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, often more prevalent when cash is tight from employees to suppliers
- Emerging technology and underlying algorithms
- Governance and compliance
- Talent and succession

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

Potential benefits and consequences if risk is not addressed by the organization

Benefits
- 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

Risks
- 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 risk and how they are managed**?
- To what extent has the Board issued **guidance for risk management**?
- 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 your cyber incident response plan? How often is the plan tested?
- How do you monitor your systems and prevent breaches?
- Have we performed **due diligence on vendors, agents representatives and other third parties**?

**Regulation**
- Have we implemented a reporting **hotline** for internal and third parties to report concerns?
- 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?

## What actions can the Board consider?

- **Require management to complete a full risk review across our organization**
- **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**

---

**About the KPMG Board Leadership Center**

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc

---

**Contact**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anne van Heerden</td>
<td>Partner, Head of Forensic</td>
<td>+41 58 249 28 61 <a href="mailto:annevanheerden@kpmg.com">annevanheerden@kpmg.com</a></td>
</tr>
<tr>
<td>Philippe Fleury</td>
<td>Partner, Financial Services</td>
<td>+41 58 249 37 53 <a href="mailto:pfleury@kpmg.com">pfleury@kpmg.com</a></td>
</tr>
<tr>
<td>Matthias Bossardt</td>
<td>Partner, Head Cyber Security and</td>
<td>+41 58 249 36 98 <a href="mailto:mbossardt@kpmg.com">mbossardt@kpmg.com</a></td>
</tr>
<tr>
<td></td>
<td>Technology Risk</td>
<td></td>
</tr>
</tbody>
</table>

---

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. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2021 KPMG AG, a Swiss corporation, is a subsidiary of KPMG Holding AG, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.