashboard or similar-type approach.
- **Board-specific practices for risk oversight vary, but Boards implement approaches to receive communication and provide oversight on risk issues.** Some organizations may have a Board-level Risk Review Committee, and others may handle risk review and oversight via existing committees and at the full Board level. Participants described practices for reporting risk assessments and anticipating regulatory impacts and trends to the Board.
- **Electronic communications, records retention, and information technology advances present challenges.** Participants discussed organizational structure for handling records retention and destruction policies and practices. They also discussed challenges associated with advances in technologies and new ways of doing businesses and how policies and practices can be practically implemented in light of these fast-paced changes.

DISCUSSION HIGHLIGHTS

ENTERPRISE RISK MANAGEMENT-GENERAL

Enterprise Risk Management/Organizational Structure & Practices: Participants described a range of organizational constructs for managing and overseeing risk management. One participant described having a Chief Risk Officer that reports quarterly to the Board on 4 categories of risk (credit, market, insurance and operational). One participant described practices that include bringing all risks under one 'umbrella,' and having the organization's General Auditor on point to manage/oversee risk management.

Enterprise Risk Management/ Compliance Personnel & Structure: One participant described having a centralized Ethics and Compliance Office that is not part of the law department (but the Chief Ethics and Compliance Officer is a lawyer by background and reports organizationally to the CLO), and compliance personnel embedded within business units who report organizationally to the heads of their business units. The Ethics and Compliance Office is on point for establishing facts and accountability; the Chief Ethics and Compliance Officer certifies that the company's process is being executed. The question of whether a particular practice is in compliance with law is viewed as a legal question. Participants asked whether there is concern regarding the ability to be objective if compliance personnel are embedded within the business function; the response: the organization's culture supports compliance and the legal department has a lot of clout in supporting compliance assessments. Another participant described having compliance personnel physically located with the business unit, but organizationally report to the legal department. For that participant, the concern was that reporting relationships to the finance or business unit could present concerns regarding objectivity. Another participant described having a Chief Compliance Officer who reports to the CLO.

Enterprise Risk Management/Chief Risk Officer & Business Operations Reviews: One participant described an approach that categorizes four main types of risks: credit, market, insurance, and operational. This participant's organization has a Chief Risk Officer that reports quarterly to the Board, and the company's Board conducts a risk review (focuses on actuarial finance, compliance and operational risks) that is separate from the Audit Committee's risk analysis. In addition, the company conducts Business Operations Reviews in each country that it operates within; these reviews are led by the business leader for the operations in that country, and some may take a few years to complete.

Enterprise Risk Management/General Auditor & Dashboard Reviews with Consistent Measurements: Another participant described an approach that includes a centralized system and processes to identify risks and measure them using a 'dashboard' approach—all overseen by the company's General Auditor. This company includes risks on the dashboard and uses the same measurement system to monitor and prioritize actions going forward. To help quantify risks, the company's internal audit group and compliance group meet with business units to ask for input on operations and risks and to coordinate and help prioritize action plans.

Enterprise Risk Management/Range of Risks; Process: One participant described a process that included bringing together an executive team (Chair of the Audit Committee, CEO, CFO, Internal Auditors) to identify risks and categorize them on a grid with probability and magnitude estimates. The organization identified around 25-30 risks, established ranges (rather than specifically quantifying each risk) and evaluated raw risk and net risk (taking into account a proposed mitigation device). Oversight of various risks was then assigned out to the Board Committees depending upon the nature of the risk.

Enterprise Risk Management/Compliance Office Focus on Process: One participant described having a centralized compliance office on point to deal with facts and accountability regarding compliance matters. The office evaluates processes for implementing compliance measures and provides internal certifications on whether the processes are being properly executed. Although the Chief Compliance Officer is a lawyer by training and reports organizationally to the CLO, that individual is not responsible for determining whether a course of action is legal or not. Instead, the focus is on process and execution of the process. The question of whether a course of action is compliant with laws would be determined by the lawyers. In addition to the centralized compliance office, the organizational structure includes compliance personnel embedded within the business units; these personnel report organizationally to the heads of the various business units.

Enterprise Risk Management/Embedded Compliance Personnel & Objectivity: Participants discussed whether embedded compliance personnel who report organizationally to the leaders of business units can be objective and whether there are concerns about that type of structure. A participant whose organization implements this structure noted that the organization's strong culture of compliance and the role and clout that lawyers have within the organization counter any potential risk from solid-line reporting of compliance personnel to business personnel. Additional organizational approaches described by participants relating to compliance personnel and business unit alignment and organizational reporting relationships include: (1) compliance personnel are embedded within business units and have solid line reporting relationships both to the Chief Auditor and to the head of the business units; (2) compliance personnel co-located with business units but without a formal organizational reporting relationship to the business units—instead, they report to the law department; and (3) centralized compliance office with Chief Compliance Officer reporting to the CLO and compliance personnel centralized within the compliance office but organizationally structured with designated responsibilities for defined business units.

BOARD'S ROLE IN RISK MANAGEMENT

Board's Role/ Board Risk Committee Considerations: Participants discussed issues surrounding creating a separate Board-level risk committee. One participant described having separate finance and risk committees at the Board level. One participant indicated that the organization considered creating a separate risk committee and decided against it for the following reasons: (1) the committee would create additional structure and administrative burden to staff, and (2) organization decided that assessment of risks would best be handled by specific committees already established or by the full Board depending upon the nature of the risk (e.g., full Board might consider matters relating to reputational risk commoditizing, etc..).

Board's Role/Reports to Board: One participant described a process that includes having the organization's Chief Risk Officer report to the full Board at every meeting. During the Board's annual meeting, the report is a broader report, and interim reports are more focused. This organization's Board decided not to create a separate risk committee; instead, the audit and compensation committees handle many of the risk issues.

Board's Role/Risk Review Committee: One participant described creating a Risk Review Committee at the Board level around 4 years ago. Part of the rationale for creating this committee was to help ease the load of the audit committee. The Risk Review Committee covers an impressive range of matters given the complex range of risks within the organization. The participant shares that the head of the committee and the CLO have lively discussions regarding written summaries of assessments and balancing the desire to show diligence with the level of written detail.

WRITTEN COMMUNICATIONS & INFORMATION TECHNOLOGY CONSIDERATIONS
Written Communications & IT Considerations/ Writing to Show Diligence: One participant described a 'sea change' with more being put in writing to show diligence. Putting more in writing puts additional pressure on the process of thoughtful writing. The participant noted that the organization offered training on written communications as part of its enterprise risk management program roll-out.

Written Communications & IT Considerations/Information Technology Strategies: One participant described a leading practice to help establish information technology needs to support compliance and risk management as a priority: an internal information technology process was initiated internally and priority for systems allocation was moved to the policy level. Accordingly, requests for IT-related systems and software are now made through the IT function rather than the law department. Another participant described practices that include an annual management meeting during which IT systems needs are described among the various managers. Another participant described implementing an organizational shift that moved the company's Chief Privacy Officer (who is a lawyer) into the IT function. Associated with this shift were some concerns regarding the nature of decisionmaking on matters relating to records and privacy policies: if IT owns responsibility, then some of the decisions may be more operationally driven; company culture plays a large role.

Written Communications & IT Considerations/ Messaging and Training: Participants discussed the need to help train risk personnel to that they properly describe and rate risk in written assessments.

Written Communications & IT Considerations/Email: Participants discussed whether organizational email policies allow personal use. They noted challenges in implementing and enforcing personal use email policies and in creating and implementing email retention policies.

Written Communications & IT Considerations/Email retention policies: One participant noted that its company adopted a 30-day soft delete and a 90-day hard delete policy around 7-8 years ago. The company has been able to successfully defend these policies and practices in the litigation context since these processes were not litigation-related at the time they were initially adopted. If a user receives a litigation hold notice, then it's the users responsibility to identify related records and set them aside for hold. Another participant indicated that the organization was in the midst of creating a team to evaluated email retention policies and is developing a grid of the various document and record-related requirements. Participants described training as a critical component of any email retention program, especially for complex systems that include a need to classify information as types of material or documents.

Written Communications & IT Considerations/Blogging and Instant Messaging: One participant indicated that blogging was not allowed. Another participant shared that instant messaging is not generally allowed (but a business unit can make a request for a certain population within the unit and then these documents would be treated like email). Participants discussed how text messaging is a natural way to communicate in some parts of the world and that a strict prohibition on text messaging could make conducting business difficult.

Written Communications & IT Considerations/Record Destruction: Participants discussed whether organizations have fixed periods for record destruction. They also discussed practices that include having different time frames by type of document; some noted having an elaborate grid specifying document types and destruction schedules.

Written Communications & IT Considerations/E-Discovery: Participants discussed challenges and burdens associated with e-discovery and very broad requests from plaintiffs. They discussed the value of having accountability on the bench for scope of discovery rulings, including the possibility of holding judges accountable for the utility of the discovery they authorize. Participants also discussed the disparity in burdens when it comes to producing documents for discovery: plaintiffs have little to produce and requests of defendants can be overly burdensome.

Written Communications & IT Considerations/Records Management: Participants discussed records management function and how it fits organizationally. One participant indicated the records management function resides outside of both IT and legal (within the Compliance Group). For that company, an individual who is a lawyer by training and who held a former position with the company as a compliance officer has recently been designated the new Records Manager. The role is viewed as a compliance role, and each business unit has individuals on point for records management within that business unit. Another participant described having a Records Retention/Governance Group that is comprised of leaders throughout the company, including the CFO and business leaders, and the CLO chairs the group. Another participant described implementing practices that moved accountability for records management from the law department to the Chief IT Officer. That person has a staff of individuals who perform records management functions exclusively, and there is an in-house lawyer dedicated to providing legal support to that group.

ANTICIPATING TRENDS

Anticipating Trends/Business Practice Review Process: One participant described an approach that includes involving business leaders in proactively assessing their risks; they meet every two weeks and can peer review each other.

Anticipating Trends/Business Unit Risk Committee: One participant has business unit risk committees, and conversations about anticipating trends and impacts on operations often occur among participants of these committees.

Anticipating Trends/External Reviews: One participant described two practices to help evaluate trends on the horizon and future issues to watch out for: (1) reviewing what others within your industry and outside of your industry are doing to see what types of risks they're identifying and how they're responding to help learn from proven successes; and (2) sending to lead plaintiffs counsel for review an organizational business plan or strategic plan to ask for feedback and thoughts based on what they see on the horizon and from their area of expertise. Lessons learned from this latter outside review of strategic planning resulted in some actions on the approach for disclosures and disclaimers.

Anticipating Trends/Vetting New Products: One participant described implementing practices that include vetting new products by sending them to agents to test and asking for feedback on how the products might be 'hacked' or abused.

MISCELLANEOUS ISSUES

Corporate Governance Ratings: Participants discussed how there used to be a broad disparity among corporate governance ratings and how questions on individual governance practices used to really affect ratings. They discussed how the 'tide is rising' and differences among company ratings are fewer. One participant described an idea to bring in professional experts on either side of the spectrum on issues like staggered Boards/lead director/other governance-related issues so that these experts can make their case in open forum on both sides. The challenge with this approach is that some professionals may be less objective than others and then the dialogue on these issues may be less useful.

Corporate Governance/Dedicated Board Meeting: One participant described a practice that includes the organization's Board having one meeting per year during which the Board discusses only governance-related issues and debates various topics relating to governance. That participant shared a view that the Board is so much better informed as a result of this type of visceral push-back opportunity.

Compensation Committees/Evolving Role: Participants discussed the role of their organizations' compensation committees and how they are doing much more research and acting in a very focused manner. They discussed use of consultants to help inform their dialogue and how the process is becoming even more rigorous.

Auditors & Audit Committee: Participants discussed challenges associated with larger audit firms. They also discussed how auditors are building large legal practices—hiring lawyers and consultants in-house.

Outside Counsel Fee Arrangements: Participants discussed disparity in in-house models for legal fee arrangements and traditional outside counsel billing models. They noted how accounting and consulting firms appear to be further up the curve than law firms in understanding the economics of their businesses and the price for their work and how law firms are behind. One participant suggested that the legal profession needs to examine itself and how and what gets 'billed' and that in-house law departments need to work with law firms on this if they want them to be successful.

Outside Counsel Management/Models: Participants described a number of alternative billing models to the straight hourly rate, including flat fees for large volumes of work and holding fees steady for three years and then re-assessing. Participants noted that flat fee arrangements can work for large litigation work as well as regulatory work.

Outside Counsel Management/Firm Selection: Participants discussed how high hourly rates are driving business away from some firms and towards other firms (for example, located outside of New York City, smaller-sized firms, etc..).

Outside Counsel Management/Legal Staffing Decisions: One participant noted a process change: before, if the organization had a large deal, the tendency was to go to a given law firm for legal work. Now, the law department determines the three most critical issues for the deal to be successful on the legal side and then assesses how the law department is staffed internally and whether that staffing is sufficient to successfully handle the deal. If there are areas where the law department falls short in expertise, then the law department can selectively go outside to get the expertise it needs with a better awareness of what is required and how best to get the expertise to satisfy that requirement.

Law Department Metrics: Participants discussed various types of metrics used by law departments, including: budget, regulatory product filing timelines, average cost of settlement, operating metrics (regulatory reviews, fines & penalties, number of cases), litigation reserves, ethics office contacts, and others.

ACC thanks its CLO ThinkTank sponsors for this session, Ogilvy Renault and Shearman & Sterling LLP