NOVEMBER BLOG

WMH ADVISORS
GROOM. GROW. GOVERN.

Written By: Wendy Morton-Huddleston

November 4th, 2024

NEW TO THE BOARDROOM:
Think Strategically About Risk Governance

As a new Board Director learn to view risks holistically and with an oversight lens across the enterprise. Risk is defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as the possibility that events will occur and affect the achievement of strategy and business objectives.[1] Remember – it takes the board and management to foster a risk aware culture that promotes risk intelligence.

Lessons learned from cybersecurity threats, market volatility, environmental issues, and supply chain disruptions are real experiences that require intentional governance, diligence and proactive management and mitigation to minimize risk exposure and severity. Board members should actively request risk assessments from management to govern and help safeguard long-term value creation.

According to the National Association of Corporate Directors (NACD) Global Risks Are Intensifying: Here Is What Boards Should Know[2]

- *Adoption of digital technologies may require new skills that are in short supply requiring significant effort to upskill and reskill existing employees*
- *The rapid speed of disruptive innovation enabled by new and emerging technologies or other market forces may outpace the organization's ability to compete without significant changes to the business model*

These risk scenarios provide context regarding common business and market risks.

Risks	Scenerios
Technology	Cyber data breach, ransomware threats, data privacy compliance, intellectual property threats, automation bias, AI advancements, disruptive innovations, and ethics
Environmental	Penalties for non-compliance and pollution liabilities
Geopolitical	Political discord, tariffs, global regulatory requirements
Financial	Issues concerning, cash flow, capital, revenue, and profits
Market	Competitive pricing erosion and business model impacts
Operations	Supply chain disruptions, workforce attrition surges, safety, fraud, mergers & acquisitions, data governance, and public relations crises
Regulatory	Non-compliance with industry standards, regulations, legal and financial penalties, litigation, and sanctions
Strategic	Shifts in consumer behavior, economic conditions, product or service offerings, long-term sustainability, and reliance on third-party relationships

*representative risks not all inclusive

Risk Aware Questionnaire

When engaging with management or fellow board members consider these questions:

1. Has management developed a multi-year enterprise risk management planning process that incorporates risk considerations into core business decisions, aligned with strategic and business objectives?
2. Is there a designated leader responsible for the development and implementation of an enterprise risk management vision?
3. Are risks aligned to board committees for ongoing oversight and discussion?
4. Does the organization have a risk assessment in place, are accountable business unit practitioners assigned to risk issues, and how are the risks mitigated and monitored?
5. What control activities (policies and procedures) are codified to mitigate and monitor risk exposures?
6. Do executive dashboards exist that provide visibility into enterprise risk status and progress on risk mitigation efforts, enabling informed risk management decisions at the highest level?
7. Does management and the workforce have "Fit for Purpose" risk management competencies and knowledge of industry standards and best practices?

Frameworks

1. Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Compliance Risk Management.

- Provides guidance on the application of the framework to the identification, assessment and management of compliance risks

2. U.S. Department of Commerce National Institute of Standards and Technology (NIST) framework. The NIST Cybersecurity Framework (CSF) 2.0 offers a taxonomy of cybersecurity outcomes and resources on practices and controls.[3]

- Helps businesses to understand, manage, and reduce cybersecurity risks and protect their networks and data.

3. International Standards Organization (ISO) standards in security, safety, and risk management. ISO 31000 Risk Management provides a level of reassurance in economic resilience, professional reputation and environmental and safety outcomes.

- Guides organizations to protect people, assets and information across various sectors. Provides frameworks for managing risks, enhancing safety protocols, and ensuring resilience against threats.[4]

In conclusion, this is an excellent opportunity as a new board member to offer objectivity regarding emerging risks, disruptive global factors, and stay curious about the control environment, risks and exposure levels. As a valued board member, it is your responsibility to ask questions, broaden your risk competencies, understand how risks are assigned to board committees, and to cultivate trusted relationships across the enterprise to approach risk management as a team player to govern effectively.

1 Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Compliance Risk Management: Applying the COSO ERM Framework

2 National Association of Corporate Directors "Global Risks Are Intensifying: Here Is What Boards Should Know" by Jim DeLoach | February 1, 2024

3 The NIST Cybersecurity Framework (CSF) 2.0

4 International Standards Organization (ISO)