Risk Intelligence Roundtable:

UCLA Anderson School of Management's Director Education and Certification Program

moderated by

Carol A. Fox, ARM

On a spring day in Los Angeles, three experienced board members - from large publicly traded companies to not-for-profit entities - met to discuss what it means to "become a risk intelligent organization". The occasion was a RIMS-planned session for board directors at the UCLA Anderson School of Management's Director Education and Certification Program (see box). The interactive session was structured to help the participants create more intelligent risk conversations within the boardrooms where they serve.

Dr. Carla Hayn, Faculty Director of the UCLA Director Education and Certification Program, introduced the panelists and moderators:

Cameron Findlay, then the executive vice president and general counsel of Aon Corporation, now the senior vice president and general counsel at Medtronic, Inc.

Cesca de Luzuriaga, the chair of the OfficeMax Audit Committee with past executive experience with Mattel, Inc.,

Patty DeDominic, chair of The Jane Goodall Institute's Audit Committee, and managing partner and cofounder of DeDominic & Associates, a business consulting firm headquartered in Los Angeles

Carol Fox, former chair of RIMS ERM Development Committee and Senior Director, Risk Management for Convergys Corporation, who moderated the session

Fay Feeney, principal of Envision Strategic Group

Carol opened the session by asking the full class of attendees, from both for-profit and not-for-profit organizations, what risks they were concerned about for their firms. Risk responses from the group ranged across a broad spectrum: environmental, political, credit, vendors, health & safety, making revenue and profit targets, obtaining funding, and legal, to name just a few.

Author's Note: The attributed comments reflect the personal opinions expressed by the panelists and do not necessarily represent official positions of the organizations with which they are or were associated.

FINDLAY: It's obvious from the answers that the participants have given that - although there may be common risks for us all - a cookie cutter approach to risk does not work in organizations that are so different from one another. That, in itself, creates a challenge for boards in risk oversight.

DeDOMINIC: In my experience, while the board is involved in all risk areas, the Audit Committee generally takes a leading role. While all risks that have been listed are important, other risks that could be added might include fraud, business continuity planning, and succession planning. We know our quick-list isn't exhaustive for all risks that organizations might face. Risk oversight is still evolving.

FINDLAY: In very large companies, the board tends to take a high level view because it doesn't have time to consider all risks. Committees take on more specific risks, but within a whole range of formality. For example, a Finance Committee would focus on risks such as counterparty, capital structure, cash and mergers & acquisitions, while a Compliance Committee reviews risk control assessments for regulatory risks.

LUZURIAGA: In order to discharge its duty of care and disclosure, boards are becoming more probing. The Audit Committee generally has responsibility for determining how risk management will be communicated to the rest of the board members. In my experience, this needs to be a board level discussion. Putting an enterprise risk management process in place helps this oversight, especially when you have a big company and a smaller board.

Responding to the moderator's question to attendees about their experiences with enterprise risk management, several noted that their boards have begun the process of conducting risk assessments - with mixed results. Many found ERM to be "process rich", but with little integration in the planning processes of the organizations.

DeDOMINIC: The apparent disconnect between risk management and planning is an important gap. Risk management needs to focus on risks that matter to the board for its consideration of appropriate risk and reward. It comes back to the board's skill in balancing profit and risk against the organization's mission, yet also to exercise due diligence.

LUZURIAGA: Even so, ERM holds value. When an emerging risk event occurred, enterprise risk management gave us the framework to work within… not only did we have the assessment, we were able to disclose and be proactive in managing the risk.

FOX: In a 2008 study of more than 500 organizations published by RIMS, we found that only 4% of companies with ERM achieved a managed or leadership level in all seven of the competency attributes. Are you surprised by these results?

FINDLAY: No, the results aren't surprising. Enterprise risk management is still in its infancy.

DeDOMINIC: Experience with SOX has helped for financial controls, but senior management's skills in this area are still evolving. Talking about tough issues matters: the more diverse the board, the better the discussion.

LUZURIAGA: You need to have the board's support and engagement to mature the risk management discipline. Risks need to be reviewed periodically by the entire board.

FINDLAY: The key is to get the right information in front of the board. Management needs to explain not only what the risks are, but what is being done about them. Enterprise risk management can't be a little project done just by external consultants, with input from the risk and internal audit functions. It needs to be embraced by the CEO, the CFO and all the busi-

ness leaders. At the same time, you have to recognize the limitations. The counterparty risk with Lehman Brothers wasn't taken seriously by many organizations in early 2008. You have to think about things that could happen, regardless of how remote. Too often company management may not consider potential catastrophic consequences if risk probabilities are low, so little or no action is taken to avoid or mitigate these risks.

DeDOMINIC: It takes courage for board members to question and help an organization move forward. You need the best advisors, but board members also have to be able to rely on the expertise of senior management.

LUZURIAGA: Formal ERM programs force that conversation between the board and management around strategy, reputation, and balancing risks against rewards. Scenario planning for risks that are relevant, yet carry high uncertainty, build in adaptability and flexibility in strategic plans if events - such as the emergence of a new competitor - play out. This type of discussion allows the board members to provide their respective expertise.

FOX: Those are great observations. In order to move ERM beyond just a huge risk identification process - which we seem to have mastered - to utilization, evaluation and implementation, it can't be considered a bolt-on, or a "plug and play" exercise. As you've pointed out, it must be integrated into business planning and normal reporting. An important aspect of planning and reporting is risk appetite management. What is the board's risk appetite? Are risk tolerances set at the board level? Are these the same as management's risk appetite and tolerances?

LUZURIAGA: That discussion is too infrequent in many board rooms. Sometimes the right information may not be getting to the board. There is a fine line between micromanaging and analyzing. As a rule of thumb, if board members don't understand a risk or the positions that management is taking, it's important to "do a gut check" and get answers so that they do understand.

FINDLAY: ERM can help with that transparency. It forces explanations around management actions and decisions regarding risk positions.

LUZURIAGA: The value of ERM is not just controls and assurance – its value is in awareness and response. ERM's success is dependent on the openness of the culture and the CEO's ability to elevate and discuss the important risks. Consultants can drive a process and provide a list of risks, but they typically aren't close enough to the business to determine what needs to be done about the risks.

FINDLAY: Beyond identifying what the risks are, ERM is communicating to the right people and having the risks acted upon. Consultants don't execute; management does.

DeDOMINIC: Consultants can add value in their specialized competencies, whether that is accounting, legal, or insurance. They see a multitude of businesses and can provide a view on what other companies are doing. What they won't do is attest to whether your risk management practices are adequate.

FOX: In RIMS' 2009 Executive Report on "The 2008 Financial Crisis: A Wake-up Call for Enterprise Risk Management", RIMS found there was an overreliance on the use of financial models and controls, as well as failures in applications of risk tolerance and in embedding risk practices throughout the organizations. Even when risk managers were sounding the alarm, as in the cases of Fannie Mae and Freddie Mac, there was no governance failsafe to alert the board. Would a fully embedded ERM discipline have helped at AIG, for example?

FINDLAY: ERM would have helped foster the conversation. People now claim they were aware but stayed silent.

LUZURIAGA: Risk-taking was approved, even rewarded, by the cultures

involved in the financial meltdown. ERM as a process won't help if it doesn't contain real risk information – if it doesn't spell out the potential calamitous consequences if a risk goes wrong. Identifying a risk does no good if no action is taken to mitigate it.

FINDLAY: If the culture is more about compliance than about what it can tolerate, the question as to whether a decision is a good business decision isn't always asked in the proper context.

The above observations by the panelists fostered a lively discussion whether the failure at AIG was a failure of controls, and whether there were limits on the size of "the bets". These discussions led to how quantification-focused AIG's ERM practices appeared to be, with a heavy reliance on and belief in its financial models. Errors within the assumptions underpinning the models mattered. If management and the board do not question the financial models, anticipate the outliers and foresee the downside potential, greater risks than intended may be taken. One participant noted that the lesson from the AIG meltdown was to not only question the modeling, but to not rely entirely in the belief in quantification and models.

FOX: David Apgar wrote in his book *Risk Intelligence: Learning to Manage What We Don't Know* that "Risk intelligence refers to an individual's or an organization's ability to weigh risk effectively." Given the financial and economic crisis as a backdrop, with emerging regulatory requirements and the cost of implementing and maintaining an ERM program, what changes, if any, should be made in board oversight of enterprise risk management?

DeDOMINIC: Board members and management should educate themselves on the best risk management practices in industry and those being used by competitors. RIMS is a great source for learning about best practices. Using specialized consultants to conduct independent audits of an organization's enterprise risk management practices, including the controls for major risks, may be helpful to understanding the organization's risk management effectiveness.

LUZURIAGA: Boards need to be more probing in understanding the company's risk management processes and questioning what management actually is doing about the risks. An ERM program should be implemented - or if one exists, it should be strengthened - to help frame that conversation.

FINDLAY: The focus shouldn't be only on the risk identification process – it has to be about transparency and the actions that management is taking to make sure the rewards are balanced against the risks being taken.

FOX: According to Apgar, striking the right risk/reward balance requires a consistent and standardized way of assessing, decision-making, acting, adjusting and communicating. Building risk competencies within the organization, while setting expectations for risk-based performance, will go a long way in making any organization more risk intelligent.

The session concluded with Dr. Hayn thanking the panelists and participants for an interesting overview of what makes a risk intelligent conversation. ■

About RIMS

The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to the advancing the practice of risk management. Founded in 1950, RIMS represents more than 3,500 industrial, service, non-profit, charitable and governmental entities. The Society serves more than 10,000 risk management professionals around the world.

This white paper is published by RIMS with permission of the author and contributions from the RIMS ERM Committee.

For more articles, white papers and resources on enterprise risk management, visit the RIMS ERM Center of Excellence at www.RIMS.org.