An effective compliance infrastructure enables strong governance, robust risk identification and mitigation processes and accountability, along with a culture of compliance across all three lines of defense. The three lines of defense structure provides for allocated compliance responsibilities across the organization defining who will own and manage risk, regardless of the size and complexity of an organization. The roles and responsibilities across the three lines of defense are typically established as follows:

— The **first line of defense** (line of business management and operations) typically owns and manages risks and controls. It identifies key risks to the organization and implements ongoing processes, systems, and programs against defined standards that build and support a culture of integrity.

— The **second line of defense** (compliance function) monitors compliance risks and controls in support of management. The compliance function is responsible for driving the overall design and implementation of the organization’s compliance function, advising management and the Board, and assessing the effectiveness of the organization’s control environment to help ensure that the business is designing and implementing effective controls intended to mitigate risks.

— The **third line of defense** (Internal Audit function) provides assurance on the effectiveness of controls in place to mitigate risk.

Although neither senior management nor the Board is considered to be part of one of the three lines, these parties collectively have responsibilities for establishing an organization’s objectives, defining high-level strategies to achieve those objectives and establishing governance structures to better manage risk. Their engagement is critical for the success of the overall model and compliance program.

One challenge many CCOs face is how to further instill ownership in the first line of defense so that the business units “own” their compliance risks, monitor their risks, and assess their controls for risk mitigation. One means of doing so is to establish formalized documented roles and responsibilities for each line with respect to management of compliance risks as well as for specific employees. This helps to ensure a consistent understanding of the role each line plays in the control framework. In addition, this exercise can provide a valuable opportunity for all stakeholders to review the responsibilities, identify if there are any gaps in control assessments across the organization, and even reduce duplication in test work. Ongoing communication and coordination is also particularly important and valuable for the three lines of defense model to be effective and functional.

> “Everything is technically compliance, so it is essential for organizations to define the risk universe of compliance and what compliance should be doing and monitoring.”
> — Greg Catron, CCO, Humana

---

Contact us

Julie Gerlach
Managing Director, Advisory
Compliance Transformation Solution
National Co-leader
T: 404-222-3389
E: jgerlach@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 667321