KPMG

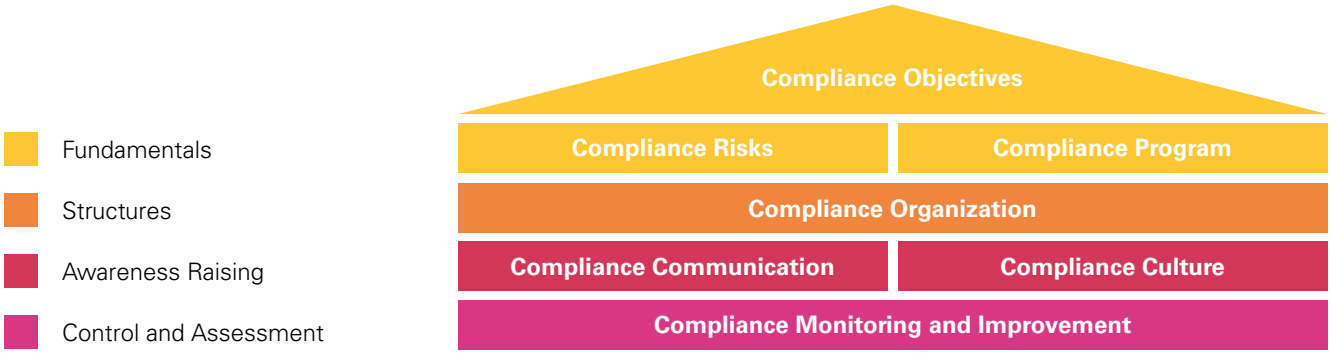
Boardroom Questions

Oversight of an organization's Compliance Management System

Guidance for the Board to achieve a reasonable and effective oversight of the organization's Compliance Management System.

An ineffective Compliance Management System (CMS) may lead to (personal) liability for those charged with governance, typically the Board of Directors. A systematic CMS and a clear understanding of commitment to compliance is required to meet legal obligations and the expectations of various stakeholders. How do those charged with governance execute a reasonable and effective oversight regarding the organization's CMS?

Common elements of a Compliance Management System (CMS)



Top takeaways for all Boards

- A CMS forms part of a company's risk management and is dedicated to those risks resulting from a possible breach of legally prescribed or voluntarily defined obligations ("compliance risks").
- A CMS requires a corresponding integration with existing governance systems such as the Risk Management System (RMS) or the Internal Control System (ICS).
- The "tone at/from the top" from the highest level of management is the most critical component of an effective CMS.

Considerations for the Board

- The Board needs to take very specific and proactive actions relative to its compliance oversight duties.
- The Board needs to set the right expectations and ask appropriate questions to gain a good understanding of the adequacy and effectiveness of the organization's compliance program.

Questions the Board should ask itself and its management team

Compliance objectives

- Do we have a clear understanding of compliance and its significance for the organization?
- Are we fulfilling the legal and regulatory requirements for our organizations and the requirements of our stakeholders?
- Do performance goals and incentives put unreasonable pressure on employees to act contrary to our compliance objectives?

Compliance risks

- Do we have a formal and regular process to identify ethics, compliance and reputational risks?
- Do we consistently monitor areas with an increased exposure to reduce risks to an acceptable level?

Compliance program

- Do we have a systematic and managed "internal house of policies"?
- Are the relevant corporate regulations sufficiently known to the corporate bodies and employees and do the latter have access to these regulations at all times?

Compliance organization

- Are the compliance roles and responsibilities adequately defined and documented?
- Is the compliance function sufficiently independent and does it have a direct reporting line to the Board?

Compliance communication

- Are the Board, management team and employees regularly trained in the area of compliance?
- Do the reports to the Board provide appropriate metrics, context and analysis of the organization's CMS?
- Is there an adequate reporting system in place to receive confidential or anonymous reports regarding misconduct and/or violations of legal requirements?

Compliance culture

- To what extent does the Board and management demonstrate their commitment to ethics and compliance?
- Do we hold our management (all levels) fully accountable for their compliance responsibilities?
- How consistent are we with discipline? Are, for example, top performers and senior staff held accountable for the code of conduct in the same way as other employees?

Compliance monitoring and improvement

- Is the effectiveness of the CMS reviewed regularly and expediently?
- Are any identified compliance flaws remedied in a timely, practical and sustainable manner?

What actions can the Board take?

Assessment

- Assessment of the current compliance risk situation
- Review of existing policies and policy management
- Interviews with internal key stakeholders
- Identification of the current roles and responsibilities
- Analysis of the processes and procedures for the implementation and enforcement of compliance
- Questionnaire amongst employees to understand their perception of compliance and the corporate culture

Evaluation

- Evaluation of the status quo and identification of any potential to leverage and integrate
- Establishment of an action plan to introduce a customized CMS or to appropriately adjust an existing CMS on the basis of strategic priorities

Action Plan

- Approval of a dedicated compliance strategy
- Alignment of the CMS with existing governance systems (RMS and ICS), including joint reporting
- Definition of control measures to continuously review the effectiveness of the CMS

Contact

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

kpmg.ch/blc

Anne van Heerden
Partner
Head of Forensic

+41 58 249 28 61
annevanheerden@kpmg.com

Jörg Kilchmann
Partner
Head of Legal

+41 58 249 35 73
jkilchmann@kpmg.com