Deloitte.

Risk Intelligent governance
Lessons from state-of-the-art board practices

Contents

This publication is part of Deloitte's series on Risk Intelligence. The concepts and viewpoints presented build upon those in the first whitepaper in the series, "The Risk Intelligent Enterprise™: ERM Done Right," as well as subsequent titles.

The series includes publications that focus on roles (the Risk Intelligent CIO, the Risk Intelligent chief compliance officer, etc.); industries (the Risk Intelligent technology company, the Risk Intelligent energy company, etc.); and issues (a Risk Intelligent view of reputation, Risk Intelligence in the age of global uncertainty, etc.). You can access the whitepapers in this series at www.deloitte.com/RiskIntelligence.

Open communication is a key characteristic of the Risk Intelligent Enterprise. Therefore, we encourage you to share this whitepaper broadly with colleagues at the executive, board, and senior management levels of your organization. Overall, the issues we outline should serve as a trigger for continuing discussions on Risk Intelligence.

Risk Intelligent governance: Lessons from state-of-the-art board practices

Preface

In 2009, Deloitte published "Risk Intelligent governance: A practical guide for boards." The intent of that paper was to help board members achieve Risk Intelligent governance by posing questions boards may consider and tools they could leverage. In this updated look at Risk Intelligent governance, we take a different approach, providing real-world examples and case studies compiled in our work with boards that employ state-of-the-art practices. We also leverage our analysis of relevant proxy statements disclosed by the Standard & Poor's (S&P) 500 in 2010, and the S&P 200 in 2011and 2013.[1]

As with our 2009 paper, six areas of focus lie at the heart of this publication. These focus areas have, of course, evolved, just as expectations have changed with respect to the board's risk oversight role and responsibilities. But these changes have not affected the grounding of this discussion in Deloitte's Risk Intelligent Enterprise™ framework, which encompasses several important themes:

- Risk taking as a means of value creation
- Candid communication and collaboration between boards and management
- Risk thinking that is embedded in the organization's culture
- The ultimate bridging of organizational silos

We offer this paper to directors as food for thought and a catalyst for focused action, with the caveat that Risk Intelligent governance is not a one-size-fits-all approach to be adopted by every organization or within each industry. The examples and case studies we provide are not universally applicable solutions. Rather, they offer a close-up look at how boards can put Risk Intelligent governance into practice.

"State-of-the-art" defined

Effective risk governance is almost assuredly more an art than science. No clear-cut formula or blueprint exists for Risk Intelligent governance, yet boards seem to recognize when they are upholding their responsibilities and performing their role well. But how can effective risk governance practices be recognized by those outside the organization?

In our experience, based on advising a number of boards in a range of industries, as well as examining the processes of the S&P top companies over the past three years, effective boards have risk management practices, strategies, processes, and approaches that:

- Encompass the entire business
- Address the full spectrum of risks
- Place significant weight on both probability and vulnerability
- Consider not just single events, but the interaction of multiple risks
- Make strategic decisions that arise from risk-informed processes

When taken together, these criteria add up to a board that is Risk Intelligent. Therefore, these are the standards we used when identifying state-of-the-art board practices.

[1] See "Risk Intelligent proxy disclosures: Transparency into board-level risk oversight," Deloitte Development LLC, 2010; "Risk Intelligent proxy disclosures 2011: Have risk-oversight practices improved?," Deloitte Development LLC, 2011; and "Risk Intelligent proxy disclosures—2013: Trending upward," Deloitte Development LLC, 2013.

Toward Risk Intelligent governance: Six actions boards can take

Events of the past decade—including the collapses of high-profile companies, economic volatility, and growing regulations and guidelines—have placed boards under greater scrutiny from regulators, shareholders, the media, and analysts. Such scrutiny has led to rising expectations for improved governance and risk management.

What can the board do to meet these expectations, be better aligned with business and marketplace trends, and help the organization achieve its goals? What is the board's role in helping to set the tone and in overseeing a risk management program that embeds appropriate risk management procedures—encompassing both value protection and value creation—into all of the organization's business pursuits? And how can directors work toward treating risk management not as a separate or standalone issue, but as an integral component of everything the board considers?

In short, how can the board become Risk Intelligent?

Based on our work with boards in their risk governance efforts, we offer six distinct actions that can help enable a Risk Intelligent governance approach:

1. Define the board's risk oversight role
2. Foster a Risk Intelligent culture
3. Understand and approve an appropriate risk appetite
4. Help management incorporate strategic risk thinking into strategy
5. Assess the "maturity" of the risk governance process
6. Make sure the organization discloses the risk story to stakeholders

As risk is intrinsic to the conduct of business, it is an essential consideration in every decision and activity. It is up to each board to decide what lessons it can glean and apply from these action items—and from the state-of-the-art examples provided—in the execution of its responsibilities.

The expanding regulatory perspective

The burgeoning number of regulations and guidelines include those set forth by:

- The U.S. Securities and Exchange Commission (SEC)
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- The Dodd–Frank Wall Street Reform and Consumer Protection Act

A few of the reports and proposed standards include:

- The Office of the Comptroller of the Currency's (OCC) proposed standards for heightened expectations of large banks
- The Federal Reserve's proposed enhanced prudential standards for foreign banks (which contains items that are applicable to U.S. banks)
- The "Consolidated Supervision Framework for Large Financial Institutions" (SR 12-17) published by the Board of Governors of the Federal Reserve System

1. Define the board's risk oversight role

An effective risk oversight process helps the board determine that the organization has a system in place for identifying, evaluating, prioritizing, managing, and adapting to critical risks. This process begins with a distinct demarcation of the board's roles and responsibilities, which includes assuring that management defines the risk governance infrastructure, positions risk as a priority for the organization, and initiates risk management communications and activities. A board can encourage and support the evolution of the company's risk program to encompass an enterprise-wide risk framework that establishes goals, roles, activities, metrics, and desired results.

The board's risk oversight role can be broken down into specific components. Risk governance includes making sure that the appropriate committees are involved in the oversight of risk processes under their jurisdiction, that the oversight of critical risks is allocated to those committees as appropriate, and that the full board engages in a robust dialogue about critical risks. Some aspects of risk oversight responsibility can be delegated to board committees—provided that it is understood that risk oversight is broader than a single committee and that the entire board is ultimately accountable. Regardless of the committee designated, roles and responsibilities should be appropriately documented in the committee charter.

Components of the board's risk oversight role

- Risk governance structure
- Oversight and monitoring of risk management processes
- Collaboration with the CEO and executive team to understand and oversee critical risks

Board members are responsible for overseeing and continually monitoring the overall risk management process. As part of this role, the board:

- Oversees the organization's processes for identifying, reporting, and managing risks
- Stays up to date on the company's vulnerabilities, risk culture, risk appetite, and risk tolerances
- Achieves an integrated view of the organization's risk management process and activities for discussions with the executive team
- Maintains committee charters that outline roles and responsibilities

Individual boards will, of course, need to be composed of members who possess the appropriate skills and experience in order to carry out these responsibilities.

Although risk management processes should be established and owned by management, the board oversees these processes and plays a significant advisory role in identifying leading practices, ensuring that processes both protect the business's assets and create value and opportunity. Furthermore, having appropriate mechanisms in place allows for information flow and discussion of the most critical risks with the full board.

In addition, board members should be satisfied that, regardless of the process, the CEO takes ultimate responsibility for risk management and that specific risks and activities are assigned to appropriate members of the management team. Also, when conducting customary board activities, such as touring facilities or engaging in "deep dive" sessions with business unit leadership, the board can enhance understanding not only of operations, but also of associated risks.

If the organization lacks an enterprise-wide risk framework that offers clear direction and guidance, the board should call upon management to develop one that encompasses appropriate board oversight processes. Several organizations, such as COSO, the Treasury Board of Canada Secretariat, and the Institute of International Finance, have developed risk management frameworks that can provide a helpful starting point. In addition, industry-specific frameworks have been modeled by regulators, such as the National Association of Mutual Insurance Companies (NAMIC) and the Federal Reserve Board.

Drilling deeper into the board's risk oversight responsibilities at ConocoPhillips

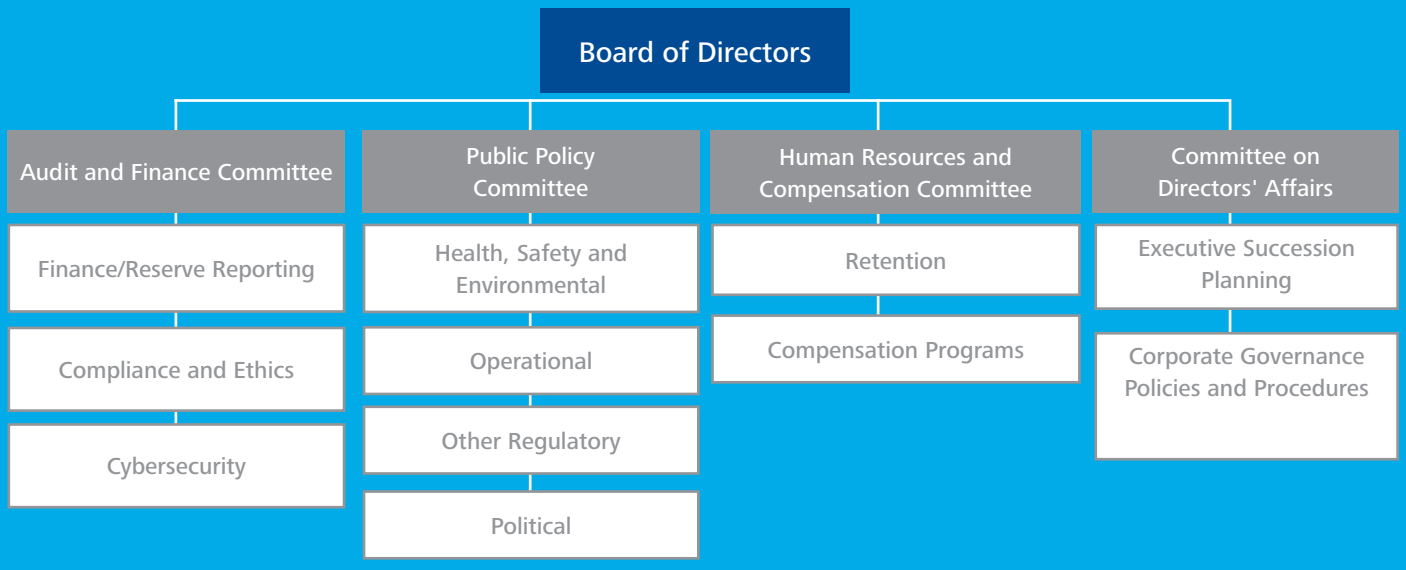
As boards continue to disclose more details about their governance processes, we are offered an inside look into risk oversight activities in practice. Consider the following description of the risk governance program at ConocoPhillips as described in its 2013 proxy statement.

The board at ConocoPhillips has oversight responsibility for risk management programs, with executive management handling the organization's day-to-day risks. In this capacity, the board confirms that the risk management processes, which have been designed and put in place by management, are functioning as intended. The board also ensures that necessary steps are taken to help implement and support risk-adjusted decision-making throughout the organization.

In carrying out this role, the board delegates certain elements of its oversight responsibility to individual board committees. Coordination of the company's risk management programs among the board's committees was assigned to the audit and finance committee. This committee regularly discusses risk assessment and risk management policies to ensure that the organization's risk management programs are performing effectively. Furthermore, the chairman of the audit and finance committee meets on an annual basis with other board committee chairs and management to review the board's oversight of the company's risk management programs.

In addition, the board receives regular updates from committees on individual categories of risk, including strategy; reputation; operations; people; technology; investment; political, legislative, and regulatory; and market risk. Such updates incorporate, among other things, the key risk areas shown in Figure 1. The board also exercises its oversight function with respect to all materials risks, which are identified and discussed in the company's public filings with the SEC.

Figure 1: Board oversight of key risk areas



Recommendations

Effective risk oversight begins with a solid—and mutual—understanding of the board's responsibilities, including those of management. This process may be further improved when boards:

- Work with management to map risk oversight responsibilities to specific board committees
- Create mechanisms for board committees to collaborate on risk-related activities through cross-membership, regular joint meetings, or the sharing of meeting materials or minutes
- Insist on clear, periodic reports on risk-related activities, including trends and assumptions, and avoid information overload by reviewing the quality, quantity, and nature of risk information received from management
- Periodically refresh all board committee charters so that each appropriately describes its role in risk oversight
- Keep informed of all committee activities in order to execute their role as overseer of their committees through robust committee reports at board meetings; provision of agendas, materials, and minutes to full board; or other mechanisms
- Oversee significant, strategic and enterprise-wide risks

"Delegating authority for oversight of our overall risk management programs to the Audit and Finance Committee, and ultimately oversight of certain risks across committees defined by where the expertise lies, provides for an effective risk oversight governance structure. Our practice of having committee chairs meet periodically establishes a platform for an enterprise-wide discussion of risk at the board level, allows us to look more deeply at key risk areas, and ensures us that ConocoPhillips has a robust process in place for identifying, managing, and monitoring critical risks."

— Jeff W. Sheets, Executive Vice President, Finance, and Chief Financial Officer, ConocoPhillips Company

2. Foster a Risk Intelligent culture

A Risk Intelligent culture[2] reflects employees' general awareness of, as well as attitudes and behaviors toward, risk. It is a key indicator of how risk is managed within an organization, and how widely the organization's risk management policies and practices have been adopted. Embedded in day-to-day practices, a Risk Intelligent culture covers all areas and activities and is influenced by an organization's incentives, management systems, and behavioral norms. It helps an organization achieve its mission and strategic objectives; it is communicated by leadership; and it promotes strong risk management, transparency, and accountability. Such a culture also helps employees understand how their actions and decisions fit within the organization's risk profile and approach.

A Risk Intelligent culture has the following characteristics:

- Risk accountabilities and responsibilities are clearly understood and defined
- Appropriate policies and practices, including formal processes to communicate, escalate, and report issues and risks are in place
- It encourages employees to challenge the organization should they have concerns
- It has a code of conduct that promotes the values and beliefs of the company, and that people understand and follow
- It is supported by education and awareness, providing employees with appropriate skill sets, knowledge, and other risk competencies
- Risk considerations are woven into performance evaluations, and an established incentive structure promotes and rewards Risk Intelligent behavior and decisions

[2] For more insights into Risk Intelligent culture, see "Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report," Deloitte Development LLC, 2012.

> "While manifestations of strong and weak risk cultures quickly become apparent, culture is a 'soft' concept that is hard to measure and about which it is hard to be objective. It is, however, of such fundamental importance that firms need to make use of all available means to create and maintain a strong risk culture. … A firm's culture can be modified over time, and it is the responsibility of each firm's Board and senior management to sustain the necessary effort to achieve a positive result."
>
> — "Governance for Strengthened Risk Management," Institute of International Finance, October 2012.

Many companies are increasingly focused on how a Risk Intelligent culture is defined—and then, once defined, how it is measured. Quantitative risk culture metrics, if appropriate to the organization, should be included in regular risk reports to the board and management. Those metrics might also be supplemented with key leading and lagging organizational cultural indicators.

Case study: Taking stock of an organization's risk culture

By encouraging management to enhance risk-related practices, boards play a significant role in improving the risk program. Moreover, improved monitoring and reporting mechanisms can provide boards with an inside look at the risk culture of the organization. Consider the following process—encouraged and supported by the board—that was implemented by one company.

A large financial services organization was in the midst of myriad changes—adapting to new leadership, expanding the business, increasing the number of employees, and keeping pace with a shifting regulatory landscape. Due to regulatory concerns, the chief risk officer (CRO) undertook an initiative to assess the company's risk culture.

With the support of the board and executive management, the company distributed a survey, which could be completed anonymously, to senior executives and key individuals, together accounting for roughly 40 percent of the organization. The survey covered four categories—risk competence, motivation, relationships, and organizational risk environment—and was designed to gain a better understanding of the existing risk culture; the role and perception of the risk management function; and the level of awareness of risk management practices, policies, and tools. The response rate was nearly 100 percent.

As a result of these survey findings, executive management committed to changing the risk culture and established several initiatives to kick off the change. Survey results and recommendations were reported to the board risk committee, which supported management's proposed changes.

Distributing this survey, getting backing and insights from the board, and then investing in programs to fill the gaps allowed the CRO to achieve one of his key risk strategy objectives: creating a stronger culture of risk awareness and mitigation across the organization. It also provided the board with a view into the risk culture of the organization and a useful baseline to compare to in the future.

Recommendations

What can boards do to help cultivate a Risk Intelligent culture?

- Build an environment in which employees are comfortable challenging others, including authority figures, and the people who are being challenged respond positively
- Establish "safe/free" zones for those reporting potential issues, problems, or concerns
- Provide the right "tone at the top" to promote ownership, accountability, transparency, and collaboration, and reinforce expectations for performance with integrity in all of its dealings with management
- Encourage management to create repeatable processes to assess and continuously improve the risk culture of the organization
- Reward people who focus on managing and mitigating risk by aligning incentive, reward, and performance systems with a focus on risk, compliance, and controls
- Support management in its commitment to enhance the risk culture through appropriate allocations in resources and funding, focused risk management training programs, and distribution of risk culture surveys and survey results

3. Understand and approve an appropriate risk appetite

In some industries, the concept of risk appetite is more quantitative; in others, it is more qualitative. Whether dealing with hard metrics or softer guidelines, determining the level and types of risks an organization is willing to take is a difficult task—yet one that is critical to business success. Therefore, evaluating, challenging, and approving appropriate risk appetite levels are key responsibilities of the board. In addition, risk appetite is an important mechanism for connecting the organization's risk program to its strategy. So the board should apply the company's risk appetite to its major decisions.

Risk Intelligent companies establish the amount of risk they are willing to take regarding acquisitions, market expansion, and other strategic decisions and initiatives. Generally speaking, companies have a higher appetite for rewarded risks (e.g., new product development) and a lower appetite for unrewarded risks (e.g., operational failures). Once the risk appetite is defined (usually by management) and approved by the board, management then communicates it throughout the organization

Management should continually monitor the company's risk exposures, evaluate actual risk exposure levels against the stated risk appetite, adjust risk tolerances and policies as necessary, and report on this process to the board. This allows board members to determine opportunities for rewarded risk-taking strategies or ascertain whether the organization is taking on too much risk. It is important to remember that risk appetite levels are meant to be a guide—not a hard and fast rule. Because the organization will not have accurate and quantifiable numbers for every risk it faces, there will always be some level of ambiguity for setting risk exposure levels. The board should be advised and provide guidance when business decisions have the potential to exceed, or come close to exceeding, acceptable risk levels. Board members should be satisfied that senior executives understand and reconcile various views of risk within the organization.

The approach for approving a risk appetite should be iterative, in order to keep pace with the organization's ability to measure risk levels, competitive pressures, regulator input, and other changes in the marketplace. Finally, while it may not be practical to precisely measure risk appetite levels, they can be considered in terms of trade-offs or from a benchmarking perspective.

Recommendations

In Risk Intelligent organizations, risk appetite is applied when signing off on new business strategy, undertaking a major acquisition, or any other important decisions. Boards can become more effective in reviewing and approving risk appetite levels—and in helping the organization apply risk appetite to strategic decisions when they:

- Provide escalation guidance when business decisions may exceed the approved risk appetite
- Work with management to create an iterative risk appetite approach to keep pace with changes within both the organization and the marketplace
- Consider advanced methods for defining risk appetite in both qualitative and quantitative ways
- Review "look back" analysis to determine how closely the organization has followed approved risk appetites in making business decisions
- Participate in scenario analysis to better understand response plans should underlying assumptions prove to be flawed and business decisions exceed the risk appetite
- Align management incentives with risk appetite and do not encourage risk-taking outside of acceptable boundaries

The role of risk appetite: A look at four S&P 200 companies

More and more boards are disclosing their role with respect to setting the risk appetite of the company. In our 2013 analysis of risk disclosures of the S&P 200 companies that file proxy statements, 12 percent specifically address risk appetite. This is an increase from 8 percent in 2010, the first year our analysis was completed. Below are excerpts from public proxy disclosures provided by four companies—American Express, Nordstrom, General Electric, and Express Scripts—that address risk appetite.

"The policy sets the company's risk appetite and defines governance over risk taking and the risk monitoring processes across the company. Risk appetite defines the overall risk levels the company is willing to accept while operating in full compliance with regulatory and legal requirements. In addition, it establishes principles for risk taking in the aggregate and for each risk type, and is supported by a comprehensive system of risk limits, escalation triggers and controls designed to ensure that the risks remain within the defined risk appetite boundaries."
—American Express Company

"The full Board has primary responsibility for oversight of risk management, and has assigned to the Board's standing committees the specific focus of the risks inherent in their respective areas of oversight. The full Board considers and reviews the Company's risk appetite, which is the amount of risk the organization is willing and able to accept. Through the risk oversight process, the Board … obtains an understanding of the risks inherent in the Company's strategy and management execution of the strategy within the agreed risk appetite."
—Nordstrom, Inc.

"We reward our executives for taking responsible risks in line with the company's strategic objectives and overall risk appetite. In order to ensure that we are executing according to our strategic objectives and that we only accept risks for which we are adequately compensated, we evaluate risk at the individual transaction level, and evaluate aggregated risk at the customer, industry, geographic and collateral-type levels, where appropriate. Risks identified through our risk management processes are prioritized and, depending on the probability and severity of the risk, escalated to the chief risk officer (CRO)."
—General Electric Co.

"Management provides periodic updates to our board of directors with respect to key risks which allows the board to formulate plans to manage these risks or mitigate their effects. At least annually, the board of directors discusses with management the appropriate level of risk relative to our corporate strategy and business objectives and reviews with management our existing risk management processes and their effectiveness. Further, at least annually, our Audit Committee discusses with management and internal audit our major financial risk exposures and the steps that have been taken to monitor and control such exposures, including a discussion of our risk assessment and risk management policies."
—Express Scripts Holding Company

4. Help management incorporate strategic risk thinking into strategy

One of the board's primary roles is advising management on the development of a strategy that aligns with the mission of the organization, as well as the short- and long-term vision of stakeholders. At the heart of all strategic issues competing for the board's attention is the risk—that is, the potential for loss or diminished opportunity for gain—that the strategy poses to the organization's priorities.

Determining whether the organization's strategic direction has been appropriately challenged, vetted, and optimized is a responsibility that lies squarely with the board. This responsibility is as much about focusing on the risks that limit a chosen strategy from being successful in the near term as it is about being aware of new risks created by the strategy. Disruptors that could fundamentally alter an organization's ability to compete must also be taken into account. Together, these considerations help shape how well the management team's portfolio of strategic options can deal with an ever-changing and increasingly unpredictable world.

The board provides important leadership in the strategic planning process by asking management the right questions, fostering an open dialogue, and considering alternative scenarios. Ongoing, proactive oversight by the board can add significant value by bringing a more expansive perspective on potential strategic risks—losses as well as diminished opportunities.

Helping management incorporate strategic risks into the strategy is a key role of the board. It is also an area that is being explored more thoroughly at Deloitte. Because this issue is of such importance, we will be addressing it more fully in a separate paper in Deloitte's series on Risk Intelligence.

Equipped with a dose of healthy skepticism, the board can also help keep planning grounded in today's market realities while challenging myopic views of the future. Finally, the board can broaden the role of risk programs to include strategic risks to allow it to "see around the corner"—understanding potential external disruptions as well as newly created risks.

Recommendations

Boards can determine if strategic risks are identified and addressed in its current strategic planning when they:

- Consider whether it provides "active oversight" in developing the strategy
- Regularly engage on strategic objectives as well as strategic risks
- Confirm that key strategic risk indicators are developed and monitored to alert decision makers to potential changes
- Assess potential new strategic risks on an ongoing basis
- Consider contingencies should the organization's risk profile change
- Encourage strategic flexibility by fully understanding the drivers of strategic risk, as well as the factors that may require a company to change course to respond to risks and opportunities

5. Assess the "maturity" of the risk governance process

An organization's risk management capabilities, along with the board's risk governance processes, may be assessed according to their "maturity"—that is, where they reside on a curve that progresses toward Risk Intelligence. From ad hoc practices to formal and embedded processes, and various stages in between, there is no definitive threshold that all organizations should achieve. But there is a level of maturity that is right for each organization, and it depends on how capable that organization needs to be in order to manage its risk profile. Regular assessments can help organizations determine their current maturity level, the level they aspire to reach, and whether the board is getting the amount of information it needs to fulfill its role.

The key to effective assessments? Asking thoughtful questions to establish the current state and then assessing the risk governance process to help management identify, prioritize, and implement improvements. For example:

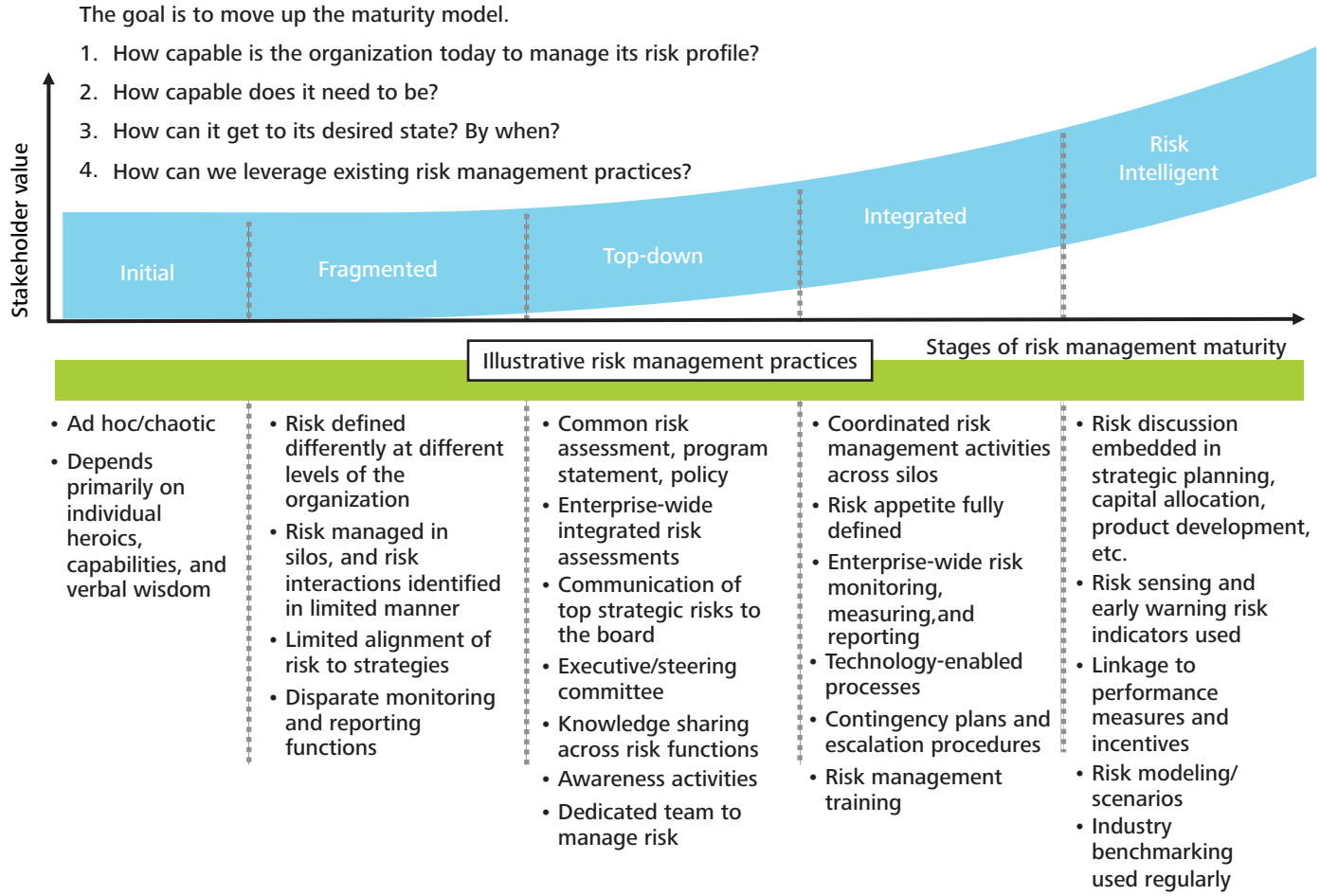
- How frequently is the board informed on risk management issues?
- Are specific risks mapped to board committees and processes?
- Which board committees are responsible for various aspects of risk governance?
- Are risk identification, analysis of key assumptions, and scenario planning considered in the strategic planning process?
- Is the board getting the necessary information on these and similar issues in a timely and accurate manner?

The answers to these questions can be a valuable guide for measuring an organization's effectiveness in providing Risk Intelligent governance.

Most boards have processes for self-assessment of the board and board committee skills and competencies. Far too often, however, the assessment considers risk knowledge in broad terms, such as "risk management experience." To enhance the ability of the board to oversee critical risk areas, boards should consider expanding the assessment criteria to be more specific to the strategic-, operational-, financial-, and compliance-related risks facing the company.

An important area for questioning is how management monitors and identifies emerging risks. How robust are the reports on key risk indicators? Is there agreement on when management should take action? What tools (e.g., risk sensing, risk modeling, scenario planning) are used to monitor the risks on an ongoing basis? Also, how can the board get reassurance that the reports it receives about known and emerging risk exposures and opportunities are reliable?

Figure 2: Risk maturity model
Understanding your risk capability—current and desired state



Finally, a critical area that is often overlooked is the assessment of the information provided to the board and board committees. Is it concise yet comprehensive? Is the level of detail appropriate and reasonable? Are key risk reports accompanied by an appropriate summary of trends and changes since the last time the material was presented? Are the key take-aways and specific actions to be taken clear to the directors? A process for management and the appropriate members of the board to periodically review the information in a facilitated session may be an efficient way to accomplish improvements.

Case study: Assessing the maturity of an organization's risk management process

Having undertaken a number of initiatives to improve its risk management process, including a strategic risk assessment and a Black Swan workshop, a professional services firm was intent on keeping this continuous improvement process on track. The next step: a maturity assessment of the company's enterprise-wide risk management process. The company's approach was unique in that it contemplated the key elements of the board's risk oversight processes. Both the C-suite and the board recognize the importance of action-oriented assessments that continuously move the organization toward leading practices and better integration of risk with strategic and day-to-day decision-making.

Executive interviews were conducted, and a report was compiled, assessing the risk management initiative in six areas: risk governance, risk identification and response, risk assessment criteria, risk tracking and reporting, the integration of risk management into company processes, and risk-aware culture. The report referenced the organization's current state and provided recommendations for improving the board's oversight of risk.

The risk governance recommendations included: updating board self-evaluations to include risk management-related questions, developing a skill matrix to assess risk management capabilities at the board level, board training to improve knowledge of risk management issues and key trends, and one-on-one meetings between the audit committee chair and the organization's risk leader. Recommendations also included enhancements to the risk management dashboard to contemplate impact/vulnerability rankings and the identification of topics for "deep dive" sessions to enhance the board's knowledge of specific risks.

Recommendations

Effective risk governance calls for a regular assessment of the maturity of the organization's process. A simple maturity model, shown in Figure 2, can help organizations gauge where they are today, as well as set plans for the future. Here are some additional considerations for assessing the maturity of a risk governance process:

- Assess the skills and knowledge of the board on a level that provides enough granularity to identify competency "gaps" in key strategic, operational, financial and compliance risk areas
- Implement an ongoing development plan to enhance competencies through recruitment, education, and the use of outside advisors (when appropriate)
- Periodically review the overall quality, quantity, and usability of risk-related information provided to the board
- Utilize a risk-based approach for the development of meeting agendas and materials so that adequate time is devoted to the most important risks
- Encourage management to include the board and relevant risk governance processes in its periodic assessment of the company's enterprise risk management (ERM) program

6. Make sure the organization discloses the risk story to stakeholders

The SEC proxy disclosure rules require U.S. public companies to explain how the board administers its risk oversight responsibilities and how the board works with management on risk-related activities. But why should Risk Intelligent organizations stop there? The SEC disclosure rules were intended to provide greater visibility and insight into governance areas. Yet these rules also present organizations with the opportunity to highlight the quality of their board oversight practices through disclosures above and beyond boilerplate requirements. Therefore, the higher the quality of information regarding the board's role in risk oversight, management's risk management processes, and how a company embeds risk monitoring into all that it does, the better.

SEC proxy disclosure rules do not dictate the governance infrastructure or processes to implement. Rather, they simply ask companies to report on established processes. So when it comes to disclosure, there are no right answers. As a result, the disclosures vary significantly from company to company.

By enhancing risk oversight disclosures, companies may be able to improve their attractiveness to long-term stakeholders. Therefore, it may be to the organization's benefit to give better insights as to the risk governance and management processes in place, how the board is involved in overseeing those processes, what risk factors have been identified, how those risks are tied to the information the board receives, if the board has a role with regard to risk appetite, and so on.

The work of improving risk oversight is an ever-evolving process. In Deloitte's analysis of proxy statement disclosures in 2010, 2011, and 2013, we have seen evidence of such an evolution. For example, a few trends that we have gleaned from our 2013 analysis include:

- Thirty percent (as opposed to 25 percent in 2011) of S&P's 200 companies that filed proxy statements separately address reputational risk[3]
- Adoption of risk oversight practices by boards continues to grow, with an increased trend toward risk-related responsibilities distributed among various board committees[4]
- Disclosures of risk-related practices with regard to discussion about risk appetite and the changes in infrastructure, including the establishment of a management risk committee, continued on an upward trend in 2013 as compared to past years[5]

Form 10-K calls for the disclosure of material risk factors. The board, and in particular the audit committee, should spend adequate time considering the company's 10-K risk disclosures. Are the risks identified through the risk program the same risks discussed in the Form 10-K as managed by the business? Are the Form 10-K risks the most material risks, and what is the board's role in addressing them? Do disclosures rely too much on boilerplate and "legalese," as opposed to thoughtful narratives and complimentary quantitative analysis?

[3] Based on proxy statements from 170 Standard & Poor's 200 companies analyzed by Deloitte in 2011 and 2013.
[4] Based on proxy statements from 132 Standard & Poor's 200 companies analyzed by Deloitte in 2010, 2011, and 2013.
[5] "Risk Intelligent proxy disclosures—2013: Trending upward," Deloitte Development LLC, 2013.

The board may find it useful to periodically analyze the company's risk disclosures to those of peer organizations. Are there risks that others seem to be concerned about that have not been adequately considered by the company?

How Coca-Cola's board shares its risk management approach with stakeholders

As mandated by the SEC's proxy disclosure rules, The Coca-Cola Company describes the board's risk oversight role and how it interacts with management. The company goes beyond what is required, however, revealing how it views risk—not in isolation but as part of decision-making—and the importance it places on including risk when discussing and determining business strategy. The following summarizes the board risk disclosures from the 2013 proxy statement.[6]

Coca-Cola's proxy disclosure states that effective risk oversight is a priority for the board of directors. The disclosure supports this statement by describing how the board has established a risk governance framework that is designed to understand critical risks, facilitate open discussion between management and the directors, and foster an appropriate culture of integrity and risk awareness.

In addition, the proxy describes a robust ERM program that strengthens the identification and management of risks. The board implements its risk oversight function as a whole, with all directors actively involved in overseeing risk, and through delegation to committees, which are chaired by strong and experienced directors. These committees meet regularly and report back to the full board, playing significant roles in carrying out risk oversight.

Because overseeing risk is an ongoing process that is embedded into Coca-Cola's strategic decisions, the board also discusses risk throughout the year at other meetings in relation to specific proposed actions.

[6] The Coca-Cola Company's entire "Board Oversight of Risk" disclosure is provided in the Appendix.

Recommendations

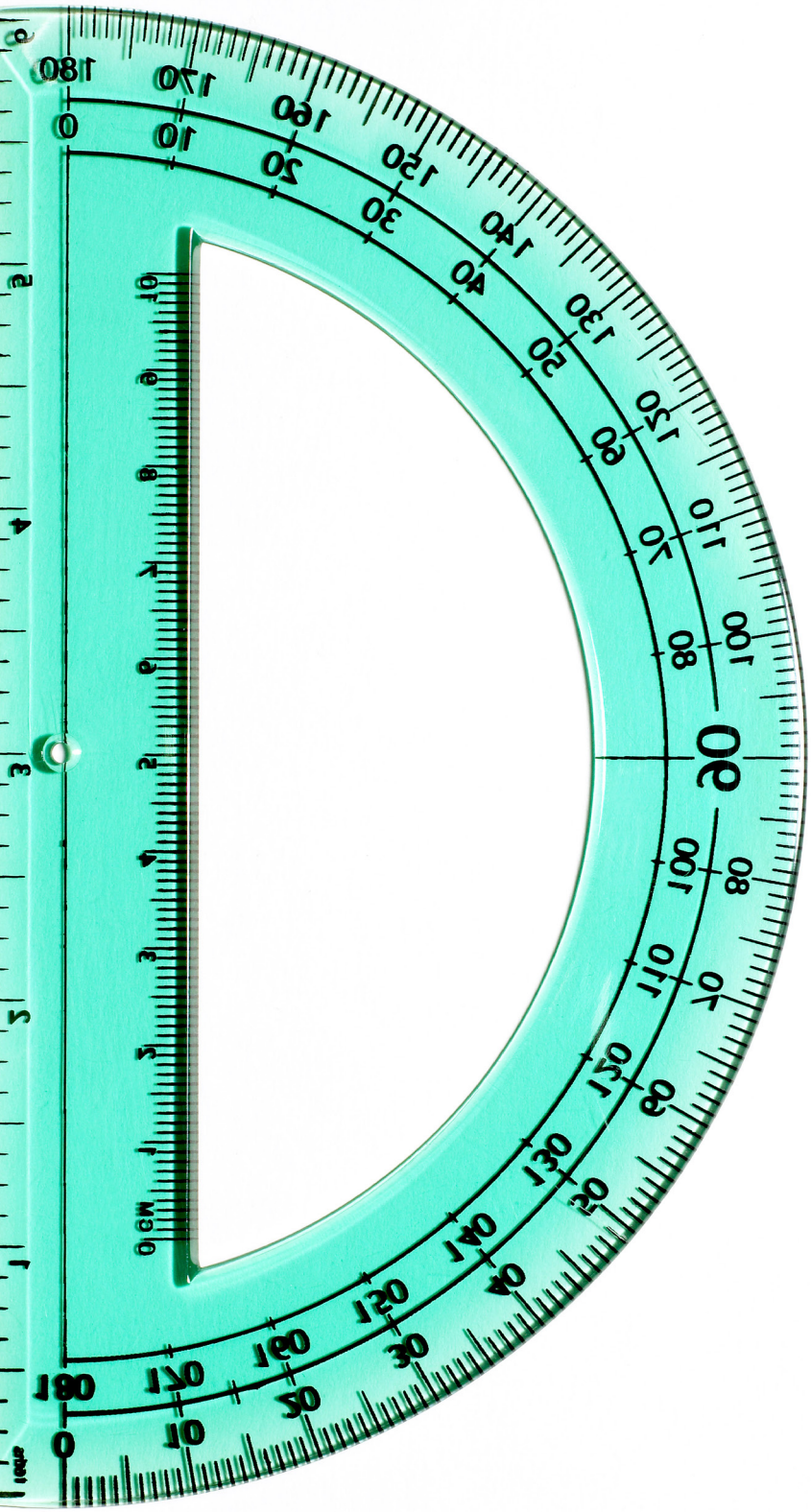
Risk-related disclosures in proxy statements can provide insight into a company's risk oversight and risk management practices. Organizations can more effectively disclose their risk story to stakeholders when they:

- Provide visibility into how the process actually works, including the roles of the board and its committees, in addition to discussing the structure of risk oversight
- Offer greater insight into board processes on risk and other matters
- Encourage plain-English disclosures or supplement risk disclosures with quantitative analysis and graphic presentations
- Evaluate risk factor disclosures so that they are current, specific, concise, and relevant

"The SEC proxy disclosure rules offer a real opportunity to provide greater visibility into the comprehensive approach we take on risk oversight. For The Coca-Cola Company, risk oversight is viewed as a critical component of both our day-to-day and longer term strategic decision-making. Giving investors and stakeholders a better view into how our Board of Directors performs this important role, as well as how the Board interacts with management, helps to illustrate the rigorous risk governance and management processes that have been implemented at our Company."

— Mark Preisinger, Director of Corporate Governance, The Coca-Cola Company

Conclusion



The trends and forces that impact business—along with the attendant risks—can change in a heartbeat. That's why the role of the Risk Intelligent board is so important. Board members' combined breadth of perspective, depth of experience, and knowledge of the enterprise can lend valuable support to risk management efforts and help the organization both create and protect value.

By having a solid yet forward-looking foundation in place—beginning with risk oversight and including risk culture, risk appetite, maturity assessments, alignment of risk and strategy, and disclosure—boards can:

- Determine that the organization has an appropriate system in place for identifying, evaluating, prioritizing, managing, and adapting to critical risks
- Satisfy themselves that consideration of risk is embedded in the company's day-to-day practices and decisions
- Oversee management's establishment of parameters with respect to the level and types of risk the organization is willing to take
- Advise management on the development of a strategy that aligns with the mission of the organization and confirm that management is considering strategic risks
- Consider areas of excellence and development opportunities in the organization's risk management process, highlighting those that may need attention
- Help make the organization more attractive to stakeholders by providing greater visibility and insight to into risk governance areas

We hope many of the insights and examples that we have provided can be applied to your own boards and organizations as you guide your organization toward Risk Intelligence.

Appendix

The Coca-Cola Company's "Board Oversight of Risk" disclosure

From "The Coca-Cola Company Notice of 2013 Annual Meeting of Shareowners and Proxy Statement," pp. 37-38.

Board oversight of risk

The Board is elected by the shareowners to oversee their interest in the long-term health and the overall success of the Company's business and its financial strength. In order to fulfill the Board's responsibilities, it oversees the proper safeguarding of the assets of the Company, the maintenance of appropriate financial and other internal controls and the Company's compliance with applicable laws and regulations and proper governance. Inherent in these responsibilities is the Board's understanding and oversight of the various risks facing the Company. The Board does not view risk in isolation. Risks are considered in virtually every business decision and as part of the Company's business strategy. The Board recognizes that it is neither possible nor prudent to eliminate all risk. Indeed, purposeful and appropriate risk-taking is essential for the Company to be competitive on a global basis and to achieve the objectives set forth in its 2020 Vision.

Effective risk oversight is an important priority of the Board

The Board has implemented a risk governance framework designed to:

- understand critical risks in the Company's business and strategy;
- allocate responsibilities for risk oversight among the full Board and its committees;
- evaluate the Company's risk management processes and whether they are functioning adequately;
- facilitate open communication between management and Directors; and
- foster an appropriate culture of integrity and risk awareness.

While the Board oversees risk management, Company management is charged with managing risk. The Company has robust internal processes and a strong internal control environment which facilitate the identification and management of risks and regular communication with the Board. These include an enterprise risk management program, a Risk Management Committee co-chaired by the Chief Financial Officer and the General Counsel, regular internal management disclosure committee meetings, Codes of Business Conduct, robust product quality standards and processes, a strong ethics and compliance office and a comprehensive internal and external audit process. The Board and the Audit Committee monitor and evaluate the effectiveness of the internal controls and the risk management program at least annually. Management communicates routinely with the Board, Board committees and individual Directors on the significant risks identified and how they are being managed. Directors are free to, and indeed often do, communicate directly with senior management.

The Board implements its risk oversight function both as a whole and through delegation to Board committees, which meet regularly and report back to the full Board. All committees play significant roles in carrying out the risk oversight function.

Oversight of risk

- The Board oversees risk management.
- Board committees, which meet regularly and report back to the full Board, play significant roles in carrying out the risk oversight function.
- Company management is charged with managing risk, through robust internal processes and strong internal controls.

In particular:

- the Audit Committee oversees risks related to the Company's financial statements, the financial reporting process and accounting and legal matters. The Audit Committee oversees the internal audit function, the Company's ethics programs, including the Codes of Business Conduct, and the Company's quality, safety, environmental assurance and information technology security programs. The Committee periodically receives reports on and discusses governance of the Company's risk management process and reviews significant risks and exposures identified to the Committee by management, the internal auditors or the independent auditors (whether financial, operating or otherwise), and management's steps to address them. In connection with its oversight of these matters, the Committee members will regularly meet separately with the Company's General Counsel, Chief of Internal Audit and representatives of the independent auditors;
- the Compensation Committee evaluates the risks and rewards associated with the Company's compensation philosophy and programs. As discussed in more detail in the Compensation Discussion and Analysis beginning on page 48, the Compensation Committee reviews and approves compensation programs with features that mitigate risk without diminishing the incentive nature of the compensation. Management discusses with the Compensation Committee the procedures that have been put in place to identify and mitigate potential risks in compensation;
- the Finance Committee oversees certain financial matters and risks relating to pension plan investments, currency risk and hedging programs, mergers and acquisitions and capital projects;
- the Management Development Committee oversees management development and succession planning across senior management positions; and
- the Public Issues and Diversity Review Committee oversees issues that could pose significant reputational risk to the Company.

In addition, annually, one meeting of the full Board is dedicated primarily to evaluating and discussing risk, risk mitigation strategies and the Company's internal control environment. Topics examined at this meeting include, but are not limited to, financial risks, political and regulatory risks, legal risks, supply chain and quality risks, information technology risks, economic risks and risks related to the Company's productivity and reinvestment efforts. Because overseeing risk is an ongoing process and inherent in the Company's strategic decisions, the Board also discusses risk throughout the year at other meetings in relation to specific proposed actions.

The Company believes that its leadership structure, discussed in detail beginning on page 33, supports the risk oversight function of the Board. While the Company has a combined Chairman of the Board and Chief Executive Officer, strong Directors chair the various committees involved with risk oversight, there is open communication between management and Directors and all Directors are actively involved in the risk oversight function.

To learn more about risks facing the Company, you can review the factors included in Part I, "Item 1A. Risk Factors" in the Form 10-K. The risks described in the Form 10-K are not the only risks facing the Company. Additional risks and uncertainties not currently known or that may currently be deemed to be immaterial also may materially adversely affect the Company's business, financial condition or results of operations in future periods.

Contact us

The following professionals have extensive experience working with boards of directors to implement Risk Intelligent governance programs. To learn more, contact:

Steve Alogna
Director
Deloitte & Touche LLP
+1 203 708 4844
salogna@deloitte.com

Scott Baret
Partner and Global Leader, Enterprise Risk Services – Financial Services
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Maureen Bujno
Director, Center for Corporate Governance
Deloitte LLP
+1 212 492 3997
mbujno@deloitte.com

Mark Carey
Partner
Deloitte & Touche LLP
+1 571 882 5392
mcarey@deloitte.com

Michele Crish
Senior Manager
Deloitte & Touche LLP
+1 516 918 7313
mcrish@deloitte.com

Jacqi Fifield
Senior Manager
Deloitte & Touche LLP
+1 503 727 5302
jfifield@deloitte.com

Robert Kueppers
Senior Partner
Deloitte LLP
+1 212 492 4241
rkueppers@deloitte.com

Sandy Pundmann
Partner
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Henry Ristuccia
Partner, U.S. Co-Leader, Governance, Risk and Compliance
Global Leader, Governance, Risk and Compliance
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

Nicole Sandford
Partner, National Governance Services Practice Leader
Deloitte & Touche LLP
+1 203 708 4845
nsandford@deloitte.com