

# Boardroom Questions

## Why is Risk an issue in the Boardroom?



### Fortify your business: risk management should be embedded within the culture of the organization



Managing risk is not about compliance and box-ticking: it is a critical investment that can underpin an organization's long-term **growth, value and sustainability**

#### How robust are your policies on

- Governance
- Risk
- Compliance

#### Can you demonstrate

- Discipline
- Control
- Responsibility

**Past corporate failings have been attributed to lack of accountability, strategy and transparency**

### What types of risk may affect the business?



#### Business risk

- Misconduct and fraud risk
- Emerging technology and underlying algorithms
- Governance and compliance
- Talent and succession
- Third Party Risk
- Operational Risk



#### Reputation

- Cyber and information security
- Third-party risks including contract defaults or a collapsing business
- Crisis management and business continuity
- Reputational risk
- Instigator or defendant in a litigation case



#### Regulation

- Local and global regulation governing suppliers investment tax and shareholders
- Credit, market and liquidity risk
- Geopolitical drivers
- Anti bribery and corruption legislation
- Privacy (GDPR and other country privacy legislation)

### Potential benefits and consequences for an organization



#### Benefits of addressing risk

- Improved agility
- Creates a strong risk culture throughout the organization
- Allows for more effective reporting, processes and internal controls
- Helps minimize disruption
- Enables better business performance



#### Consequences of not addressing risk

- Possible reputational damage
- Long term growth potential
- Lost market opportunities
- Long term business sustainability
- Additional resources required to find replacement suppliers including due diligence

## Boardroom Questions



### Business risk

- Does our company's risk reporting provide management and the Board information we need about the **top risks and how they are managed**?
- To what extent has the Board issued **guidance for risk management**?
- Does the Board comprise a good **cross section** of professionals with the **right skills to assess risks** to the firm?
- What is our company's strategy to **manage ethics**?
- Are people in our firm equipped to recognize and resolve **moral dilemmas**?

### Reputation

- Is the company prepared to respond to **extreme events**?
- What is the current level and business impact of **cyber security** to our company? What is the plan to address identified risks?
- How comprehensive is our cyber **incident response plan**? How often is the plan tested?
- How do we monitor our systems and **prevent breaches**?
- Have we performed **due diligence on vendors, agents representatives** and other third parties?

### Regulation

- Are we under **any regulatory actions**?
- Do we have a **transaction monitoring system** or program to detect suspicious activity?
- Do we have a formal robust practice for addressing **regulatory change** and its corresponding impacts?
- Have we implemented a **reporting hotline** for internal and third parties to report concerns?

## What actions can the Board consider?



### Business risk

- Require management to complete a **full risk review** across our organization which includes prioritization of risk
- Develop a **formal process** to review risk. Require a formal written report from management
- Consider engaging **outside expertise** to drive or conduct an ERM review – experience at both risk identification, impact measurement and mitigation
- Make risk an **annual agenda item** – not part of a three-year strategic plan
- Full **active involvement** of Board members to participate in the process
- Hold **management accountable**. Require management to integrate risk management into core management processes across the organization
- Ask the **tough questions**
- Ensure the Board has a mixture of **the right skills** to address risk issues across an organization

## Contact us:



**Jitendra Sharma**  
Global Services Group Leader,  
Risk Consulting  
KPMG International  
Principal, Advisory  
KPMG in the US  
T: +1 212 872 7604  
E: [jitendrasharma@kpmg.com](mailto:jitendrasharma@kpmg.com)



**Click here**  
for more information  
[kpmg.com/risk-consulting](https://kpmg.com/risk-consulting)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.