KPMG
cutting through complexity

Audit Committee Institute
kpmg.com/globalaci

Global Boardroom Insights
September 2015

Calibrating risk oversight

Global Boardroom Insights

Lindsay Maxsted – BHP Billiton (Australia)

Maggie Wilderotter – Frontier/Xerox/Proctor & Gamble (U.S.)

Artur Gabor – PKN Orlen (Poland)

Dame DeAnne Julius – Roche (Switzerland)

Marie Gemma Dequae – FERMA/Belfius (Belgium)

Mike Nolan – KPMG's Global Leader Risk Consulting

A NOTE FROM KPMG'S AUDIT COMMITTEE INSTITUTE

U.S. investor Warren Buffet has said quite simply that "risk comes from not knowing what you are doing." Of course, underlying that observation – as any board member or business leader well knows – are all the challenges, complexities, and uncertainties of running a business.

For many boards and audit committees today, helping to ensure that the company is headed in the right direction and taking appropriate risks – that the company "knows what it's doing" – is requiring deeper engagement as the business and risk environment becomes more complex and faster paced. In this edition of *Global Boardroom Insights*, seasoned directors and risk professionals from around the world share their thoughts on how boards are strengthening their oversight of risk – particularly in the context of strategy. Risk and strategy, they agreed, are two sides of the same coin.

Is the board getting the information – and the context – it needs to understand the company's key risks and add real insight and perspective? Does the company have an enterprise-wide view of its critical risks – and does it include a healthy diversity of perspectives? Are the board's risk oversight activities appropriately allocated and well-coordinated among its committees? Does the board have access to the expertise it needs – either from third parties or on the board – to assess specific areas of risk, such as cyber security? Are risk and strategy effectively linked in boardroom discussions?

As one director suggests, a good risk management and governance process "can be compared to the brakes of a car. The better the brakes, the faster the car can drive." Indeed, good brakes are essential. The challenge for many businesses and boards will be to effectively link risk management with the strategy that's driving the company forward – and to calibrate along the way.

We hope you find this edition of *Global Boardroom Insights* helpful in guiding your company forward in the months ahead.

Timothy Copnell
United Kingdom

Dennis T. Whalen
United States

Philipp Hallauer
Switzerland

Chris Hall
Australia

Wim Vandecruys
Belgium

Monika Bartoszewicz
Poland

KEY INTERVIEW INSIGHTS

Good risk management is an ongoing business discussion – dynamic and enterprise-wide. The "old idea of risk management being undertaken by a specialist function that enters your world occasionally and then moves on to someone else's world is ineffective and outdated." Managing and overseeing risk should be a dynamic process, starting with front-line management. Is the board getting a consolidated, enterprise-wide view of the company's risks from various C-level perspectives – and outside sources – that helps connect the dots? Make sure the full board and individual directors are staying apprised of the issues that different committees are dealing with – through robust committee reports, joint committee meetings, and voluntary cross-attendance.

Risk and strategy go hand in hand. While boards are clearly spending more time debating risk, "make sure it's being done in the context of making good decisions, not making no decisions." Understand the risks around key growth assumptions, and how much risk the company is willing to take. "Unless you know what your risk appetite is, there's no way to gauge whether you're taking too much risk or not enough."

Getting the risk culture right starts at the top, but succeeds (or fails) in the middle. The right tone at the top is a must; but a good risk culture – marked by "an openness and transparency…where employees are comfortable providing feedback in an open and honest discussion and different views are heard" – hinges on the middle. Is it clear that risk management "starts with the front line"? How does line management respond to issues that arise? Spending time outside of the boardroom – visiting facilities, talking to employees – is essential to effectively gauge (and reinforce) the culture.

Recognize that cyber security is a critical business risk, requiring the full board's attention. Because cyber risk cuts across so many aspects of the business – from data privacy and third-party vendors to new product development – make sure all the key players (CIO, CRO, CCO, and chief audit executive, for starters) are in sync, and that cyber has sufficient time on the full board's agenda. Tap outside expertise for an independent view of the company's vulnerabilities and defenses, and consider whether the board would benefit from having a member who is versed in information technology.

Step back and assess whether risk oversight roles and responsibilities are clear and still make sense. Challenging management on how the company is responding to a dynamic risk environment that could impact the strategy, operations, and compliance – e.g. cyber security and geopolitical risk – requires more and more time and focus. "Give a lot of thought to what gets discussed where" – particularly when it comes to the agenda-heavy audit committee. Make sure that risk oversight roles and responsibilities are clear – particularly on issues (like cyber security) that may involve more than one committee.

Lindsay Maxsted – BHP Billiton (Australia)

"The 'old' idea of risk management being undertaken by a specialist function that enters your world occasionally and then moves on to someone else's world is ineffective and outdated."

Lindsay has been a director of BHP Billiton Plc since March 2011 and is the chairman of the risk and audit committee. He is also currently chairman of Westpac Banking Corporation and of Transurban Group. Lindsay is a corporate recovery specialist who has managed a number of Australia's largest corporate insolvency and restructuring engagements and, until recently, continued to undertake consultancy work in the restructuring advisory field.

Maggie Wilderotter – Frontier/Xerox/Proctor & Gamble (U.S.)

"The right culture has an openness and transparency in terms of how the leadership works with each other and the wider organization – where employees are comfortable providing feedback in an open and honest discussion, where there are checks and balances and different views are heard."

Maggie Wilderotter was named executive chairwoman of Frontier Communications in April 2015, where she served as CEO since January 2006. She also serves on the boards of Xerox, Procter & Gamble, Juno Therapeutics, and other organizations. Mrs. Wilderotter is a member of the Board of Advisors of BoardroomIQ, Women Corporate Directors, and The Committee of 200. In 2011, she was named to the Directorship 100, and frequently appears in the FORTUNE magazine ranking of the '50 Most Powerful Women in Business.'

Artur Gabor – PKN Orlen (Poland)

"Some level of risk is inherent, and attempts to have it completely eliminated are not only futile but also wrong from a business point of view."

Artur Gabor is chairman of the audit committee of PKN ORLEN S.A., the largest capital group in Poland and Central East Europe. Following his graduation from University College London and Warsaw University, he held executive positions with Credit Lyonnais Investment Banking Group, GE Capital, and IBM Business Consulting Services. He serves on the boards of Orbis S.A. (Accor Group), Masterlease Poland, Idea Bank, and Sfinks S.A.

Dame DeAnne Julius – Roche (Switzerland)

"In discussions with the CRO, I do not want to have too much formalism – quantification is important, but my experience is that understanding the qualitative aspects is even more fundamental."

Dame DeAnne Julius currently is the chair of University College London and a non-executive director of Roche and Jones Lang LaSalle. At Roche, she is the chair of the audit committee. In her executive career she served as chief economist of British Airways and Shell and economic advisor of the World Bank's Energy Department. Dame DeAnne Julius has previously served on the boards of BP, Deloitte UK, Serco, Lloyds Bank and the Bank of England.

Marie Gemma Dequae – FERMA/Belfius (Belgium)

"Good risk management and governance can be compared to the brakes of a car. The better the brakes, the faster the car can drive."

Marie Gemma Dequae is the former president of the Federation of European Risk Management Associations (FERMA). She currently serves on the audit committee of Belfius Bank and Belfius Insurance, and the group Vinçotte. Marie Gemma was group risk manager of Bekaert Group, a global provider of advanced solutions based on metal transformation and coatings, until 2009.

Mike Nolan – KPMG's Global Leader Risk Consulting

"Good oversight of risk requires a robust management process for consolidating and articulating the company's risks in a consistent way. Without an integrated view of risk at the management level, I think the board gets put in a really difficult spot."

Mike Nolan is global leader of KPMG's Risk Consulting practice. He has more than 30 years of experience providing audit and advisory services – including internal audit, enterprise risk management, Sarbanes-Oxley, and regulatory compliance – in the energy, consumer, and industrial sectors.

Given the heavy workloads many boards and audit committees have today, is it time to take a step back and reassess risk oversight responsibilities?

LINDSAY MAXSTED:

In terms of where primary responsibility lies in a governance sense, it depends on your sector. For an industrial or mining company I think it is generally appropriate for oversight of risk and audit to be dealt with by a single committee. However, given my financial services background I wouldn't contemplate a bank combining risk and audit oversight responsibilities into one committee.

The important thing is that the board and board committees have absolute clarity as to their respective roles and responsibilities; and that, if risk and audit are combined, the risk element is allocated sufficient time at risk and audit committee meetings. The danger is that 'risk' becomes an afterthought – particularly given the heavy 'audit' workload around the financial year-end and half year. The other important overlay here is the allocation of time by the full board, as opposed to its committees, to risk – particularly emerging operational risks. Cyber security threats and the emergence of disrupters in the financial services sector are two very real examples of risks with such a possible broad impact on businesses, that the discussion ought to be, and generally is, held at the board level.

In relation to the specific issue of time allocation in combined audit and risk committees, at the start of any particular year you have to have a fairly good understanding of the agenda items for each meeting. If you are meeting quarterly, then use the 'off-quarters' for the heavily risk oriented discussions, leaving the meetings around the half year and full year end to focus more on financial reporting and audit issues. It would be odd, if not impossible, for the 'year-end' meeting to be heavily focused on the risk oversight agenda when attention should be on significant accounting issues and the financial statements.

On the more broad issue of whether the audit and risk committee is focusing on the right suite of risks, it is really a matter of understanding the business and hence being aware of material risks. Increasingly, that understanding includes an awareness of trends in the sector such that emerging material risks are dealt with as early as possible.

MAGGIE WILDEROTTER:

I would say yes. All of the public boards I'm involved with look at risk as a dynamic category, not as a static category – because risk is situational to what a company is going through at any particular period of time. And while the audit committee tends to have what I would call the deep dive responsibility on risk, the board has the overall responsibility for overseeing the company's risk mitigation strategies. To help alleviate some of the audit committee's workload, I think you're seeing more boards looking at how risk oversight responsibilities are allocated, or they're setting up specific committees – for example, an IT committee, to look at the IT side of what an audit committee would have looked at in the past.

ARTUR GABOR:

The financial crisis and the accounting scandals of the past decade made us aware of the importance of proper risk management. Together with the current volatile business environment, risk oversight is the key challenge for audit committees today. Dealing with this challenge requires going beyond regular oversight of the entity's activities.

The audit committee's role changes from simply 'reviewing and approving' a strategy to more actively participating in its creation and modification. In this respect, we realized that the risk appetite framework should be consistent with the adopted business model, and also with short- and long-term strategy and financial plans. In this respect, the audit committee works closely with the enterprise risk management department. We perform self-assessments of the risks faced and the related internal controls. The resulting risk map illustrates our current risk profile, factors in the results of our testing of internal controls and links all key risks to business processes and risk owners.

Certain elements are fundamental to effective risk oversight by boards in the current business environment. First, the board's competence – individually and collectively – must enable them to fully appreciate the risk management challenges of the company – directors need to understand the business and environment and its different dimensions, and the information presented. Secondly, effective oversight requires full agreement between the board and management on the major risks and how they should be addressed. Finally, being effective in risk oversight as a board requires diversity of perspectives and multi-optional thinking skills.

DAME DEANNE JULIUS:

Indeed, various risk dimensions are changing constantly because of globalization, technology and other external factors. For large companies like Roche with global operations and presence, this means that we live in the midst of continuous transformation in our business environment. In the pharma sector, developments in the regulatory framework are also crucial. This requires us to act, adapt and react rapidly. The Roche risk management policy focusses on managing material risks – whether they be strategic, operational or financial risks. This is vital in obtaining our business objectives. Our operating principle at Roche is that risks are managed locally – where they arise and where appropriate expertise is present to manage them. Line managers are responsible for ensuring that internal controls are effective and that appropriate action is taken to respond to the risks they face. However also – at least once a year – a 'top-down' risk identification and assessment process takes place for managing material risks at the business unit level and at group level. Based on this, an annual inventory of major group-wide risks is compiled, reviewed and discussed in the executive committee and the audit committee. Risk management plans are integral to our overall business plans and are linked to performance assessments.

MARIE GEMMA DEQUAE:

Yes. Risks are emerging and evolving constantly. In order for boards to stay successful in their oversight, the need to have a risk committee or other forum for a robust discussion is increasing. And you also actually see separate risk committees appearing more regularly – also outside the financial sector. Where a risk committee sits in the organisation depends on size, sector and the risk portfolio – on board level as a separate advisory committee, on executive level or on operational level for very specific risks – e.g. supply chain risk or cyber risk.

In general, I believe two things are critical to stay effective in risk oversight. Firstly, a robust three lines of defense framework, where the role of each line of defense is clear. Effective communication and coordination among these three lines is essential to get the right information to the board at the right time. The second (advisory) and third (audit) lines of defense have to have the authority to communicate independently from the first (operational) line to the board and its committees. Too often the information flowing to the board is only coming from the top executives.

Secondly, risk, reward, and strategy should be viewed as a dynamic process so that the company's portfolio of risks and opportunities are regularly reviewed and action can be taken by the board on a timely basis ('emergency risk governance'). For example, cyber risk is evolving so quickly, it's unrealistic to manage it effectively by reassessing your risk portfolio only once a year.

MIKE NOLAN:

I do think boards need to step back more frequently and evaluate business risks and how they approach risk oversight. Being able to challenge management on how the company is responding to signals of change that could impact the strategy, the business model, and operations in general requires more and more time and focus; so allocating and balancing risk oversight responsibilities appropriately is critical. Take 3-D printing as an example. It has huge implications for the supply chain, servicing, product quality, and working capital. What are the implications for the company's strategy and growth assumptions? Do we understand the risks involved? Risks like these may need to be allocated to one or more committees, ideally with the talent and know-how to challenge management – and then ultimately it goes back up to the full board. But boards need to step back periodically and ask whether the allocation of risk oversight responsibilities is still appropriate.

How can the board and audit committee get a better handle on their oversight of cyber risk?

LINDSAY MAXSTED:

You have to draw the material risks out. Most likely that will be through presentations from the CIO and/or external security experts to the board on what's happening in the cyber security world; the extent of the threats and where they are emanating; and what's being done to protect the organisation. On one view, cyber-crime is now so sophisticated it is no longer a question of having sufficient firewalls to prevent access. Rather it is about how companies are organized internally to ensure that, if hackers do penetrate, they are set up so that damage is minimized.

Good boards are spending a lot of time thinking about cyber and trying to understand – just as they do with every other aspect of what goes on in the organization – whether management has sufficiently robust processes and controls in place. In this sense there is a very important role for external advice and benchmarking.

We have not necessarily got to a stage where boards need people with specific cyber expertise – although it could be a bonus to have such skills – because it is a pretty narrow field. That said, we are at the stage where it is very important for most companies to have board members who are familiar with technology. Not technology necessarily in a 'technology boffin' sense, but more so the impact of technology on the business and the customer.

MAGGIE WILDEROTTER:

At Frontier, we have hundreds of thousands of denial-of-service attacks every week – so, at the board level, we're very focused on the macro picture. But the audit committee is also looking at where the vulnerabilities are and understanding at a more technical level what's being done to shore those up. There's still a big educational component – what systems we have, how we strengthen them, what kind of access-management is in place, how we're dealing with employees' personal devices, how we respond to breaches. The audit committee tends to do the deeper dive on cyber risk, but ultimately it's a full board discussion.

Another good practice – which we do at Frontier, P&G, and Xerox – is to have the CISO come in and do a full presentation for the audit committee on cyber security. What's being done not only to maintain security but to continually upgrade for detection and prevention? How is the company collaborating across its industry to benefit from what other companies have learned? At Frontier, the CISO comes in twice a year – and for all of these presentations, we invite the entire board to attend on an optional basis.

ARTUR GABOR:

Oversight of cyber security by the audit committee would benefit from having at least one individual on board having a reasonable understanding of IT and cyber security and awareness of current developments in these areas. The starting point would be to understand an entity's potential exposure: which of its assets could be exposed to cyber threats, who could pose potential threat, how the attackers could attempt to attack the systems, etc.

I believe that – except for certain industries – the issue of cyber security is currently still somewhat neglected by audit committees in Poland. We certainly all understand that cyber is a risk and how they can affect the business, but in the spate of all other board and committee duties, dealing with cyber risk maybe is not as high on the agenda as it should. Cyber risks should be a part of the company's risk management process like any other risks. It is the audit committee's responsibility to help ensure that appropriate policies and procedures have been developed and implemented.

DAME DEANNE JULIUS:

Cyber risk is one of our business sustainability risks. As with other risks, it is under continuous review internally and the audit committee is provided with periodic updates. We have learned that it is impossible to completely prevent cyber-attacks, but it is important to detect them quickly and to identify the key information within a company that needs to have extra protection and monitoring. We also work with other large companies to share information and best practice in this rapidly changing field.

MARIE GEMMA DEQUAE:

A more general knowledge of IT is certainly valuable for directors, together with a focused risk management approach related to cyber. Having a specialist in cyber or IT on the board may be one bridge too far, but proper education and training of all board members on the basics of IT and cyber risk is essential.

In companies facing significant cyber risk exposure, I think cyber risk has to be tackled in detail both at executive risk committee level and audit committee level, because it simply can't all be tackled in-depth at the board level. To effectively address cyber risk, the executive risk committee should include the CIO, as well as senior decision-makers and external experts as needed – with good dynamic reporting to the audit committee and the board on the external and internal cyber security environment.

MIKE NOLAN:

Cyber risk is clearly a priority in the C-suite today, which means it's also high on board agendas. We're seeing CIOs and CISOs getting more time on the agenda to discuss controls and risk management processes around cyber security. Many boards are engaging independent advisors to bring an outside perspective, and then marrying that against the CIO's perspective to get a fuller picture.

Because cyber cuts across so many aspects of a company, it's really important to take an enterprise-wide view and make sure there's alignment across the organization – among the CIO, CRO, CCO, and chief audit executive, for starters. Boards are also taking a harder look at their own expertise. You don't want to go searching for a new board member every time you have a new risk, but given the huge business implications of cyber security I do think it's important to have at least one board member who is versed in information technology.

How do you help ensure effective communication and coordination among the board and its standing committees regarding oversight activities around the company's key risks?

LINDSAY MAXSTED:

You have to have robust reporting processes between the committees and the board, but also you have to give a lot of thought to what gets discussed where.

Even though certain risk categories might fall within the remit of a particular committee, you might identify certain issues that are so material and integral to the business that they warrant a full board discussion. That might be achieved by an issue being reviewed and debated by the audit (and risk) committee in the first instance but then the matter proceeding as a formal paper for the whole board to debate – rather than simply as a reporting back by the committee chair. Conversely the issue might be so large and imposing that you conclude that the proper forum is not the audit (and risk) committee but the board itself. Another important point is to ensure that risks are always identified and assessed when any major decisions are taken by the board. So, risk makes its way into the board discussion in many ways.

The quality of risk information in the boardroom is getting better – driven by a regulatory push, a compliance push, a safety push, or otherwise. I think boards, board committees and senior executives are all much more conscious about the importance of properly managing risk. Overall, there is generally a much greater understanding of principal risks and in particular emerging risks. It is important to place emerging risks on the agenda ahead of a negative event. That is still one of the greatest challenges for all of us.

There is a clear benefit for the board or committees to be exposed to third-party or dissenting views. Risk and audit committees can, in part, obtain that independent view through the second and third lines of defense – whether that be through discussions with the CRO, the internal auditor or indeed the external auditor. Discussions with (say) a large accounting firm or an investment bank – not necessarily the firms retained by the company – to better understand what the market is thinking about a certain issue beyond the party line can be extremely important for directors. In my opinion, being aware of – but not necessarily beholden to – market opinion by obtaining inputs from outside the organisation, goes to the heart of being a good board member.

MAGGIE WILDEROTTER:

Cyber security is a good example. As I mentioned, the audit committee does the deep dive on cyber, but on all the boards I sit on, we give all members of the board the option to participate or sit in on that discussion. We also bring in outside experts to talk about cyber, so the entire board can hear that as well. It helps everyone stay up to speed.

Solid committee reports to the board are also important. They're more detailed than they have been in the past – particularly the audit committee's report-out on risk – and they can provide context and opportunity for a quality discussion at the full board level on specific risks.

On all the boards I sit on, we set aside time each year to do a deep dive on enterprise risk management at the board level, and several times a year at the audit committee level.

ARTUR GABOR:

We make sure that all board members have access to all the information discussed by the standing committees. Moreover, each board member is free to participate in the standing committee meetings as an observer. Also, we have introduced joint audit and strategy committee meetings which immensely help to oversee key strategic and operational risks. It is the attitude and integrity of the supervisory board that ensures adequate distribution of responsibilities and decision-making rights as well as evaluation of the decision-making process related to risk management.

High-quality risk-related information is fundamental. We managed to achieve the highest standards in Poland. We can always ask for additional and specific information – not only from the top management, but also from second or even third tier managers – independently. In addition, our board and committee meetings at subsidiary level – our company has several downstream, upstream and retail assets – substantially enhance our practical knowledge of operational risk management.

DAME DEANNE JULIUS:

The audit committee reviews the process of risk management, internal control systems, risk plans and risk assessments that have been coordinated by the internal audit team and approved by the executive committee. Roche has another board committee – the corporate governance and sustainability committee – which is responsible for overseeing social, environmental and ethical risks which we refer to as 'business sustainability risks'. A key activity is the annual discussion by the full board of the group risk report. In this discussion, every member can share his or her view of the strategic risks based on their individual expertise and experience which encompasses many geographies and industries. This year the audit committee also had a joint session with the corporate governance and sustainability committee to ensure that the full range of risks was being covered.

MARIE GEMMA DEQUAE:

Good communication between the board, its committees, and executive risk management is never easy due to the heterogeneity in the way risk managers often report. Also, board members don't always express clearly what kind of information they want to see on risk. And because open and constructive dialogue between the risk manager, the senior executives, and the board and its committees is so important – but often doesn't happen – the role of the chair of the board in leading the discussion is very important.

In my view, a good risk conversation at the board level has three dimensions: top-down – the board's and C-level's concerns about risk management have to be properly communicated downwards and fed into lower level risk assessments; bottom-up – lower-level risk insights have to be reported up to be considered in the top-level risk assessments; and enterprise-wide – in an interconnected way. It is crucial that all layers in the organization can inform the board if things are going wrong without hesitation or fear for recourse.

Another prevailing challenge is that risk managers often use complex technical language that is often not the language of the board members. Risk managers are generally very strong technically, but they don't always have the right set of soft skills to be fully effective in reporting up to the board or one of its committees. There's a real need for risk managers to step up and become strategic boardroom advisors.

For their part, board directors need to be genuinely interested in the business and eager to challenge and probe management. In this context, I am in favor of the concept of a 'contrarian director' – a director tasked solely with questioning and probing to help ensure all views are taken into account and truly informed conclusions are reached.

MIKE NOLAN:

Having a good lead director and strong governance practices for the board in terms of process and effective communication go a long way. You need the mechanisms to make sure that the right level of information is being rolled up to the board, and that the board has confidence in the committee process. But even before that, I think good oversight of risk requires a robust management process for consolidating and articulating the company's risks in a consistent way. Without an integrated view of risk at the management level, I think the board gets put in a really difficult spot. The audit committee may have a direct line to the chief compliance officer and the chief audit executive, and then the CRO and CIO and some other folks may be coming in with their views on other discrete risks. And if they're not aligned, the board is left connecting the dots, and that can be a real challenge. It's getting better, but most companies have a long way to go.

What is the nature of your board's interaction with the chief risk officer or equivalent – and how is that relationship evolving?

LINDSAY MAXSTED:

It depends on the sophistication of the organisation and where risk sits within the organisation. In my experience, regular contact is essential and I would expect, as chair of an audit and risk committee, to have a dialogue with the CRO prior to committee meetings in preparation for those meetings; and from time to time attend the CRO executive group meetings to discuss plans/ issues and meet the teams. Elsewhere I've seen CROs and risk committee chairs meet every two or three weeks or so, between formal meetings.

CROs are getting more board savvy coming from increased exposure to the board or its committees. There is now a well understood view by boards and management that risk management has to start with the front line. There can be no doubt that employees who don't understand that an awareness and management of risk is part of their job are not doing their job properly. The 'old' idea of risk management being undertaken by a specialist function that enters your world occasionally and then moves on to someone else's world is ineffective and outdated.

MAGGIE WILDEROTTER:

It's interesting – none of the companies whose boards I sit on have a chief risk officer. The CFO, CEO, CIO, and typically the head of internal audit and the chief accounting officer collectively share that role and responsibility – which gives us a great enterprise-wide view. I think it's healthier to have dispersed capability looking at risk constantly because it provides different perspectives and checks and balances on risk. When you delegate the risk role to one person – or to one board committee – I think you actually increase the chance of there being an issue. "Oh, that's the risk department's issue, not mine." Or "the risk committee has risk, so the other committees don't have to worry about it." That's why risk oversight needs to be a full board and an enterprise-wide responsibility.

ARTUR GABOR:

In my organization it is CFO – the highest level management responsible for risk – who plays the leading role in communication with the audit committee on risk. This relationship is very intense and frequent. It includes formal as well as informal working meetings.

As an audit committee we expect prompt, detailed and up to date information regarding major changes in strategic and operational risks. As to the nature of that information, I think that both looking 'farther out' onto the horizon and 'connecting more dots' can be helpful to better understand complexity of interrelated risks.

Spending time outside the boardroom is extremely rewarding. Apart from holding board meetings in the countries where we have assets, quite often the board is visiting production facilities or investment projects on site. Meeting employees, second tier management and confronting real problems helps immensely to encompass the culture of the organisation.

DAME DEANNE JULIUS:

We have clear processes to manage our risks. We have evolved our processes and structure over the past – for example, with the introduction of the Corporate Governance and Sustainability Committee to oversee non-financial risks. We believe that our current structure fits the various challenges we face, but we need remain agile and alert to external developments. It is important to allocate sufficient time to risk discussions throughout the entire organisation. This cultural aspect is essential. Risks need to be transparently addressed, discussed and mitigated. That is why proper risk management takes time. In discussions with the CRO, I do not want to have too much formalism – quantification is important but my experience is that understanding the qualitative aspects is even more fundamental.

MARIE GEMMA DEQUAE:

It is important that the board expresses exactly what they want: whether they want a dialogue, a simple formal presentation or otherwise. In financial services, the CRO is usually on the board ensuring a direct link with the executive risk management committee. In the non-financial sector it is not always easy to know what boards want to see as information from the CRO or its equivalent. In any case, it is important to know who is in charge of the major risks and how they evolve. In this context, the audit committee's role is to evaluate the risk management framework and how the systems function. Directors can't be satisfied with just a risk register update once a year because often the actual major risks impacting companies in the end are not among the top ten risks on the formal risk register.

The information related to risk up-streamed to the board is evolving due to the fact that the risks are also changing, often influenced by globalization. Take the example of the 'internet of things' which is further globalizing cyber threats. Data can be hacked, manufacturing processes interrupted, and energy plants stopped from anywhere in the world. Many of the more prevailing risks these days are the ones that are emerging, so we need to look at long-term evolution of what emerging risks the company will be facing in the future. I know companies that have appointed a 'long term risk manager' – a type of futurologist looking at what the world will look like in 20 years.

MIKE NOLAN:

The CRO role continues to evolve, but as I mentioned, many companies still have a hard time getting an enterprise-wide view on risk. Interestingly, particularly for companies that don't have a CRO – where the risk monitoring responsibilities are assumed by a combination of roles… the chief compliance officer, the chief audit executive, legal, and others – I believe there is a need for collaboration to focus on developing a consistent view around risk and compliance. Based on that consolidated view, the board can take those risks and invite respective members of management to come in and articulate how they're managing the risk and ensuring that it's in line with the risk tolerances that management and the board have agreed on. And, of course, this risk dialogue should be taking place within the context of the strategy – which really good CEOs and boards do well, but often times it happens intuitively and informally. I think it's important to actually articulate and reinforce the risk/strategy linkage.

A strong risk culture is fundamental for effective risk management. What are some of the determining factors that can 'make or break' a strong risk culture?

LINDSAY MAXSTED:

It's primarily about leadership and setting the right example. Having the right vision for the company and its underlying values. This starts with the behavior of the board collectively and the individual board members themselves. Selecting the right CEO is fundamental – the board has to ask itself how the CEO goes about his or her business (values); how the CEO thinks about risk, how does he/she lead and in turn appoint the right type of executive to the organisation. You need to have an open and transparent view of the business and encourage, through your own actions, a culture where issues get surfaced early. You want people to come forward and not be condemned because there's a problem. Of course, it's relatively easy to come up with a list of preferred underlying behaviors, but much harder for a board to assure itself that the right things are actually happening.

There are a few things that can be done. Board and risk committee members should make sure they go out into the business to observe things first hand. Of course, staff might be on their 'best behavior', but there is value to be had in simply showing employees that the board is interested and is asking the right questions. People surveys can be instructive too – but again you have to ask the right questions. Also, depending on how concerned one is, there is a place for independent risk culture reviews where a third party can question employees about their experiences; understand whether they feel comfortable about raising issues, and so on.

I think 'safety' is a good barometer for risk culture. While a good 'safety' culture – early reporting of incidents; responding promptly with remedial action, and so on – doesn't necessarily mean there is a good culture overall, it can be used as an example, or a catalyst, to help embed similar behaviors in different areas. My final barometer is how an organisation deals with complaints. Are they embraced as an opportunity to right a wrong and improve processes or are they dealt with in some other way?

MAGGIE WILDEROTTER:

When you run companies, you're taking risk every single day. Every decision you make has risk associated with it. What you want is a culture within the company of taking calculated risk and taking risk where you try to identify up front, as best you can, the outcomes of taking those risks. You look at the best and worst case scenarios and try to anticipate what could go wrong and what could go right.

As a board member, I try to make sure the culture is healthy and that there's diligence around the risks that could have significant downside for the company. And it's not about the board saying "Don't take the risk." It's about the board saying "Have you thought through all of the issues associated with the risk posed by that decision?" You also want to make sure the culture itself brings in voices that serve as a check and balance within the senior leadership. If somebody says "stage left" and everybody just turns left without asking why, you probably don't have a healthy risk culture.

The right culture has an openness and transparency in terms of how the leadership works with each other and the wider organization – where employees are comfortable providing feedback in an open and honest discussion, where there are checks and balances and different views are heard.

ARTUR GABOR:

Since the strongest example comes from the top, it is crucial for management to promote activities which are ethical and which promote proper attitudes in the organization. As an audit committee chair, I expect management to be fully committed to supporting a proper tone at the top. What I see in my organization, is increased involvement in the creation and promotion of a culture based on high ethical standards – a culture whose purpose is to support the management process, including management of the corporate risks. Each of the business areas is directly responsible for monitoring and reducing the risks to acceptable levels. The responsibility of every employee is communicated and emphasized and their awareness is further strengthened by well-thought-out information campaigns. The company emphasizes the importance of its code of ethics that each employee is obliged to be familiar with and to adhere to. We also have an ethics spokesman, to whom employees can address any related issues.

DAME DEANNE JULIUS:

At Roche, our culture is shaped by the strong scientific underpinning of what we do. This scientific rigor is also key for risk awareness. In addition, our tradition as a Swiss company with strong family links fosters a long-term view in which long-term success is highly valued. This is also an element for a balanced risk culture. Taking risky short-cuts in the pursuit of short-term gains is just not on the agenda.

MARIE GEMMA DEQUAE:

Boards and audit committees have to set the right tone at the top – not only defining and approving the risk strategy, but also communicating a 'risk vision' and fostering a culture where everybody has ownership and responsibility for doing the best for the organization.

Management has to spread the risk culture message by working on a number of aspects. An effective risk reporting should be in place allowing timely escalation of risk events. A good risk culture is one in which it is acceptable that bad things are brought to the higher levels proactively and timely without fear of being condemned. Reporting is one element, but getting the right information in that reporting is even more important. You really have to promote a culture of openness to bring all information to the table – the very good and the very bad.

Management has to make sure proper systems of communication are in place to continually reinforce awareness around risk culture at all levels in the organization. It is important to learn from each other's best practices. During my time as risk manager, when I noted a specific good practice in a department, I promoted this actively and organized roundtables around it to share the practice with all functions and departments.

Finally, management has to work to make sure learning and development programs are in place – not only internally but also from outside experts – and that performance management and incentives take into account properly factors in risk culture aspects.

MIKE NOLAN:

Tone at the top should be a given. What's really important is tone in the middle. Issues often develop on the front lines of the business, at the middle manager level. If something's brought to their attention, how are they dealing with it? How they respond is critical – and a lot of that comes down to good ethics and compliance training, and setting clear expectations. Metrics and processes are important – and in fact the U.S. Federal Sentencing Guidelines require measurement as to the effectiveness of your compliance program – but in my experience the best organizations are consistently talking about the culture. There's a very clear expectation and ongoing communication. Because most incentives are still performance-based, the alignment of risk culture and risk appetite – defining and communicating that clearly – is critical.

To understand and monitor all of this, the board needs to be fully engaged, beyond the boardroom – visiting locations, speaking to middle management, understanding the expectations of regulators, and so forth. Whistleblower hotline reports, employee surveys, and ethics and compliance training are important, but really understanding the company's risk culture requires a combination of quantitative and qualitative measures and monitoring.

How can the board help ensure that the company is not too risk averse?

LINDSAY MAXSTED:

I think the board has a huge role – setting risk appetite is a really important part of what boards do. If the two most important decisions/roles of the board are the appointment of the CEO and overseeing the strategy of the company – you certainly can't do the latter unless you understand the risks involved in what you are doing and understand your tolerance for events to occur as set out in the risk appetite statement.

For me, strategy and risk are two sides of the same coin. Any discussion on strategy can be turned into a risk discussion and vice versa. The two are so entwined it's impossible to have a discussion on strategy without talking about the risks. The way you address any inclination to become too risk averse is to tackle it from the strategy side and look at where you are trying to take the organisation. If you can do that then you are embedding risk into all of your important discussions.

MAGGIE WILDEROTTER:

I think it's a challenge for a lot of boards. You can't just stick your head in the sand and take no risks. You have to have courage to be on a board because part of it is being able to assess the risks and enable the company's leadership to go take those risks.

I do see boards spending much more time debating risk. But you want to make sure it's being done in the context of making good decisions, not making no decisions. One of the things we emphasized in the NACD (Blue Ribbon Commission) white paper on Strategy Development is that strategy and risk go hand in hand. There's risk in the direction that the company chooses to take. There's risk in the implementation of the strategy. There's risk in the unknowns and the outside factors that you can't control. Risk has to be part of that strategic discussion. You try to identify what the risks could be and whether they're surmountable or not, how much risk you're willing to take, and how far you'll go in pursuing those strategic decisions.

It's important to spend time on risk and strategy at the corporate level and the operating level. At every meeting, we're touching at some point on an operating strategy of the company, whether it's the business model, a new market, partnerships, M&A, industry and competitive strategies, or pricing strategy. And then two or three times a year – rather than a one-time offsite – the board focuses on the macro strategy for the company. Are you a leader in your market? Are you an acquirer? Are you dressing up to sell? Are you splitting parts to the business out to create value in a different way? Are you rethinking how you manage cash on the balance sheet? This macro-level discussion is really where you get into whether the company is taking the right risks.

ARTUR GABOR:

An ever-increasing number of companies are beginning to use their risk management process in a more offensive manner. In my opinion, the courage in strategic thinking and clearly defined and communicated risk appetite determines the competitive value of a company. Sound business decisions at every level are those that consider the risks involved but which also entail taking calculated risks. A good organization should therefore create and provide favorable conditions to help employees make such decisions. My audit committee is certainly not 'risk averse', as evidenced by the number of risks on the risk map and also the risk weights we consider acceptable. Some level of risk is inherent, and attempts to have it completely eliminated are not only futile but also wrong from a business point of view.

DAME DEANNE JULIUS:

In our industry, we have to be open minded about future possibilities and research avenues. We want to develop innovations for the future. This means that we have to be courageous in our research agenda and take risks in deciding what to further investigate. If we are too risk averse we would fail in our strategic goal, which is doing today what the patients need tomorrow.

MARIE GEMMA DEQUAE:

Risk managers should never be a blocking factor of the future of the company. A good risk committee can be compared to the brakes of a car. The better the brakes, the faster the car can drive.

It's important to discuss the proposed risk appetite at the board level but certainly also at the executive level, because many companies work divisionally and often risk appetite is specific per type of product. Remuneration packages should be directly linked to risk appetite, with a long-term focus and claw-back features. Also, transparency should be included in the bonus system.

MIKE NOLAN:

Unless you know what your risk appetite is, there's no way to gauge whether you're taking too much risk or not enough. Articulating the company's risk appetite can feel somewhat soft, but it really comes down to the variability you're willing to accept – market cap swings, volatility of earnings, impacts on working capital, and the like. What are the risks around each key growth assumption? Will the operating model work? Risk needs to be directly linked to the strategy – and this gets to a question that I often pose to the board: "Is the risk lens equal to the growth lens?" In other words, are you putting enough rigor around the risk side of your strategy – i.e., are you stress-testing your growth assumptions? Are you doing some scenario planning and aligning your growth ambition with your risk appetite? If you don't spend enough time quantifying your risk appetite, you don't really know if you're taking the right amount of risk in relation to your strategy.

KPMG's Audit Committee Institutes

Sponsored by more than 30 member firms around the world, KPMG's Audit Committee Institutes (ACIs) provide audit committee and board members with practical insights, resources, and peer exchange opportunities focused on strengthening oversight of financial reporting and audit quality, and the array of challenges facing boards and businesses today – from risk management and emerging technologies to strategy and global compliance.

To learn more about ACI programs and resources, contact us at: **auditcommittee@kpmg.com**

More Global Boardroom Insights

Issue 1
Top Challenges:
The Audit Committee Perspective

Issue 2
Audit Quality and Communication with Shareholders and Others

Issue 3
The Cyber Security Challenge

Issue 4
Audit Committee Effectiveness

Issue 5
Audit Committee Workload

Issue 6
The Future of Audit

KPMG's Audit Committee Institutes around the world