Board Perspectives: Risk Oversight

Is Your Compliance Management Making a Difference?

Issue 35

Compliance management consists of an organization's processes for adhering to laws, regulations and internal policies. To be effective, it requires metrics, measures and monitoring that provide assurance to 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.

Key Considerations

For many companies, as new policies and procedures have evolved and are added onto the existing management structure, several elements of compliance management common to many organizations 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 they can contribute to an ineffective and inefficient control structure.

The true cost of compliance consists of (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 undertakes a quality focus on managing compliance with the same passion with which it attacks improving 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 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 helps 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 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 responsibilities. Appropriate compliance language and representations should be incorporated in third-party contracts.

- **Effective internal controls and monitoring:** There are many compliance areas with reputational impact. Effective internal control over financial reporting is critical, as 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 assurance to executive management and the board. In addition, significant areas of noncompliance and recommended solutions to enhance compliance should be reported.
- **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 that everyone is knowledgeable about the appropriate behavior, legal requirements and company policies.
- **Investigatory and disciplinary mechanisms:** Thorough investigation and remediation of reported 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 and 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.

Questions for Directors

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

- 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?
- Is the board satisfied that the organization's culture fosters open communication and transparency regarding compliance issues? Are there periodic compliance risk assessments that impact business plans and decisions? Is it clear who is responsible for the most critical compliance areas?

How Protiviti Can Help

Protiviti takes a holistic enterprise view to assist boards and executive management with developing, implementing and maintaining effective regulatory compliance programs that maximize the benefits of their investment and protect their reputations.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

protiviti®
Risk & Business Consulting.
Internal Audit.