Your compliance program:

What the new guidance from the Department of Justice could mean to you

Revised guidance issued by the DOJ aims to sharpen prosecutors' understanding of what works — and what doesn't — when evaluating a company's compliance program design, effectiveness, and application. The bar has been raised — there are a number of steps that your organisation can take now.

Compliance program excellence

Is your compliance program...

- **Well designed?**
- **Adequately resourced and empowered to function effectively?**
- **Working in practice?**

Elements of a compliance program

- Program governance and resources
- Risk assessment
- Policies and procedures
- Compliance controls
- Communication and training
- Enforcement, discipline, and incentives
- Investigations and response
- Monitoring and auditing

"Are you proud of how your program has evolved?"

If you had to explain your resourcing and structural choices today, **would you be able to backup your rationale? Could you demonstrate that your program has evolved with the risk?**

Key components to start thinking about now

Resource empowerment and effectiveness

Mentions the importance of being purposeful about focusing compliance resources on the **highest risk areas** to own as a central compliance function, and how compliance can **support the business** who functions as a **first line of defense** for most compliance risks.

Data-driven, effective compliance program and controls

Highlights that compliance and control personnel should have continuous **direct or indirect access to relevant sources of operational data and information across functions** to allow for **timely and effective monitoring and/or testing** of policies, controls, and transactions. Impediments that limit data access should be addressed.

Third party risk management

Clarifies that risk management of third parties should be **performed throughout the lifespan of the relationship**, not just during the onboarding process.

An effective compliance program guided by a robust framework protects and preserves the integrity of your business.

Compliance risks are typically owned by the business and the compliance function - Corporate Compliance Group (CCG) maintains oversight on certain risks. The illustrative wheel on the left depicts the risks for which CCG has different levels of ownership and/or oversight. The key below outlines expectations for each ownership level.

Ownership level	Expectation
Direct ownership	• CCG owns/ defines policies and procedures • CCG defines controls, which may be implemented centrally or at a regional/ business unit level • CCG defines and monitors metrics
Shared ownership/ significant oversight	• Risk owner defines policies and procedures in collaboration with CCG • Risk owner defines controls, CCG tests design and effectiveness of the controls on a periodic basis • CCG agrees with risk owners on metrics to be reported on a defined cadence (monthly)
Moderate oversight	• CCG agrees with risk owners on metrics to be reported on a defined cadence (at least quarterly)
Minimal oversight	• Only significant issues/ regulatory inquiries are escalated • Limited metrics may be reported on a defined cadence (annually)

Note: The risks may be further updated based on the ERM work being performed

Contact us:

Michael Peer
Partner
michael.peer@pwc.com

Dmitry Kosarev
Director
dmitry.kosarev@pwc.com

Daniel Fu
Director
daniel.j.fu@pwc.com