

## Leading risk management practices

On October 22–23, 2009, members of the Audit Committee Leadership Network (ACLN) met to discuss leading risk management practices and the audit committee’s role in overseeing the link between compensation and risk.<sup>1</sup> For the discussion on risk management, members were joined by Carl Berquist, executive vice president and chief financial officer, Marriott International. This document<sup>2</sup> reflects a summary of the key points raised during the discussion, along with selected perspectives that members shared before and after the meeting. For further information about the network, see “About this document” on page 13. For a full list of participants, see Appendix 1 on page 14.

### Executive summary

Members agreed that in order to fulfill their risk oversight responsibilities, directors ought to understand and benchmark specific risk management techniques across a broad range of companies and situations. In a spirit of appreciative inquiry, ACLN members shared some of the leading enterprise risk management (ERM) practices in place in the companies on whose boards they are serving or have served. Mr. Berquist shared in-depth insights into Marriott International’s ERM program. During their discussion, members focused on the following four broad topic areas:

- **Design: organization and processes** (Page 3)

Meeting participants noted a diversity of approaches to the design of risk management processes at the organizational level. Some companies assign risk management responsibility to an individual, oftentimes the chief risk officer (CRO), while others have formed management committees to drive risk management efforts. Marriott International takes a decentralized approach to risk mitigation, with centralized monitoring techniques. Network members emphasized the importance of ensuring that organization culture supports risk management efforts.

- **Assessment: identification and prioritization** (Page 5)

Members agreed that an effective risk management program should ultimately strive to identify and assess all risks, including those that are most challenging to foresee, such as emerging risks and catastrophic risks. Mr. Berquist described Marriott International’s survey of its top-ranking executives and board members that is used to identify and assess risks, and to stimulate an ongoing dialogue about these risks amongst these business leaders. Members highlighted and discussed other effective risk identification and prioritization processes, such as scenario planning and surveying external stakeholders.

---

<sup>1</sup> See Audit Committee Leadership Network, “Compensation, risk, and the role of the audit committee,” *ViewPoints*, November 30, 2009. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_EY\\_ACLN\\_Nov09\\_View28.pdf](http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Nov09_View28.pdf).

<sup>2</sup> *ViewPoints* reflects the network’s use of a modified version of the Chatham House Rule whereby names of members and guests and their company affiliations are a matter of public record, but comments made before and during meetings are not attributed to individuals or corporations. Member quotes, from conversations held prior to the meeting as well as during the meeting, appear in italics. Mr. Berquist’s remarks are not italicized.

▪ **Mitigation and reporting** (Page 7)

Members discussed how risk mitigation efforts vary depending on the type of risk to be mitigated. Mr. Berquist provided several examples of how Marriott International mitigates risks – such as financial and credit market risk – and ensures risk mitigation processes converge to provide a system of checks and balances. Members also discussed ways to support management efforts to mitigate and report risk, and again emphasized the importance of extending corporate values and culture to newly acquired businesses in order to help new staff members understand “*what’s acceptable and what’s not.*”

▪ **Oversight of risk: key challenges and practices** (Page 10)

Members acknowledged that many companies are still in the process of determining the best approach for overseeing risk at the board level. Assigning risk oversight responsibility is a key challenge and the right approach is company-specific: while one member’s company has assigned oversight to multiple committees, another’s is in the process of determining whether to create a risk committee. Members also emphasized the importance of working with management to ensure risk reporting is effective, and to encourage a dialogue on risk. Several members agreed that the board plays a crucial role in bringing balance to risk discussions: overriding management on strategic decisions that would entail excessive risk, as well as emphasizing the importance of taking risk in order to be innovative.

Appendix 2 on page 15 includes a list of questions for audit committees to consider on risk management practices.

## Introduction

Many have characterized the current economic crisis as a failure of risk management. Recent legislative and regulatory efforts to address how boards provide oversight of risk management illustrate the level of concern.

Recent studies have also found risk management programs wanting. In a 2009 survey sponsored by Ernst & Young, the Economist Intelligence Unit found that the average Fortune 500 company spends about 4% of its revenues on risk management activities, yet 96% believe their risk management programs could be improved.<sup>3</sup> Another survey, also conducted in 2009, revealed that 85% of corporate executives believe an overhaul in risk management is required if the lessons of the economic crisis are to be used to improve business results.<sup>4</sup>

The public attention on risk management and the regulatory changes that are afoot are driving company leadership and boards – and not just those in the financial industry – to take a close look at risk management practices and consider improvements. A member said, “*A lot of [companies] are flailing on the issue of risk. It is [perhaps more] straightforward in banks – that business is risk. The rest of us have lots to focus on.*”

---

<sup>3</sup> Ernst & Young, *The future of risk: Protecting and enabling performance* (Ernst & Young Global Limited, 2009), 1. Available at [http://www.ey.com/Publication/vwLUAssets/The\\_future\\_of\\_risk/\\$FILE/The%20future%20of%20risk.pdf](http://www.ey.com/Publication/vwLUAssets/The_future_of_risk/$FILE/The%20future%20of%20risk.pdf).

<sup>4</sup> Accenture, *Managing Risk for High Performance in Extraordinary Times* (Accenture, 2009), 8. Available at [http://www.accenture.com/Global/Consulting/Finance\\_and\\_Performance\\_Mgmt/Risk\\_Management/Research\\_and\\_Insights/ManagingStudy.htm](http://www.accenture.com/Global/Consulting/Finance_and_Performance_Mgmt/Risk_Management/Research_and_Insights/ManagingStudy.htm).

## Design: organization and processes

Establishing a framework for understanding risk, assigning organizational responsibility, and adopting processes to operationalize its management are the underpinnings of an effective risk management program. When executives in the Ernst & Young survey cited earlier were asked where they plan to commit more resources to strengthen their risk management capabilities, 85% said they intended to improve the alignment of their risk management approach with their business strategy, and 72% intended to redefine risk ownership roles, processes, and structure.<sup>5</sup>

Companies take a number of approaches to assigning responsibility for risk management, including identifying a centralized risk leader, such as a CRO, creating a small senior risk team, establishing a management-level risk management committee, or alternatively, decentralizing risk responsibility to operating management. At the 2008 joint European and US Audit Committee Leadership Summit, some audit chairs advocated for a CRO, while others felt risk should be owned throughout the company, not just by those ‘tasked’ with it.<sup>6</sup> The choice of approach depends upon company specifics.

### Marriott International’s decentralized approach to ERM

- Mr. Berquist described Marriott’s ERM approach: “Our philosophy is that risk is decentralized and pushed into the business because we believe the business owns the risk. We do not have a centralized risk group. We have a cross-functional process to ensure risk mitigation techniques are in place; therefore we have centralized monitoring techniques.”
- “For example, if Marriott wants to develop a new hotel property to offer more rooms, we have controls in place throughout the business that will protect the company from risks. We have [criteria] that our hotel feasibility group ensures are met; we have operational staff approve the proposed deal and metrics that our treasury group ensures are met in order to advance the deal, and all of this must be approved with a centralized corporate growth committee. With the committees, it is an iterative process to get to the best decision. And after the property is developed, our internal audit group conducts a post-audit assessment on lessons learned, which includes information on what didn’t work and how we got through it.”
- Mr. Berquist said that Marriott’s culture provided critical support for the company’s ERM program: “Our culture is a cross-check and collaborative culture ... We often have several departments monitoring one risk, or even the same people overseeing the same risks. The idea is responsibility and accountability; how our staff is evaluated is tied to this.”

<sup>5</sup> Ernst & Young, *The future of risk: Protecting and enabling performance*, 9.

<sup>6</sup> Audit Committee Leadership Summit, “Enterprise risk: recurring challenges and new considerations for the audit committee,” *ViewPoints*, October 31, 2008, 9. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_EY\\_Summit\\_View8\\_Oct08.pdf](http://www.tapestrynetworks.com/documents/Tapestry_EY_Summit_View8_Oct08.pdf).

ACLN members emphasized the importance of ensuring that risk management efforts are aligned with company culture. One member said, *“You can never have an organization with the exact values you would like. So you set up a system of incentives and penalties that are consistent with the values you want, in the interest of the company. You guide employee behaviors to be consistent with what you want.”* Executives surveyed by Ernst & Young recognized this challenge as well: 61% intended to commit more resources to promoting a “risk culture” – a company culture that recognizes the importance of managing risk.<sup>7</sup>

ACLN members shared the following practices used by their companies to design an effective risk management program:

- Establishing functional risk teams
- Establishing a culture that effectively manages risk appetite

#### **Establishing functional risk teams**

Many companies establish risk management programs along business unit lines to allow risks deep within the company to be reported up through the business planning process. However, this may lead to gaps on an enterprise-wide level. One member’s company takes a different approach: it establishes functional risk teams for particular types of risk, including people risk, environmental risk, financial risk, and compliance risk. The functional teams then work across the business units in the risk assessment process and report upward via various specialist committees to an enterprise-wide management-level risk committee headed by the CFO. The member said, *“We assign horizontal [groups] to diagnose, monitor, and feed back [information] on these risks.”*

Compliance risk is of particular concern for this member’s company, which must interact with an increasing number of regulatory agencies and governments globally. The member said, *“We need to understand these and be responsive.”* To that end, the compliance risk team has developed a customized framework for handling compliance risk and has embedded measurement of this risk into the core processes of the business. Risks that are identified are reported up to a policy and compliance review board that is led by the head of compliance, who reports to the audit committee chair.

The member said, *“Every business spends a whole day with the compliance team, where it is all brought together.”* The policy and compliance review board then reports outcomes to the audit committee in a 90-minute session and submits a shorter report to the full board. The member said this approach provides a rigorous and effective way to understand and report compliance risk on an enterprise-wide level, and added, *“I feel good about this [approach].”*

#### **Establishing a culture that effectively manages risk appetite**

One ACLN member described the importance of an organizational culture that values restraint when it comes to assuming risk. This member was proud of the fact that his company identified the type of returns it wanted and stuck by them even when its competitors did not. In order to maintain this discipline,

---

<sup>7</sup> Ernst & Young, *The future of risk: Protecting and enabling performance*, 9.

management throughout the organization rigorously questioned the assumptions behind business decisions. The member said, “All things that fed into [our decision making] had to be tested to the  $n^{\text{th}}$  degree.”

This member stressed that the company culture’s support for this discipline at every level of the organization was ultimately driven from the top: “Our risk people have always had a lot of respect because of the tone from the top ... Our CEO goes around the world and talks to people and says, ‘You have friends at the top. Don’t be afraid; speak up.’ People need to feel they can raise their hand ... and that their opinion is respected.” He also emphasized the importance of removing any individual who penalizes staff for reporting risk issues – a practice that sends a strong message that staff can speak up.

### Assessment: identification and prioritization

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines risk assessment as “the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed.”<sup>8</sup> Identification and prioritization of risks is often one of the first areas in which companies focus their risk management efforts.

Yet the dynamic nature of risk means that even though many companies report benefiting from their efforts to identify and understand key risks (58% of the executives surveyed by Ernst & Young said their organization receives a high to very high benefit from this effort),<sup>9</sup> there is always plenty of room for improvement (84% of respondents in the Ernst & Young survey say they will invest in improving their risk assessment, aiming for a more comprehensive view of risk and an enhanced ability to anticipate risks).<sup>10</sup>

Members discussed the challenge of preparing for “black swan” events – risks defined by the National Association of Corporate Directors (NACD) as “significant threats to the enterprise ... unquantifiable and unforeseeable events often unrelated to a corporate strategy.”<sup>11</sup> One member said, “By definition, we can’t predict all risks. [So] it is better to have a solid balance sheet to deal with [unforeseen risks].”

However, others described company efforts to brainstorm possible black swans. One member described his company’s approach of preparing for more than one catastrophic risk hitting at the same time: “We ask ourselves, ‘What if not just one risk is realized, but if two or three hit at the same time?’ For example, if H1N1 hits at the same time as an earthquake in Los Angeles? We do scenarios with more than one catastrophic risk occurring at the same time.” Members also felt that noting shareholders’ views on the different risks is important; for instance, shareholders are more likely to forgive the company’s handling of catastrophic, black-swan risks such as an isolated terrorist attack.

<sup>8</sup> Institute of Internal Auditors, “Applying COSO’s Enterprise Risk Management – Integrated Framework,” PowerPoint presentation, slide 33. Available at <http://www.theiia.org/download.cfm?file=24193>.

<sup>9</sup> Ernst & Young, *The future of risk: Protecting and enabling performance*, 4.

<sup>10</sup> Ibid. 9.

<sup>11</sup> National Association of Corporate Directors, *Report of the NACD Blue Ribbon Commission, Risk Governance: Balancing Risk and Reward* (Washington, DC: National Association of Corporate Directors, 2009), page 7. Available for purchase at [https://secure.nacdonline.org/source/orders/index.cfm?section=unknown&task=3&CATEGORY=BRC&PRODUCT\\_TYPE=SALES&SKU=BRC-021&DESCRIPTION=&FindSpec=risk&CFTOKEN=25736397&continue=1&SEARCH\\_TYPE=FIN&StartRow=1&PageNum=1](https://secure.nacdonline.org/source/orders/index.cfm?section=unknown&task=3&CATEGORY=BRC&PRODUCT_TYPE=SALES&SKU=BRC-021&DESCRIPTION=&FindSpec=risk&CFTOKEN=25736397&continue=1&SEARCH_TYPE=FIN&StartRow=1&PageNum=1).

Mr. Berquist's discussion of Marriott's practice of having external sources identify relevant near-term (three-to-four-year) emerging risks caused several members to recognize a clear gap in their own processes for identifying such risks. These members indicated they planned to raise this issue with management after the discussion.

#### **A tool Marriott International uses to identify and prioritize enterprise risk**

Mr. Berquist described a proprietary online survey, administered annually to Marriott's 200 most senior executives, as well as members of the board, to identify and prioritize enterprise risks and to facilitate multiple discussions of these risks within the board and between the board and management.

Mr. Berquist, who oversees the survey, has members of the internal audit organization and a small, ad hoc committee of managers populate the survey with a list of the top risks, which survey participants will assess. The survey is administered at the end of the calendar year so that results may be analyzed and discussed both prior to and during the board's strategic offsite meeting in February. Mr. Berquist said, "The survey is populated with 15–20 risks, some of which are static risks and others that are emerging risks that are relevant to our company. We draw on external sources of information for these emerging risks, such as those discussed at the World Economic Forum in Davos. We [ask participants to rate] the possible impact the risk could have on the company and how good we are at mitigating the risk." In addition, if participants are aware of a risk that is not in the survey, they can write it in and assess it along the same dimensions.

If a risk is given a high score (meaning it would have a high impact on the organization, and the organization's effectiveness at mitigating it is low), senior management and the board discuss it further. Mr. Berquist said, "A primary goal of the survey is to have an interaction with the board [on the results]. For example, if the board ranked a risk lower, we want to talk about it ... We look at each risk, we discuss how it was ranked last year, and we include the external view on the risk ... The goal is discussion."

ACLN members also highlighted two other leading risk assessment practices:

- Scenario planning
- Surveying external stakeholders to identify and prioritize risks

#### **Scenario planning**

Companies such as Royal Dutch Shell have been using "scenarios to explore the future' for more than three decades."<sup>12</sup> One member described his company's initiation of the practice: "I found at the time that ERM was

---

<sup>12</sup> Leading View, "Perils of looking around corners," *Financial Times*, July 7, 2009. Available at <http://www.ft.com/cms/s/0/b2c8d5ce-6ad6-11de-861d-00144feabdc0.html>.

broken. We met with a company that was experimenting with scenario planning, and we brought it into the mix.” The member’s company reframed how it assessed risk by “looking at what was going on in the marketplace, or in another market that wasn’t directly applicable but [could be] three years later. For example, what if we didn’t have power? We used risks like 9/11 ... What would happen to businesses in prime locations, such as data centers?”

In order to carry out the scenario planning in a way that would inform the broader organization, this company developed teams within each business that would cascade the scenario outputs into the units. The member described the practice this way: “It was a hybrid approach: we centralized the control but the scenario planning was pushed down into the business units ... Each team would create ‘unrealistic’ scenarios [relevant to its business unit]. In the end, corporate would assemble the ten biggest scenarios that crossed all businesses. Teams would then meet once per month to review the planning. [We realized] there was enough exposure along the way to underscore the importance of this process.” For this company, scenario planning made possible a robust conversation about the key risks. The member said, “The thought process in the scenario planning raised the bar.”

### Surveying external stakeholders to identify and prioritize risks

Building on the benefit of surveying internal stakeholders like Marriott, one member’s company recently extended the process by asking key external stakeholders for their input on the company’s enterprise risks.

Working with executives in the investor relations department, the ERM group designed a series of questions to elicit the thoughts and feedback of buy-side investment analysts during one-on-one conversations. The member said, “We went out and asked our investment analysts what they thought our risks were. They said, ‘Here’s where we think you have issues,’ and we mapped it back to the risk categories we have.” The company was careful in undertaking this survey not to bias the views of the institutional investors.

Once the analysts’ views were taken into consideration, the company asked Standard & Poor’s to review its ERM program. The information gathered from these external stakeholders was reported to the audit committee and used as part of the committee’s annual deep-dive session on risk. The member said, “We learned something we didn’t expect. [The analysts] thought our biggest risk was leadership ... [They] thought we needed to do more to develop leadership.” As a result, the company has prioritized senior management succession and development. The member highlighted his role as the audit chair in driving this process: “I pushed hard to get this done ... And it was a lot more positive for the company than they thought it would be.”

### Mitigation and reporting

Risk mitigation is arguably the most difficult aspect of any risk management program. The COSO framework articulates three components of risk mitigation and reporting:

- **Risk response** – avoiding, accepting, reducing, or sharing risk and developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
- **Control activities** – policies and procedures that are established and implemented to help ensure the risk responses are effectively carried out.

- **Information and communication** – the identification and capture of relevant information in a form and time frame that enable people to carry out their responsibilities.<sup>13</sup>

Company practices for risk mitigation vary depending on the nature of the risks: while some may simply necessitate the preparation of back-up plans, others may warrant modifying operating practices or designing specific programs tailored to mitigate the risks. Risk reporting may entail separate processes designed for that task or may be embedded in business planning, decision making, and financial forecasting processes. Network members highlighted the importance of reporting both qualitative and quantitative data.

#### **Marriott International's approach to risk mitigation**

Marriott's risk mitigation approach includes acceptance, avoidance, sharing or transferring of the risk, or remediation based on risk tolerance and cost/benefit analysis. Specific mitigation activities are based on the specific risk.

For example, to address financial and credit market risk – a top priority for companies during the financial crisis – Marriott International engages in the following risk mitigation activities (among others), which are monitored by specific internal groups:

- Portfolio risk assessment and management
- Proactive monitoring of loan and guarantee exposure
- Impairment reviews
- Maintaining an adequate liquidity cushion through revolving credit facilities
- Preserving investment-grade corporate credit rating to assure preferred access to credit markets
- Identification of new, emerging capital sources to support development
- Hedging of balance sheet exposures and cash flows

ACLN members highlighted two additional risk mitigation practices:

- Use of a management tool to ensure accountability for and mitigation of risk
- Extending corporate culture to overseas staff

---

<sup>13</sup> Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework: Executive Summary* (Committee of Sponsoring Organizations of the Treadway Commission, 2004), 4. Available at [http://www.coso.org/Publications/ERM/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf).

### Use of a management tool to ensure accountability for and mitigation of risk

In order to drive the ownership of risk into the organization, one member's company has recently developed a proprietary tool consisting of *"a series of questions to trigger managers at every level of the organization to think about the enterprise risks they are responsible for."* Risks are identified for each business area and broken down into workable elements to help management think through who is responsible for each one and how to mitigate them. Describing the tool, the member said, *"It is very thorough. It is extremely well organized and user friendly (only 25–30 pages), and I've never seen an entire enterprise risk scenario written in such detail."*

Internal audit drove the development of this tool, which became a company-wide effort over a number of months. *"It was a huge effort, and the CEO went over it thoroughly,"* said this member.

### Extending corporate culture to overseas staff

For companies with international operations, the challenge of indoctrinating new overseas staff in the company culture – which includes its values, ethics, and code of conduct – is a complex challenge. ACLN members last discussed the increasing risk of violating the Foreign Corrupt Practices Act (FCPA) at the July 2009 summit, prompted in part by the vigorous prosecution of FCPA violations in recent years.<sup>14</sup>

One member provided an example, pertinent even in the initial stages of an acquisition: *"Even if [the company] has passed our due diligence reviews, including background checks on senior management, we make sure all senior management and mid-level management have extended exposure to people who understand [our company's] culture and values [so they can] understand what's acceptable and what's not."*

In addition to training employees regarding its code of conduct and compliance efforts, this company takes the additional step of ensuring new staff work alongside long-time company staff for a significant period so that new staff can observe and learn to incorporate this information operationally. The goal, this member said, is for new overseas employees to learn that *"transparency and clear, quick communication are every bit as important as putting up the sales numbers."* While the most senior staff of new operations are sent to headquarters for a period to allow enculturation to take place, staff from headquarters are also sent to the new operations to spend time working with mid-level staff to ensure expectations are clear.

The member noted that internal audit is involved from the beginning to *"make sure the process is put in place"* and continues to be involved on an ongoing basis to *"review the operations and test on a variety of levels to determine if we are doing what we should."* Internal audit must have a good working relationship with management for this practice to be effective.

---

<sup>14</sup> Audit Committee Leadership Summit, "Risk in emerging markets," *ViewPoints*, August 4, 2009. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_EY\\_Summit\\_View11\\_Jul09.pdf](http://www.tapestrynetworks.com/documents/Tapestry_EY_Summit_View11_Jul09.pdf).

## Oversight of risk: key challenges and practices

In the United States, the board's responsibility for overseeing risk management is guided by a legal and regulatory framework provided by "state courts' considerations of directors' fiduciary duties, stock exchange listing requirements, and the Sarbanes-Oxley Act."<sup>15</sup> As a result of the financial crisis, that responsibility may weigh more heavily. For example, the Securities and Exchange Commission (SEC) has proposed requiring that new disclosures on the board's role in company risk management processes be included in company proxy and information statements, as well as in the annual report. The proposed rule states:

Disclosure about the board's involvement in the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company ... For example, how does the board implement and manage its risk management function, through the board as a whole or through a committee, such as the audit committee? Such disclosure might address questions such as whether the persons who oversee risk management report directly to the board as whole, to a committee, such as the audit committee, or to one of the other standing committees of the board; and whether and how the board, or board committee, monitors risk.<sup>16</sup>

Members discussed the critical role the board and audit committee can play when it comes to overseeing major strategic decisions. For instance, one member described how a board had to decline a particular business proposal: *"The CEO presented us with something he wanted to do. It was met with dead silence, and he presented it again. We said no. It was not good for our shareholders. He came back later and said thank you."* Several members agreed with Mr. Berquist who said, "Some of the best deals we do are the ones we don't do."

However, members also noted that boards need to provide balance, which in some cases may mean pushing management to be less risk averse. One member said, *"We've had it both ways. [The board has] actually said, 'You need to take more risk.' This dilemma is actually harder than turning people down. [We worry that] management is becoming too risk averse."*

Members also reflected upon the increased importance of utilizing the external auditor's assessment of the company's risks. Members felt this should be fed into the company's risk assessment phase and used to stimulate discussion at the board level. Members noted that the board and audit committee should leverage the external auditors' objective view of risk as an important and independent addition to the company view.

---

<sup>15</sup> Lead Director Network, "The board's role in risk management," *ViewPoints*, July 24, 2009, 5. Available at [http://www.tapestrynetworks.com/documents/Tapestry\\_KS\\_LDN\\_View4\\_Jul09.pdf](http://www.tapestrynetworks.com/documents/Tapestry_KS_LDN_View4_Jul09.pdf).

<sup>16</sup> US Securities and Exchange Commission, "Proxy Disclosure and Solicitation Enhancements," proposed rule, July 10, 2009, 35. Available at <http://www.sec.gov/rules/proposed/2009/33-9052.pdf>.

### **Risk assessments drive the audit committee agenda and audit plans at Marriott International**

Mr. Berquist highlighted the importance of a regular, ongoing dialogue between management and the audit committee about key risks and what is being done to mitigate them. The risk survey is an important tool for doing so and is used to help shape the agenda for the annual board offsite meeting and the audit committee agenda for the following year. Mr. Berquist also makes sure the board weighs in on the risks associated with specific strategic opportunities: “On the big deals, we talk to the audit committee every quarter.”

Marriott’s risk assessments drive the internal and external audit plans that are overseen by the audit committee:

- For example, internal audit will ensure its plan audits risks identified in the risk assessment phase. For its part, the audit committee will follow through on the outcomes of the risk survey by selecting the important risk issues and inviting business unit managers to come talk with the audit committee about them.
- Mr. Berquist uses the external auditor’s risk assessment of the major risks when working with the audit committee to determine the external audit plan: “We provide the audit committee with a written report, we discuss it with them, and [together] we determine how the audit partner and plan will address [the risk assessment].”

ACLN members highlighted two other risk oversight practices:

- Assigning risk oversight to multiple board committees
- Shaping risk reporting from the CRO to the board

#### **Assigning risk oversight to multiple board committees**

The allocation of risk oversight responsibility across the board and its committees has been a popular topic of discussion for audit chairs in recent years. The conversation has intensified under the increased government and regulatory attention that the financial crisis has triggered. Some boards are considering the addition of a risk committee at the board level, though other directors oppose such a move. In August, for example, two Hershey directors resigned from the company’s board, citing its creation of a finance and risk committee and objecting to the duties of the full board being transferred to this committee.<sup>17</sup> At the ACLN meeting, a member said, “*We have established an ad hoc committee looking at the question of whether we should have a risk committee.*”

One ACLN member’s board assigns responsibility for risk oversight to three committees of the board, while retaining an important role for the full board: “*Risks are assigned depending on the risk.*” On this member’s

---

<sup>17</sup> “Two Hershey directors resign over new committee,” *Reuters*, August 13, 2009. Available at <http://www.reuters.com/article/managementIssues/idUSN1322053520090813>.

board, the finance committee oversees risks associated with insurance, hedging, mergers and acquisitions, and other financial risks; the compliance committee oversees legal, regulatory, and compliance issues; the full board is responsible for strategic risk; and the audit committee “has everything else.” Describing how this works in practice, the member said, “[For example,] when the audit and finance committees get together, we get a report from the director of risk management on the whole program and the array of risks, and we focus on all risks other than the strategic risks or [regulatory compliance] risks.”

The member went on to say, “I resisted the audit committee having oversight for all risks. There were other people on the board who are better suited to oversee some risks.”

### Shaping risk reporting from the CRO to the board

A recent NACD Blue Ribbon Commission on Risk Governance identified the need to “work with management to understand and agree on the types (and format) of risk information the board requires” as one of its top ten principles of effective risk oversight.<sup>18</sup> Moreover, 19.2% of board directors who participated in a survey conducted by the NACD said they disagreed with the statement that “management provides the board with the information necessary to effectively execute its risk oversight.”<sup>19</sup>

One member described being actively involved, as the audit committee chair, in working with the CRO to shape the monthly presentation the board receives. The member said, “The materials the board uses on risk are pretty complicated ... I have been pushing back and asking for more of this and less of that. It’s developing. It’s been an iterative process.”

This member also goes through each page of the monthly presentation with the CRO: “[We go through] slide by slide on each of the items in the monthly risk report [so that I can get] a slide-by-slide education.” When other members of the board learned of this meeting, “they signed up as well.”

### Conclusion

Enterprise risk management is set to be on public companies’ agendas for some time to come. As companies seek the right ERM approaches, boards too are working on defining the right degree of involvement, allocating responsibility for risk to the various board committees, and developing board processes to support their oversight responsibility. Audit committee chairs feel they benefited both from sharing risk practices in use at their companies and from the discussion that ensued. The meeting’s success highlights a clear need for more positive, leading-practice sharing in place of what has been a prolonged focus on what has gone wrong with ERM.

---

<sup>18</sup> National Association of Corporate Directors, *Report of the NACD Blue Ribbon Commission, Risk Governance: Balancing Risk and Reward* (Washington, DC: National Association of Corporate Directors, 2009), 14. Available for purchase at [https://secure.nacdonline.org/source/orders/index.cfm?section=unknown&task=3&CATEGORY=BRC&PRODUCT\\_TYPE=SALES&SKU=BRC-021&DESCRIPTION=&FindSpec=risk&CFTOKEN=25736397&continue=1&SEARCH\\_TYPE=FIND&StartRow=1&PageNum=1](https://secure.nacdonline.org/source/orders/index.cfm?section=unknown&task=3&CATEGORY=BRC&PRODUCT_TYPE=SALES&SKU=BRC-021&DESCRIPTION=&FindSpec=risk&CFTOKEN=25736397&continue=1&SEARCH_TYPE=FIND&StartRow=1&PageNum=1).

<sup>19</sup> Ibid, 37.



## About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is convened by Ernst & Young and orchestrated by Tapestry Networks to access emerging best practices and share insights into issues that dominate the new audit committee environment.

*ViewPoints* is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives *ViewPoints* may share it with those in their own network. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

*The views expressed in this document represent those of the Audit Committee Leadership Network. They do not reflect the views nor constitute the advice of network members, their companies, Ernst & Young, or Tapestry Networks. Please consult your counselors for specific advice. Ernst & Young refers to all members of the global Ernst & Young organization, including the US member firm of Ernst & Young LLP.*

*This material is copyright Ernst & Young and prepared by Tapestry Networks. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends.*



## Appendix 1: Participants

Audit Committee Leadership Network members participating in the meeting, who sit on the boards of about 25 large-, mid-, and small-cap public companies between them, included:

- Denny Beresford, Audit Committee Chair, Kimberly-Clark
- Dick Harrington, Audit Committee Chair, Xerox
- Labe Jackson, Audit Committee Chair, JPMorgan Chase
- Mike Losh, Audit Committee Chair, TRW
- George Muñoz, Audit Committee Chair, Altria and Marriott International
- Chuck Noski, Audit Committee Chair, Microsoft and Morgan Stanley
- Sandy Warner, Audit Committee Chair, General Electric Company
- Steve West, Audit Committee Chair, Cisco Systems
- Chris Williams, Audit Committee Chair, Wal-Mart

Ernst & Young partners participating in the meeting included:

- Tom Hough, Americas Vice Chair of Assurance Services
- Steve Howe, Americas Managing Partner

## Appendix 2: Questions for audit committees to consider on risk management practices

- ? How effective are the organizational and process components of your company's risk management programs?
- ? Does your leadership team support a company-wide emphasis on the importance of risk management? Is there an individual designated to lead risk management activity at your company? Why was that person selected? Do risk professionals garner the respect and attention they need? How is the risk management group supported by the organizational culture and by the audit committee?
- ? What sources of external expertise does your company rely upon for risk management? What value do they bring?
- ? How does your approach to risk identification compare with those outlined in this document? How is your list of risks generated? What screening criteria are applied? Who participates in the identification process? What sources does your company turn to for risk identification (e.g., line management, external expertise, industry benchmarks)?
- ? What methodology is used to prioritize the list of potential risks? What quantitative and qualitative factors are taken into account? Are your company's risks aggregated centrally so as to allow for a company-wide view?
- ? Do you feel your company approaches risk mitigation effectively? What tools does management use to mitigate material risks once they are identified?
- ? Is there sufficient risk expertise in your business areas to ensure that risks are properly addressed? How is this expertise developed and shared with new staff?
- ? How does the full board support the risk management activity? Have you made any changes to the role and remit of any board committees? What might you like to change?
- ? How does management report the status of the risk management effort? How frequently are these reports prepared? To whom are the reports distributed, and how are they used? How do companies ensure that risks are reported up through the organizational hierarchy without being filtered? What is the nature of the risk management discussions between the board and management?
- ? What risk oversight practices has your audit committee or full board taken on that you feel are particularly useful or innovative?