Wolters Kluwer

CT
ESSENTIAL COMPLIANCE INSIGHTS

CORPORATE RISK MANAGEMENT: 4 KEY FOCUS AREAS

"...the rising volume of legal and regulatory risks has forced companies to change tactics, as investors, government agencies and the public are demanding improved methods of handling risk management."

Traditionally, corporations and legal departments have taken a bottom-up approach when implementing risk management strategies. They seek to minimize damage to company assets once the threat materializes, while allowing other risks to remain undetected and unaddressed. But the rising volume of legal and regulatory risks has forced companies to change tactics, as investors, government agencies and the public are demanding improved methods of handling risk management. Here are four key focus areas that corporations should consider when evaluating their current risk management program.

ORGANIZATION & ACCOUNTABILITY: WHO OWNS RISK MANAGEMENT?

While many companies have departments dedicated to managing and mitigating risk, the responsibility needs to also be shared throughout the organization. A recent article by the Harvard Law School Forum on Corporate Governance and Financial Regulations states that the board should provide "risk oversight", while leaving the development and execution of the risk management policies to senior executives and risk managers. The board should set the tone in viewing risk management as an integral part to how a company performs business and operates internally. It should clearly outline the duties performed by key officers in order to prevent inefficiencies in process and to eliminate confusion regarding specific roles and responsibilities.

In some situations, it is up to executive management to facilitate strong collaboration between stakeholders, including counsel and compliance managers, in order to avoid conflict and the possibility of overlooking risk areas.

CYBERSECURITY

Cybersecurity concerns have brought a sense of urgency to data (or information) security compliance for companies. After several recent, high-profile data breaches affecting multinational corporations, companies have faced increased scrutiny from the government and global consumers on how to handle cybersecurity. The fallout from these incursions can extends beyond the company's bottom line, with some organizations viewing the loss of reputation as equally damaging.

Corporations must develop and implement data security policies and cyber-attack action plans according to best practices for what many experts are seeing as an eventual, rather than potential, occurrence. Companies should also consider information system management controls and third-party auditing of control objectives as part of risk management protocols.

The implementation of continuous monitoring of cybersecurity controls; development and deployment of a prevention, detection, and response plan; and the creation of written policies and procedures will allow companies to mitigate the risks of data breaches.

GLOBAL COLLABORATION AND MANAGEMENT

Global expansion for a company means having to deal with additional risks. When engaging in business operations on a global scale, companies must pay close attention to the sometimes thorny ways in which international laws can affect doing business. They must also keep up-to-date with the latest developments in compliance. One example to help illustrate this complexity is the handling of global management of entity data, with the knowledge that data laws vary from country to country.

Companies must rely on teams who understand the nuances of federal and international regulations, as well as have the ability to maintain productive sustainable relationships between these teams across all jurisdictions. By recognizing and taking the appropriate actions to deal with coverage and competency issues with their teams, companies can put in place comprehensive risk management policies and procedures that can be adhered to by legal counsel and employees.

BUSINESS ETHICS

Business ethics is another area that is receiving increasing domestic and international government scrutiny. Compliance failure can lead to lengthy investigations, legal action, and civil and criminal liability. Corruption, conflicts of interest, and antitrust issues are some of the risks that must be assessed in an objective manner.

Corporate counsel, however, may find it difficult to reconcile the desires for company success with its ethical obligations. The solution is to adopt a top-down approach for business ethics where senior management provides structural support to in-house counsel. This facilitates a more effective handling of potential ethical conflicts. Compliance standards and ethics policies should be communicated to all employees. Senior management must cultivate an environment where employees do not fear reprisals for reporting ethical issues. The fostering of accountability leads to better corporate risk management.

CONCLUSION

Senior management, general counsel and board members need to recognize key risk areas in order to develop policies and programs that are comprehensive, flexible, and easily deployed throughout an organization. Strong and active leadership and oversight can determine the success of a company's risk management program.

"When engaging in business operations on a global scale, companies must pay close attention to the sometimes thorny ways in which international laws can affect doing business."

LEARN MORE

To learn more about how CT can help you better manage your legal service needs, contact a CT representative at 844-206-9033 (toll-free US).

Related services:

Entity Management Services

Global Corporate Services

Service of Process workflow customization

Business License Managed Services

Annual Reports Managed Services

Global Managed Services

Join the conversation. Follow us on Twitter, LinkedIn, Google+ and Facebook.