Powerful Insights. Proven Delivery.®

Making Enterprise Risk Management Work for You

Jim DeLoach

protiviti®
Risk & Business Consulting.
Internal Audit.

Introduction

In June 2011, when Maurice Gilbert invited me to blog for Corporate Compliance Insights on topics germane to enterprise risk management (ERM), I accepted for several reasons. First, ERM is an enigma, with different executives having different views as to what it is. Therefore, it is not surprising that most attempts to implement ERM are rarely enterprisewide and applications of ERM are rarely integrated with strategy-setting. In some cases, ERM is viewed merely as a risk assessment – no more, no less. Second, there is no one-size-fits-all in implementing ERM, which makes it particularly challenging. Because ERM can't be implemented overnight, companies must evolve their thinking and tailor their implementation of ERM to their structure, strategy, culture and needs. Finally, only since the financial crisis have companies and their boards started to warm up to the idea of implementing some form of ERM. Before the crisis, ERM was viewed by many as a solution in search of a problem. Once the crisis occurred, the problem became clearer. Now boards are asking different and tougher questions, leading to a higher level of interest in ERM in the marketplace that has real substance as a process that informs the board's risk oversight.

So with Maurice's support, we've been providing monthly contributions for more than two years and counting. Now Maurice has invited us to publish a compilation, and once again we accepted. What you have here are the monthly columns we contributed to CCI from January to June of 2013.

In January, we discussed managing reputation risk. This is a high-end ERM objective, as a company's reputation management is inextricably linked with its risk management and crisis management. Effective identification and management of risk can identify major threats to reputation and ensure they are reduced to an acceptable level. Effective response plans and teams can minimize reputation damage when threatening events occur. Together, these disciplines are fundamental to managing reputation risk.

In February, we introduced 10 questions to provide a framework for executive management and boards of directors to take a fresh look at the organization's risk management process given

Jim DeLoach, a Managing Director with global consulting firm Protiviti, has 35 years' experience in governance, risk and compliance matters. He has advised and delivered numerous presentations on governance and risk management to hundreds of companies and groups in 30 countries. Since Protiviti's 2002 founding, DeLoach has authored over 260 thought leadership pieces on various aspects of governance and risk and served for eight years on the COSO Advisory Council. He writes ***The Bulletin and Board Perspectives: Risk Oversight****, Protiviti's publications on governance issues. DeLoach has written several books, including* ***Enterprise-wide Risk Management: Strategies for linking risk and opportunity****, the first book addressing ERM, and* ***Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements****, the most comprehensive treatment available about Sarbanes-Oxley Section 404 compliance. DeLoach is widely published and quoted in leading media. In 2011, he was named to* ***Consulting Magazine****'s Top 25 Consultants list. In 2012, he was named to the NACD Directorship 100 list.*

the speed of change in the business environment. Answers to these questions may provide insight on how the company can evaluate its ERM capabilities.

Our March column talked about paring down the company's risks to the ones that really matter. This is the crux of making ERM relevant in the C-suite. The context of the discussion is on identifying and communicating the critical enterprise risks to the board and the types of reports that would benefit executive management and the board as they engage in an ongoing dialogue about the organization's top risks.

In April, we reported on the results of a study Protiviti and North Carolina State University's ERM Initiative conducted among more than 200 C-suite executives and board members to obtain their views about the risks they believe are likely to affect their organization during 2013. The results suggested that executives and boards of directors can benefit from a periodic enterprise risk assessment to position their organizations to respond proactively to emerging risks that potentially impact their ability to deliver expected business performance.

In our May column, the discussion focused on the "tone of the organization," a term I like to use to broaden the usual focus on "tone at the top" to include the "tone in the middle" and "tone at the bottom." Because the top-down emphasis on ethical and responsible business behavior in an organization is only as strong as its weakest link, it is vital that the organization's tone at the top be translated into an effective tone in the middle before it can reach the rest of the organization. The tone of the organization is a vital enabler to ERM.

Finally, the June column focused on whether your compliance management is making a difference. Compliance is a major category of risks and the management of these risks is of concern in implementing ERM, particularly from a strategic standpoint. This article discussed the true cost of compliance, why managing compliance is a challenge and the key elements of an effective compliance program.

We thank Maurice and CCI for asking us to assemble this compilation and for the opportunity to connect with the readership of CCI each month. We hope that CCI readers obtain a few insights from this compilation that they can use to make a difference within their organizations.

These articles were first published at www.corporatecomplianceinsights.com

Managing Reputation Risk

From a risk oversight standpoint, a company's reputation management is inextricably linked with its risk management and crisis management. Effective identification and management of risk can identify major threats to reputation and ensure they are reduced to an acceptable level. Effective response plans and teams can minimize reputation damage when threatening events occur. Together, these two disciplines are fundamental to managing reputation risk.

The organization's culture sets the tone for protecting reputation. When organizational blind spots exist, causing executive management to miss warning signs that something is wrong or isn't working which objective parties can see easily from a mile away, reputation is clearly at risk. A reputation-preserving culture often encourages a strong control environment, a balanced incentive compensation structure, clear accountability for results, open communication, transparent reporting, continuous process improvement, and a strong commitment to ethical and responsible business behavior.

Reputation risk management begins with an effective risk assessment process. From a reputation standpoint, it is important to consider the following factors in addition to significance of impact and likelihood of occurrence: (a) velocity to impact once an event occurs, (b) persistence of the impact, and (c) resiliency of the company in responding to the event. These criteria help management identify threats to reputation.

A complicating factor in managing reputation risk is the boundaryless enterprise. Uncompensated risks sourced across the value chain can be sources of reputation risk. These risks require attention because they offer the potential for catastrophic events that have significant downside with little or no upside potential, and can cause severe damage to reputation. They include "stop-the-show" supply chain disruptions, mega warranty costs and/or product recalls, or headline-grabbing environmental, health and safety exposures. Lead content, toxic materials, impure ingredients and other inputs provided by suppliers that fail to meet specifications set by the laws and regulations to which a company is subject can damage that company's brand image and reputation.

For such significant uncompensated risks, prevention is the prescription. Effective due diligence when evaluating strategic suppliers, channel partners and M&A candidates can be time well spent.

With regard to opportunities for enhancing reputation, innovation can be vital. Organizations that are known for their differentiating strategies, distinctive products and brands, proprietary systems, and innovative processes are more likely to possess a strong, sustainable reputation. They also acquire, develop and retain the best people, providing the cornerstone for enhancing and protecting reputation.

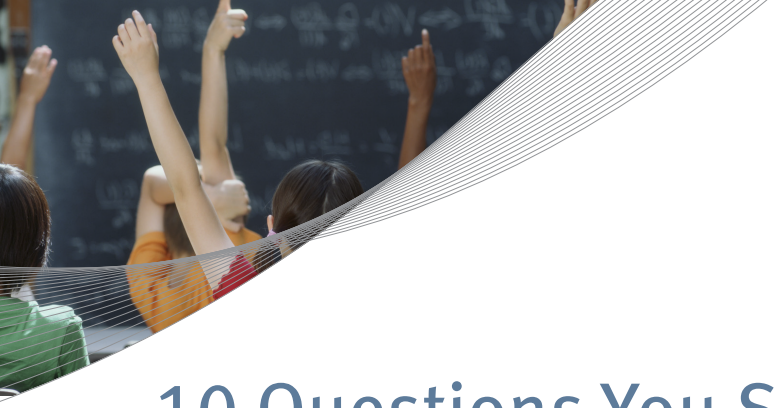
Often, reputation damage is a result of unmanaged risks. Strategic error and financial surprises can result in lost investor confidence. Significant operational issues can lose customers and market share. For example, quality failures and breakdowns as well as high-profile security breaches can severely affect reputation. Non-compliance with laws, regulations and/or contractual arrangements can result in penalties, fines, increased costs and lost revenue, calling into question the "tone at the top." For public companies, financial reporting is a highly visible compliance risk.

Crisis management is an integral component of effective reputation management. Rapid and effective response to sudden, unexpected events can enhance reputation, as astute observers know that even the most respected organizations can be tested. In a great many instances, it is not the event itself that impairs a company's reputation irreparably, but rather the quality of the company's response to that event following its occurrence. Accordingly, it is a management imperative to build a crisis management capability for

high-impact, high-velocity and high-persistence risks. A world-class response to a severe crisis is vital to the company's ultimate recovery from it, and is enabled by a crisis management plan updated and tested periodically by a designated crisis management team that is properly trained and supported by a communications plan pre-approved by legal.

In addition, the organization should have a clear view how it deploys the media to inform and educate the market and the industry. To that end, social media offers a new model for connecting with markets and customers and obtaining insights for improving processes and products. In today's environment, a company must be watchful for parties squatting on its brands or using them for nefarious purposes. Top-level domains, social network sites and news sites all are potential sources of online traffic where potentially damaging commentary on the company's products and services may exist. Companies must know how to use social media tools effectively in times of crisis.

First published January 23, 2013



10 Questions You Should Ask About Risk Management

Rapid change seems to be the order of the day, as the speed and complexity of business continue to increase. Technological advances such as cloud computing, mobile devices and social media continue to take hold. Regulatory demands continue to expand. Workforce dynamics continue to evolve. These and numerous other trends spawn new risks, altering risk profiles and exposing business models to disruptive change. Because of this dynamic environment, enterprise risk management should provide the discipline to ensure a fresh look at the organization's risk management capabilities from time to time.

Following are 10 questions for management and boards to consider:

1) ***What are the company's top risks, how severe is their impact and how likely are they to occur?*** – Managing enterprise risk at a strategic level requires focus, meaning generally emphasizing no more than five to 10 risks. Day-to-day risks are an ongoing operating responsibility.

2) ***How often does the company refresh its assessment of the top risks?*** – The enterprise wide risk assessment process should be responsive to change in the business environment. A robust process for identifying and prioritizing the critical enterprise risks, including emerging risks, is vital to an evergreen view of the top risks.

3) ***Who owns the top risks and is accountable for results, and to whom do they report?*** – Once the key risks are targeted, someone or some group, function or unit must own them. Gaps and overlaps in risk ownership should be minimized, if not eliminated.

4) ***How effective is the company in managing its top risks?*** – A robust process for managing and monitoring each of the critical enterprise risks is essential to successful risk management, and risk management capabilities must be improved continuously as the speed and complexity of business change.

5) ***Are there any organizational "blind spots" warranting attention?*** – Cultural issues and dysfunctional behavior can undermine the effectiveness of risk management and lead to inappropriate risk taking or the undermining of established policies and processes. For example, lack of transparency, conflicts of interest, a shoot-the-messenger environment and/or unbalanced compensation structures may encourage undesirable behavior and compromise the effectiveness of risk management.

6) ***Does the company understand the key assumptions underlying its strategy and align its competitive intelligence process to monitor external factors for changes that could alter those assumptions?*** – A company can fall so in love with its business model and strategy that it fails to recognize changing paradigms until it is too late. While no one knows for sure what will happen that could invalidate the company's strategic assumptions in the future, monitoring the validity of key assumptions over time as the business environment changes is a smart thing to do.

7) ***Does the company articulate its risk appetite and define risk tolerances for use in managing the business?*** – The risk appetite dialogue helps to bring balance to the conversation around which risks the enterprise should take, which risks it should avoid and the parameters within which it should operate going forward. The risk appetite statement is decomposed into risk tolerances to address the question, "How much variability are we willing to accept as we pursue a given business

objective?" For example, separate risk tolerances may be expressed differently for objectives relating to earnings variability, interest rate exposure, and the acquisition, development and retention of people.

8) ***Does the company's risk reporting provide management and the board information they need about the top risks and how they are managed?*** – Risk reporting starts with relevant information about the critical enterprise risks and how those risks are managed. Are there opportunities to enhance the risk reporting process to make it more effective and efficient? Is there a process for monitoring and reporting critical enterprise risks and emerging risks to executive management and the board?

9) ***Is the company prepared to respond to extreme events?*** – Does the company have response plans for unlikely extreme events? Has it prioritized its high-impact, low-likelihood risks in terms of their reputational effect, velocity to impact and persistence of impact, as well as the enterprise's response readiness?

10) ***Does the board have the requisite skill sets to provide effective risk oversight?*** – To provide input to executive management regarding critical risk issues on a timely basis, directors must understand the business and industry, as well as how the changing environment impacts the business model.

These 10 questions can provide a framework for taking a fresh look at the risk management process given changes in the business environment. The answers may provide insight on how the company can measure the success of its risk management capabilities.

First published February 18, 2013

These Top Risks Can Threaten A Company's Business Model

Of particular interest to executive management and the board of directors are normal and ongoing business management risks, emerging risks, and critical enterprise risks. In this column, we focus on the last category, which we define as the top five to 10 risks that can threaten the viability and/or execution of the company's strategy and business model. These risks should be a significant focal point for executive management and the board as they provide an important foundation for the board's risk oversight.

Paring down the company's risks to the ones that really matter is a test of the effectiveness of enterprise risk management. If the *risk assessment* process generates a laundry list of risks, it's "game over" in the C-suite and boardroom. What senior management and directors want to know is information about the risks that can make or break the company. It all starts with an appropriately designed risk assessment process based on the following principles:

- Periodically evaluate changes in the business environment to determine if they affect the critical assumptions underlying the corporate strategy (regarding such matters as technological innovation, competition, economic trends, regulation, etc.) and, when one or more assumptions are rendered invalid, ensure the corporate strategy is revisited in a timely manner.
- Consider an end-to-end view of the value chain when evaluating the most significant exposures to the effectiveness or viability of the business model in creating value for customers and delivering expected financial results. Consider the velocity or speed of an event to impact, the persistence of that impact over time, and the resiliency of the company in responding to the event creating the impact, in addition to considering the severity of the impact and likelihood of occurrence. Pay attention to the uncompensated risks the company faces across the value chain, e.g., the risk of significant warranty costs and/or product recalls, or environmental, health and safety exposures.
- Ensure the risk assessment process provides insight, promotes debate and adds to the collective understanding of what is really important for the business to be successful. Focus on identifying significant changes in the enterprise's risk profile, with emphasis on identifying emerging risks and worst-case extreme events, along with appropriate response plans to such scenarios, on a timely basis.
- Involve the board in a timely manner in decisions involving the acquisition of new businesses, entry into new markets, introductions of new products or significant alterations of the corporate strategy.
- Review the risk assessments over the last three to five years and evaluate their effectiveness against actual experience.

To illustrate, one consumer products company filters its risks down to the vital few through a risk assessment process that considers velocity and persistence of impact in addition to significance of impact and likelihood of occurrence. Also, the assessment process focuses on upstream supply chain issues and on protecting the company's brands. The risk assessment criteria are considered by various risk sub-committees that identify potential critical risks and provide input regarding such risks to the corporate risk management committee. Meanwhile, the operating units and corporate functions report critical risks (as well as emerging risks) to the strategic planning function. Based on their respective assessments using the inputs they receive, the corporate risk

management committee and strategic planning function provide input on the critical risks to executive management which, in turn, reports "The Top Risks List" to the board. The company's chief risk officer supports the process at all points. For example, he consolidates all potential critical risks identified by the individual risk subcommittees and submits a summary to the corporate risk management committee membership prior to the next scheduled committee meeting.

While management is responsible for addressing the critical enterprise risks, the board should consider the information it needs to understand them. Both might benefit from the following reporting:

- High-level summary of the critical risks for the enterprise as a whole and its operating units and the reasons why they are critical
- Status of risk mitigation efforts, with input from the executives responsible for managing the risks, including significant gaps in capabilities for managing the risks and status of initiatives to address those gaps
- The effect of changes in the environment on core assumptions underlying the company's strategy
- Scenario analyses evaluating the effect of changes in key external variables impacting the organization
- Changes in the overall assessment of risk over time
- Reliability and value added of prior risk assessments

The above information is illustrative and is not intended to be exhaustive or applicable to every organization. Reporting to executive management and the board is an iterative process and is fine-tuned over time.

First published March 27, 2013

Executive Perspectives on Top Risks for 2013

The first question most organizations seek to answer in risk management is, "What are our most critical risks?" Given that management's answer to this question lays the foundation for formulating responses with appropriate capabilities for managing the risks, Protiviti and North Carolina State University's ERM Initiative recently surveyed more than 200 business executives to obtain their views about what risks they believe are likely to affect their organization over the next 12 months.

This survey provides insights across different sizes of companies and across multiple industry groups as to what the key risks are for 2013 based on the input of the participating executives. The respondent group of over 200 board members and C-suite executives provided their perspectives about the potential impact of 20 specific risks across three dimensions:

- ***Macroeconomic risks*** likely to affect their organization's growth opportunities over the next 12 months
- ***Strategic risks*** the organization faces that may affect the validity of its strategy for pursuing growth opportunities over the next 12 months
- ***Operational risks*** that might affect key operations of the organization in executing its strategy over the next 12 months

Each respondent was asked to rate 20 individual risk issues using a 10-point scale, where a score of 1 reflects "No Impact at All" and a score of 10 reflects "Extensive Impact" to their organization over the next year. Also, the respondents were given an opportunity to identify other risks.

There were several notable findings in this study:

- Executives are significantly concerned about the magnitude and severity of risks that could affect the achievement of profitability or funding goals over the next year. Overall, two risks stand out as being of the highest concern across most industries, all types and sizes of organizations, and all types of respondents.

The first risk relates to profitability constraints due to overall economic conditions that could limit growth opportunities. That the responding directors and executives rated this risk as high as they did suggests that many of them are finding organic growth at acceptable levels harder to achieve in the current business environment. By inference, we can surmise that most management teams prefer a business environment in which they are able to grow organically so they can hire and invest with confidence. In periods of decline or slow growth, it is harder to remain profitable and can even be dangerous for highly leveraged companies. It also bears noting that this rating from the survey participants is consistent with the economic megatrends we are currently experiencing in many countries.

The second risk relates to concerns about the potential for regulatory changes and heightened regulatory scrutiny that will affect how products and services will be produced and delivered. This one is not a surprise as it is a factor is virtually every industry.

- In addition to concerns about the economy and regulatory change, the third "Significant Impact" risk relates to growth opportunities being restricted by uncertainty surrounding political leadership in national and international markets.
- Other top risks, while not perceived as having a "Significant Impact" overall, include risks related to succession planning and attracting/retaining top talent; anticipated volatility in global financial markets; and cyber threats, privacy, identity management, and other

Executive Perspectives on Top Risks for 2013

The first question most organizations seek to answer in risk management is, "What are our most critical risks?" Given that management's answer to this question lays the foundation for formulating responses with appropriate capabilities for managing the risks, Protiviti and North Carolina State University's ERM Initiative recently surveyed more than 200 business executives to obtain their views about what risks they believe are likely to affect their organization over the next 12 months.

This survey provides insights across different sizes of companies and across multiple industry groups as to what the key risks are for 2013 based on the input of the participating executives. The respondent group of over 200 board members and C-suite executives provided their perspectives about the potential impact of 20 specific risks across three dimensions:

- ***Macroeconomic risks*** likely to affect their organization's growth opportunities over the next 12 months
- ***Strategic risks*** the organization faces that may affect the validity of its strategy for pursuing growth opportunities over the next 12 months
- ***Operational risks*** that might affect key operations of the organization in executing its strategy over the next 12 months

Each respondent was asked to rate 20 individual risk issues using a 10-point scale, where a score of 1 reflects "No Impact at All" and a score of 10 reflects "Extensive Impact" to their organization over the next year. Also, the respondents were given an opportunity to identify other risks.

There were several notable findings in this study:

- Executives are significantly concerned about the magnitude and severity of risks that could affect the achievement of profitability or funding goals over the next year. Overall, two risks stand out as being of the highest concern across most industries, all types and sizes of organizations, and all types of respondents.

The first risk relates to profitability constraints due to overall economic conditions that could limit growth opportunities. That the responding directors and executives rated this risk as high as they did suggests that many of them are finding organic growth at acceptable levels harder to achieve in the current business environment. By inference, we can surmise that most management teams prefer a business environment in which they are able to grow organically so they can hire and invest with confidence. In periods of decline or slow growth, it is harder to remain profitable and can even be dangerous for highly leveraged companies. It also bears noting that this rating from the survey participants is consistent with the economic megatrends we are currently experiencing in many countries.

The second risk relates to concerns about the potential for regulatory changes and heightened regulatory scrutiny that will affect how products and services will be produced and delivered. This one is not a surprise as it is a factor is virtually every industry.

- In addition to concerns about the economy and regulatory change, the third "Significant Impact" risk relates to growth opportunities being restricted by uncertainty surrounding political leadership in national and international markets.
- Other top risks, while not perceived as having a "Significant Impact" overall, include risks related to succession planning and attracting/retaining top talent; anticipated volatility in global financial markets; and cyber threats, privacy, identity management, and other

information security and system protection risks. Rounding out the top 10 list of risks are organization resiliency to change, and ability to meet the performance expectations required to compete in the market.

A number of other insights about the overall risk environment for 2013 can be gleaned from this report:

- Consistent with the overall results, respondents across all industry groups rated the economy as having a significant impact over the coming year. Most industry groups also believe regulatory risk may significantly affect how they operate. Most industry groups identified three to four risks as having a "Significant Impact;" however, both the Financial Services and the Technology, Media, and Communications industry groups had the greatest number of "Significant Impact" risks.
- The most significant risks were macroeconomic and strategic in nature, suggesting the participants were more concerned with what they didn't know (uncertainties in the environment over the planning horizon) than with what they did know (such as operational risks).
- The largest organizations (those with revenues greater than $10 billion) view a greater number of risks to have, potentially, a "Significant Impact" on them than do smaller organizations, perhaps reflecting their greater complexity and global reach.
- There is overall agreement in perspectives about risks across different types of respondents, with the exception of chief risk officers (CROs), who view more risks at a "Significant Impact" level. Perhaps not surprisingly, these same executives indicated the greatest likelihood that their organization will be investing more resources in risk management over the next year.
- When we analyzed the data by type of organization (publicly held, private, not-for-profit/government), fewer risks are considered as "Significant Impact" risks relative to our industry analysis. This suggests that differences in risk conditions are linked more to industry or size and less to type of organization.

Rarely has there been a greater need for transparency into the nature and magnitude of risks undertaken in executing an organization's corporate strategy than today. The above synopsis suggests that executives and boards of directors can benefit from a periodic enterprise risk assessment to best position their organizations for a proactive versus reactive response to emerging risks that potentially impact their ability to achieve profitability and funding objectives. To that end, the risk assessment should be integrated with the strategy setting and business planning processes.

First published April 26, 2013

Focus on the "Tone of the Organization"

"Tone at the top" is an often-used term to describe how an organization's leadership creates an environment that fosters ethical and responsible business behavior. While tone at the top is important and a vital foundation, is it enough?

The reality is that when leaders communicate the organization's vision, mission, core values and commitment to appropriate ethical behavior, what really drives the culture and resonates with the organization's employees is what they see and hear every day from the managers to whom they report. If the behavior of middle managers contradicts the messaging and values conveyed from the top, it won't take long for lower-level employees to notice. Because the top-down emphasis on ethical and responsible business behavior in an organization is only as strong as its weakest link, it is vital that the organization's tone at the top be translated into an effective tone in the middle before it can reach the rest of the organization.*[1]*

Three dynamics drive this collective culture, or the "tone of the organization":

1) ***Don't assume that both tone in the middle and tone at the bottom are aligned with the tone at the top***. Alignment is the name of the game. The greater the number of layers of management in the organization, the greater the risk of incongruities in the respective tones at the top, middle and bottom, and likewise, the greater the risk of executive management being unaware of serious financial, operational and compliance risks that may be common knowledge to one or more middle managers and rank-and-file employees. Further, information is often distorted as it moves up the management chain, creating disconnected leaders.*[2]*

2) ***Don't assume everyone is engaged***. The extent of engagement is vital to building a strong, ethical culture. A lack of engagement drives absenteeism, turnover, fraud, misappropriation of assets, safety incidents, quality defects and loss of customer focus.*[3]*

3) ***Recognize the stakes: Many financial, operational and compliance risks are embedded in the organization's processes***. Many decisions are made and actions are undertaken on the front lines by middle managers and their teams, not by executive management. The decisions to act or not to act present opportunities for excellence as well as the potential to undermine the organization. To the extent these actions result in policy violations and significant omissions, they present risks in a wide variety of areas, such as product or environmental liability, health and safety, trading, employee retention, or security and privacy concerns. Risks can fester and smolder when repeated errors and omissions occur within processes, creating potential for significant surprises later.

To address these "tone of the organization" dynamics, executive management and directors should:

- ***Make every effort to implement a strong tone at the top***. Without this starting point, it's game over. Be aware of inappropriate performance pressures, a myopic short-term focus on profitability or a "fear of the boss" within the ranks. In certain areas of the organization, management may look the other way when people act inappropriately, especially when those individuals are valued rainmakers, rather than take fair and appropriate disciplinary action. Issues may exist even when executive management is of the view that a strong tone at the top exists.

- ***Ascertain whether the organizational structure supports or impedes the culture***. For example, flattening the organization may reduce the risk of executive management being unaware of risks embedded in the organization. On the other end of the spectrum, compensation arrangements may encourage inappropriate risk-taking behavior, e.g., competing metrics such as cost and schedule trumping safety.

- ***Consider conducting a periodic assessment of the tone in the middle and tone at the bottom***. Seek periodic independent assessments of the organization's culture and tone up and down the organization to affirm the belief system driving behavior. Address any lack of alignment with leadership.
- ***Ensure the organization has effective escalation processes***. A survey by the Ethics Resource Center noted the percentage of an organization's employees who witnessed misconduct at work was 45 percent in 2011, down from 49 percent in 2009. Of those employees, 65 percent reported the misconduct they saw, up from 63 percent in 2009. While the rate of escalation is moving in a positive direction, there is still room for improvement.*[4]*
- ***Act on the warning signs in audit reports***. Internal audit can play a key role in monitoring the tone of the organization, either as part of a comprehensive assessment or through aggregating relevant findings from multiple audits in different areas. Incongruities among the tones at the top, in the middle and at the bottom may warrant internal training initiatives and communications that reaffirms the organization's core values and beliefs.
- Is the board alert for warning signs that the tone at the top may not be optimal, e.g., turnover of key executives, tolerance of significant control issues, a warrior culture, a short-sighted focus on profitability, and/or evidence of an overly dominant chief executive?
- Does executive management work closely with middle-line and functional managers to ensure everyone is effectively aligned in terms of the organization's vision, mission, core values and strategy, so that the right messaging and behavior is stressed across the organization?
- Are there effective escalation processes to ensure significant problems are recognized and addressed at the appropriate level of the organization?

First published May 23, 2013

---

[1] "Managers and Ethics: The Importance of 'Tone in the Middle,'" Gael O'Brien, Business Ethics, February 2012.

[2] "Boards Should Monitor the Tone at the Bottom", Dr. Larry Taylor, NACD Directorship, October/November 2011.

[3] The Coming Job Wars, Jim Clifton, 2012.

[4] 2011 National Business Ethics Survey®, published by Ethics Resource Center, *http://www.ethics.org*.

Is Your Compliance Management Making a Difference?

Compliance management consists of the organization's policies and processes for adhering to applicable laws and regulations. Effective compliance management can inform the enterprise risk management process of the most significant compliance risks. For example, corruption risk is often a critical issue for a multinational.

To be effective, compliance management requires metrics, measures and monitoring that provide assurance to executive management and the board that established policies and procedures for fostering compliance are performing as intended. Without effective management of the compliance risks that really matter, the organization is reactive, at best, and noncompliant, at worst.

For many companies, complex accountabilities for compliance have evolved in an *ad hoc* manner over a long time. As new policies and procedures have evolved and are added onto the existing management structure, several elements of compliance management common to many companies have emerged – fragmented control environments, unnecessary and often redundant infrastructures, lack of automation, redundant requests of process and risk owners, reduced organizational transparency, inefficient communications, and high audit costs. Accepting these elements as mere *status quo* comes with a cost, as it can contribute to an ineffective and inefficient control structure.

The true cost of compliance consists of three elements – (1) the cost of internal compliance efforts, both specifically identifiable in various functions and embedded within processes, (2) the cost of oversight at all levels of the organization, and (3) the cost of noncompliance, e.g., fines, penalties, lost revenues and loss of brand equity, among other things. If management were to undertake a quality focus on managing compliance with the same passion with which it attacks the improvement of core operating processes, costs can be reduced in specific areas as confidence is gained that compliance risks are effectively managed.

There are several key elements of an effective compliance program for executive management and boards to consider:

- ***Board oversight***: Proactive understanding of potentially significant compliance risks and oversight of relevant compliance programs by the board or one of its standing committees help to establish an effective tone at the top.
- ***Executive management supervision***: Coordination and management of the compliance program by a designated senior executive are vital for organizations with complex, diverse operations.
- ***Policies, standards, procedures and reporting mechanisms***: These elements should be documented and up-to-date in critical areas and communicated to employees across the organization.
- ***Risk assessment and due diligence activities***: The risk identification process should include explicit consideration of compliance risks. Appropriate subject-matter experts should be accountable for monitoring changes to the regulatory environment continuously and identifying modifications required in the compliance risk area(s) for which they are responsible. The organization should exercise appropriate due diligence with respect to acquisitions, new employees, joint-venture partners and third-party agents to ensure they have the necessary background, resources and experience to discharge their assigned responsibilities. Appropriate compliance language and representations should be incorporated into third-party contracts.

- ***Effective internal controls and monitoring***: There are many compliance areas with reputational impact. Effective internal control over financial reporting is critical. So are environmental, health and safety issues; security and privacy matters; FDA compliance; anti-money laundering; and other compliance domains, depending on the industry. Due to the nature of compliance being managed in silos by different groups, it is important that gaps and overlaps be avoided. Periodic audits of compliance program policies, procedures and controls to assess their effectiveness at ensuring compliance at all levels and across the organization provide welcome assurance to executive management and the board. Significant areas of noncompliance and recommended solutions to enhance compliance should be reported to senior management and the board.
- ***Training and awareness programs***: Compliance awareness education for employees, third-party agents and consultants conducting business on behalf of the organization both in and out of the home country should ensure everyone is knowledgeable of the appropriate behavior, legal requirements and company policies.
- ***Investigatory and disciplinary mechanisms***: Thorough investigation and remediation of reported potential compliance violations are necessary to establish the appropriate discipline. Disciplinary mechanisms that are consistently enforced for those who violate compliance policy send an important message.

In summary, companies should ensure that established policies and procedures provide reasonable assurance that the organization is adhering to the requirements of applicable laws and regulations as well as internal policies. While not intended as a one-size-fits-all, the above elements provide evidence of due care and can help lay the foundation for an effective compliance program.

Key Questions to Consider:

- Is the board satisfied with its understanding of the enterprise's significant compliance risks and its oversight of relevant compliance programs, whether through activities of the full board or by one or more of its standing committees?
- Do the board and senior management have a shared view as to whether the organization's culture fosters open communication and transparency regarding compliance issues? Are there periodic compliance risk assessments and, if so, do they impact business plans and decisions? Is it clear who is responsible for the most critical compliance areas?
- Are the board and senior management confident that compliance management is operating efficiently and effectively such that duplicate efforts have been eliminated and the use of technology maximized?

First published June 18, 2013

protiviti®
Risk & Business Consulting.
Internal Audit.