Growing demands on boards

The role of the board has always been an important and demanding one, but today’s board members face increasingly complex challenges in overseeing an organization’s risk management, including:

- Demands for greater accountability from investors
- Increasingly complex regulatory oversight
- Sluggish economic growth
- The convergence of industries
- Disruptive new technologies
- Scarcity of resources and the effects of a changing climate
- Human capital and talent management challenges

In the aftermath of the global financial crisis, stakeholders and regulators intensified their focus on the board’s risk management oversight role. Directors are now expected to take a more proactive role in understanding the company’s risk appetite, its risk culture, and risk management policies and procedures. And more than ever, boards must understand the risks their organization faces.

Those risks are many. Organizations are pressed to meet quarterly financial targets, while complying with accounting standards and new reporting requirements (e.g., new revenue recognition standards). On the operational side, increased outsourcing of major elements of manufacturing processes in emerging markets and countries can increase risks.

Meanwhile the regulatory environment has grown more active, with fines and sanctions on the rise. And the recurring front-page headlines about cyber-attacks and data breaches at companies across the world make it clear that cybersecurity has become a primary concern. Finally, the immense impact of social media means that any misstep in dealing with these challenges can feed into reputational risk.

Boards recognize the significance of risk management and some have created stand-alone committees to address the changing risk climate. See below for more on how boards are addressing risk management.

Where is risk management addressed at the board level?

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full board</td>
<td>36%</td>
</tr>
<tr>
<td>Audit committee</td>
<td>33%</td>
</tr>
<tr>
<td>Risk committee</td>
<td>19%</td>
</tr>
<tr>
<td>Not addressed</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>8%</td>
</tr>
</tbody>
</table>

EY Governance, risk and compliance survey 2015
What organizations are telling us

In this year’s Governance, Risk, and Compliance (GRC) survey, we focused on an array of topics (e.g., risk strategy, coordination of functions, internal audit, technology) to gain a better understanding of how well organizations are managing risk today.

While organizations demonstrated they are making progress, they indicated that further opportunities exist to improve the way that they identify, manage and respond to risk.

Survey findings

### Top five risks

<table>
<thead>
<tr>
<th>#</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Financial</td>
</tr>
<tr>
<td>2</td>
<td>Operational</td>
</tr>
<tr>
<td>3</td>
<td>Regulatory</td>
</tr>
<tr>
<td>4</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>5</td>
<td>Reputational</td>
</tr>
</tbody>
</table>

### Link risk to the business

- **97%** of organizations have made progress in linking their risk management objectives and business objectives...
- **16%** but only 16% of the 97% consider them to be closely linked today

### Risk involvement

- **66%** of organizations indicated that risk management has limited involvement...
- **90%** but 90% expect to be directly involved or providing inputs within the next 3 years

### Trends/risk drivers

<table>
<thead>
<tr>
<th>Risk</th>
<th>Challenges</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emerging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Markets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shifts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Changing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Implications

- While organizations have expanded their view of risk, they continue to primarily focus on preventable risks.
- Organizations that also focus on strategic and external risks can convert those risks into opportunities.
- Organizations have made a significant amount of progress in bridging the gap between risk management objectives and business objectives.
- However, greater opportunity exists for organizations to achieve stronger alignment.
- Organizations recognize the value of directly involving risk management in business decision-making.
- Organizations that directly involve risk management are better able to identify, manage and respond to the risks that impact their business.
- We are seeing businesses impacted by a multitude of disruptive forces and mega trends globally, each requiring a different response to manage the associated risk.
- Organizations are challenged with developing a comprehensive view of risk, as well as regularly identifying and responding to existing and emerging risks.
- While a rapidly changing risk landscape creates challenges, it also presents opportunities.
- Organizations that manage risk well are better positioned to capitalize on the upside potential of risk.
Framing the board’s oversight of risk

Boards of directors need to know where to focus when surveying this changing risk landscape. Although risks historically have been categorized in different ways, it helps to consider risks in the context of an organization and how best to respond to those risks. Many organizations categorize risk into three categories according to their impact:

- **Strategic risks** that must be accepted because they offer benefits. Examples include risks related to user adoption, return on assets, market penetration, and talent management.
- **Preventable risks** that should be avoided or mitigated because they would have a negative impact. Examples include employee fraud and risks related to information security, financial integration, and regulatory compliance.
- **External risks** that the organization cannot control. These can have positive or negative effects. Examples include competitive shifts, geopolitical risks, and natural disasters.

Looking at the risk landscape through the lens of strategic, preventable and external risks can help sharpen the board's focus to build a risk-aware organization, as can frequent and regular updates of the organization’s risk profile.

When it comes to identifying, understanding and linking risks to strategic objectives, the three lines of defense model offers significant advantages. The model is based on the premise that risk management is everyone’s job, which is the most appropriate approach given today’s risk landscape. Accordingly, the Institute of Internal Auditors recently issued a report formally linking the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework and the three lines of defense. The three lines of defense include:

- **First line (operations and business units)**: This group comprises the line management directly responsible for identifying and managing risks. This group must consider risk management as a crucial element of its everyday job.
- **Second line (management assurance)**: This group is responsible for ongoing monitoring of the design and operation of controls in the first line, as well advising and facilitating risk management activities.
- **Third line (independent assurance)**: The groups responsible for independent assurance over managing of risks. Internal Audit (IA) plays the leading role.

Not all companies have the resources to develop and sustain three distinct lines of defense, but every organization should make sure that its risk coverage mitigates gaps and avoids unnecessary duplication.

In the three lines of defense model, the first line usually reports to senior management and is typically responsible for management controls and internal control measures. The second line is typically responsible for the effective management and oversight of risk and control. The third line, which includes IA, is independent of the first two and usually reports to the board as well as management. IA is the impartial, conduit between the business and the board. To make sure the organization appropriately deals with the risks it faces, the board and audit committee should work with IA, which has a wide line of sight into the business.

Regardless of the framework it adopts, be it the COSO framework – the most widely used framework in the US and adopted or adapted by numerous businesses and countries around the world – or the principles-based, “comply or explain” approaches used in the UK and the EU, the board should make sure as it works its way through the strategic, preventable and external risks that it has sufficient knowledge to gain comfort that each risk area is covered. The board needs to be sure that it has been effectively informed about governance policies and procedures.

---

Do your GRC functions prepare an integrated report addressing the organization’s risks and management actions for the board and executive management?

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annually</td>
<td>28%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>33%</td>
</tr>
<tr>
<td>Monthly</td>
<td>4%</td>
</tr>
<tr>
<td>Not prepared</td>
<td>35%</td>
</tr>
</tbody>
</table>

*EY Governance, risk and compliance survey 2015*
Global approaches to managing risk

Countries around the world have taken varying approaches to corporate governance and risk management. Some examples:

- In the US, the COSO framework lists 17 principles that organizations should follow.
- Companies with a premium listing on the London Stock Exchange must report how they have applied the UK Corporate Governance Code. In general, listed companies must “comply or explain” – in other words, they must clearly and meaningfully explain why they have chosen not to apply the Code in a given area.
- The European Commission has recommended a similar “comply or explain” regime across the EU.
- In Hong Kong, issuers are expected to comply with the Corporate Governance Code. Companies that deviate from the Code must give “considered reasons” in their annual report.
The evolving role of internal audit in risk management

A proactive and involved IA function can play an important role in the three lines of defense model: auditing governance processes and procedures; validating the monitoring being performed by second-line functions; and evaluating incentive metrics put in place across the business. IA also plays a key role in verifying that the efforts of the first and second lines are meeting the expectations of management and the board. Among other items, leading organizations should have IA evaluate:

- The alignment of risk management with the organization’s strategic objectives
- The view the organization is taking toward the nature and origin of risks – strategic, external or preventable
- Whether the organization has the means to identify and appropriately respond to emerging risks
- The organization’s governance processes

As the risk landscape changes and boards grapple with increasingly complex business environments, there is further opportunity for IA to better assist the board in its oversight role. Leading organizations and boards are asking IA to focus on key business processes and deliver more beyond enhancing internal controls and compliance and validation efforts. As leading boards increase their focus on monitoring company performance and creating more shareholder value, they are starting to better leverage the knowledge and expertise of the IA function to glean business and strategic insights to drive value creation.

According to Harvard Business Review, 86% of significant losses in market value are a result of strategic risk. IA should take this into account as they select their areas of focus and priorities.

By providing insights above and beyond the control environment, IA also can provide consolidated and comprehensive risk and management response reporting; use its knowledge of the organization to identify and report areas of potential operational improvement and upside risk potential; and provide insight on strategic priorities and risks on the front end. Boards can use the IA function to improve the linkage between risk and business performance, making sure that the organization accepts the appropriate level of risk to achieve its strategy.

As IA’s mandate expands and its scope shifts, the function may need to address the need for additional skills and adjust training to ensure it has the right competencies to meet changing expectations.

A proactive and involved IA function can play an important role in the three lines of defense model.

Top opportunities to enhance the way organizations manage risk:

1. Better alignment of risk objectives with business objectives
2. Clearer risk ownership processes and operating model
3. Improved ability to provide a comprehensive view of risk
4. More structured and frequent risk communications to key stakeholders and decision-makers within the organization
5. The more effective leveraging of technology across the organization to efficiently manage risk

*EY Governance, risk and compliance survey 2015*
Conclusion

Now more than ever before, today’s complex, evolving risk landscape requires boards to focus on the risks that matter to the organization. Leading organizations have adopted the three lines of defense model, or a suitable variant, to make sure that risks are appropriately covered and that the board has the necessary transparency into risk management across the organization.

IA plays a key role in the three lines model, and in verifying and validating that risks are appropriately and correctly categorized as strategic, preventable or external risks. IA can make sure the board is effectively informed about governance policies and procedures and regularly updated on the organization’s risk profile.

That puts the board in position to help create a risk-aware organization – one that advances strategic thinking, optimizes functions and processes and embeds solutions. By moving beyond its traditional role as a best-in-class assurance function, IA can serve the board’s needs as a trusted advisor, providing insights that give the organization the competitive edge.

Questions for the board to consider

- How aligned are your organization’s risk management activities to its strategic objectives?
- Has the organization correctly identified and assessed its strategic risks in the context of its risk appetite?
- What role do risk management professionals (e.g., chief risk officer, risk management staff, internal audit, compliance) play in the organization’s strategic planning process?
- Are IA activities aligned with the strategic objectives of the business?
- How can IA help the board understand the overall health of the internal control environment in the organization?
- Has the organization correctly identified and assessed the external risk landscape, and does it have appropriate mitigation plans in place?
- Is IA providing the board with a comprehensive, balanced assessment of the organization’s governance processes, including risk management?
- How are the company’s IA and risk functions leveraging big data and analytics to help the organization achieve its objectives?
- Does IA have the skill set to deal with the increased complexity presented by emerging risks?

Room to grow

As IA looks to build on its traditional strengths – moving from a best-in-class assurance function to a key role as a trusted advisor – here are five areas where it can extend its capabilities:

1. Enhance IA’s ability to identify and assess emerging risks
2. Better leverage the work of other risk, control and compliance functions
3. Enhance reporting to present findings in the context of risk to the enterprise
4. Maximize usage of technology to reduce costs and improve risk coverage
5. Increase the use of data analytics

EY Governance, risk and compliance survey 2015
Contacts

Ruby Sharma
EY Center for Board Matters
+1 212 773 0078
ruby.sharma@ey.com

Mark Manoff
EY Center for Board Matters
+1 212 773 1954
mark.manoff@ey.com

Ann Yerger
EY Center for Board Matters
+1 202 327 7697
ann.yerger@ey.com

Michael O’Leary
Global Internal Audit Leader
+1 312 879 4605
michael.oleary@ey.com

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters is committed to bringing together and engaging with boards, audit committee members and investors to exchange ideas and insights. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content and practical tools and analysis to boards, audit committees, institutional investors and others interested in governance topics.

©2015 Ernst & Young LLP.
All Rights Reserved.

EYG no. AU3510
CSG No. 1509-1641896
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

This publication and other EY board and audit committee resources are available online at ey.com/boardmatters.