ISSUE 88

protiviti®
Face the Future with Confidence

Board Perspectives:
Risk Oversight

The Four C's in Overseeing Internal Audit

> *We've always believed that boards should ensure that their organizations maximize the full potential of internal audit. There are four C's directors should consider when evaluating the sufficiency of any risk-based audit plan: culture, competitiveness, compliance and cybersecurity.*

In 2016, The Institute of Internal Auditors (The IIA) and Protiviti conducted the world's largest ongoing study of the internal audit profession — the Global Internal Audit Common Body of Knowledge (CBOK) — to ascertain expectations from key stakeholders, including board members, regarding internal audit performance. There were several imperatives for internal audit gleaned from the directors who participated in the study — among them: focus more on strategic risks, think beyond the scope of the audit plan, and add more value through consulting.

Key Considerations

As we reflect on directors' expectations from both the CBOK study and our own experience working with boards, we see several opportunities for internal audit:

- Watch for signs of a deteriorating risk culture.
- Approach the work of internal audit with a strong business context that addresses the underpinnings of what makes an organization competitive in the marketplace. Chief audit executives (CAEs) and their staff should "connect the dots" when considering the findings of multiple audits, particularly findings that could lead to opportunities for improving the efficiency and effectiveness of the operating model.
- Broaden the focus of the audit plan on important compliance matters and the quality of related reporting.
- Focus on risks of major importance; for many companies, cybersecurity is currently center stage.

These four C's — culture, competitiveness, compliance and cybersecurity — offer suggestions to directors regarding what they should expect from a risk-based audit plan. Here's a closer look:

CULTURE

Executives and directors understand that a breakdown in risk management, internal control or compliance is almost always due to a dysfunctional culture. They also know that cultural dysfunction doesn't develop overnight. The risks it spawns often require a lengthy incubation period before noticeable symptoms appear — and lead to inevitable consequences that could result, potentially, in a reputation-damaging event.

Examples of dysfunctional culture include an environment that isolates senior leaders from business realities, allows cost and schedule concerns to override legitimate public safety priorities, empowers falsification of emission reports, or drives unacceptable risk-taking through inappropriate performance incentives. Once the culture is shaped in such a way as to enable these types of environments, it may take a long time for their consequences to emerge. But emerge they will, if the dysfunction is left unaddressed. And what happens every time serious consequences finally emerge? Everyone runs for cover.

An organization's culture is much more than a commitment to ethical and responsible business behavior. It is the mix of shared values, attitudes and patterns of behavior that give the organization its particular character. In addition to corporate value statements, codes of conduct and ethics programs, culture related to risk management is influenced by established policies and procedures, risk committee oversight activities, incentive programs, risk assessment processes, key risk indicator reporting and performance reviews, and reinforcement processes, among other things. It also includes the risk appetite dialogue of the executive team and board, as well as the decomposition of risk appetite into risk tolerances and limit structures used daily in executing the corporate strategy.

So, how does a board get its arms around culture? How do directors and executives know when cultural dysfunction exists? Most important, how do boards nip cultural dysfunction in the bud before it may be *too* late?

An opportunity we see is for directors to look to the CAE as the independent "eyes and ears" with respect to the organization's culture. Specifically, internal audit can be asked to understand the overall working environment; identify the unwritten norms and rules governing employee interactions and workplace practices; highlight possible barriers to an effective internal control environment and communication flow; report unacceptable behaviors, decisions and attitudes toward taking and managing risk; and make recommendations to address identified problems.

Internal audit can post warning signs suggesting a need for further investigation (e.g., unrealistic performance metrics that encourage risk-taking to hit short-term targets, complex and unclear legal/reporting structures, poorly executed takeovers that allow "pockets" of bad behavior to thrive, lack of financial discipline, and employees constantly on edge because they fear being fired). Internal audit can assist in assessing whether the tone in the middle and at the bottom match the leaders' perceptions of the tone at the top. This contrast can be quite revealing and a powerful reality check to a management team who really wants to listen.

COMPETITIVENESS

This area poses an opportunity for internal audit to improve operating efficiency and effectiveness when the company has business processes that are not performing at a competitive level because practices are inferior relative to competitors or best-of-class performers. In essence, the board should expect internal audit to look beyond traditional compliance areas and financial reporting to help the organization continuously improve its operations.

Most organizations use some form of a balanced scorecard when monitoring whether they are successfully establishing and sustaining competitive advantage in the marketplace. Key performance indicators address critical areas, such as quality, time, cost and innovation performance. They often include indicators of customer and employee satisfaction. Internal audit can assist with assessing the reliability of these metrics for decision-making. In addition, internal audit can benchmark selected metrics against competitors and best-in-class performers to identify performance gaps that must be corrected in a timely manner.

COMPLIANCE

Traditionally, the internal audit plan deals with ensuring that important areas related to the organization's compliance with laws, regulations and internal policies are under control. As the third line of defense, internal audit should ascertain whether:

1. Front-line operators and functional leaders whose activities have significant compliance implications (first line of defense) own the responsibility for identifying and managing compliance risk and have effective controls in place to reduce the risk of noncompliance to an acceptable level.
2. The scope of the independent compliance function (second line of defense) is commensurate with the significance of the company's compliance issues and results in reliable and timely insights to management and primary risk owners.

Regardless of whether there is a compliance function, internal audit can determine whether a cost-effective monitoring process is in place to address the top compliance risks. It also can assess the overall implementation of the compliance program, as well as periodic updates of the program in light of changes in applicable laws and regulations and the company's needs.

CYBERSECURITY

This area continues to be a significant concern to boards, and it's not going away any time soon. In a recent survey, cybersecurity was cited as the third most critical uncertainty companies are facing as they look forward into 2017.[1] Internal audit can assist boards in this area in several ways.

First, internal audit can assess whether the company's processes give adequate attention to high-value information and information systems. Rather than all-systems-are-equal protection measures resulting in unnecessary costs and lack of attention to the information assets that really matter, internal audit can assess whether the IT organization and business leaders agree on what constitutes the company's "crown jewels." This evaluation includes identifying the organization's most critical data and information assets and information systems, and understanding why they are of highest value, what the company cannot afford to lose and who is authorized to access these vital assets.

Second, internal audit can assist the board and senior management with understanding the threat landscape. Management should assess the organization's cybersecurity risks based on the company's crown jewels, the nature of the company's industry and operations, and the company's visibility as a potential target. For example: Who are the likely adversaries? How are they likely to attack? Where are our biggest vulnerabilities? How effective are our current internal controls? Do we conduct penetration testing and, if so, what are the results? Answers to these and other questions help to clarify the changing threat landscape.

Finally, internal audit can assess the organization's response readiness to a cyber incident. The question here is whether the company has an effective incident response plan in place. The underlying assumption of a cyberattack being a relatively low-likelihood incident has given way to the realization that such attacks are not just *high*-likelihood incidents but actually inevitable. Therefore, effective incident response processes are critical to a company's preparedness to reduce an attack's impact and proliferation.

Internal audit can assist with evaluating incident response plans to ascertain whether strategies for reducing the risk of security incidents to an acceptable level are proportionate and targeted; the organization is being proactive in periodically testing the incident response plan to determine its effectiveness; and the plan is complemented by procedures that provide direction as to what actions to take in response to specific types of incidents.

In summary, by focusing more broadly on the implications of audit findings and thinking beyond the expressed or implied boundaries set by the audit plan, internal audit is better positioned to deliver stronger, more practical and harder-hitting recommendations aligned with what directors are seeking. The four C's provide perspective as to the areas where boards should be looking.

[1] *Executive Perspectives on Top Risks for 2017*, Protiviti and North Carolina State University's ERM Initiative, available at www.protiviti.com/TopRisks.

Questions for Boards

Following are suggested questions that boards of directors may consider in the context of the nature of the entity's risks inherent in its operations:

- Are directors satisfied with the scope of internal audit's activities in view of changes in the business environment and the company's operations? Is the board getting the assurances it needs from internal audit in the appropriate areas?
- Does the CAE provide insight to the board and executive management on potential blind spots and other issues with respect to the organization's culture?
- Does the internal audit plan allocate sufficient resources to address key areas of emphasis in competitiveness, compliance and cybersecurity?

How Protiviti Can Help

Protiviti is a global leader in providing comprehensive internal audit services. We work with audit executives, management and audit committees at companies of virtually any size, public or private, to assist them with their internal audit requirements. This can include starting and running the activity for them on a fully outsourced basis or working with an existing internal audit function to supplement its team when it lacks adequate staff or skills. Our service offerings support our clients' focus on the four areas discussed in this article.

The Board Institute Launches New Board Risk Oversight Evaluation Tool

The TBI Protiviti Board Risk Oversight Meter™ provides boards with an opportunity to refresh their risk oversight process to ensure it's focused sharply on the opportunities and risks that truly matter. Protiviti's commitment to facilitating continuous process improvement to enable companies to confidently face the future is why we collaborated with The Board Institute, Inc. (TBI) to offer the director community a flexible, cost-effective tool that assists boards in their periodic self-evaluation of the board's risk oversight and mirrors the way many directors prefer to conduct self-evaluations. Boards interested in using this evaluation tool should visit the TBI website at http://theboardinstitute.com/board-risk-meter/.

Learn more at
www.protiviti.com/boardriskoversightmeter

Protiviti partners with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on https://blog.nacdonline.org/author/jdeloach/. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* are consolidated into a printed booklet that is co-branded with NACD. Protiviti also posts these articles at protiviti.com.

protiviti®