

# The KPMG Difference

---

**KPMG has extensive experience and a tested methodology to deliver solutions across the spectrum of governance, risk and compliance. We differentiate ourselves by:**

**Expertise.** Our team of subject matter professionals have the skills and knowledge to provide implementation and support services that meet varied GRC needs across a wide range of industries.

**Flexible methodology.** KPMG's GRC methodology enhances risk management programs, quality processes, regulatory- and industry-mandated compliance programs, and corporate governance initiatives, all tailored to each company's specific needs.

**Track record of success.** We have effectively assisted multiple clients in implementing holistic, GRC solutions, as well as transitioning vendors with little disruption.

**Tested strategy.** We identify and offer tools that accelerate readiness and implementation activities for core GRC applications, and our strong relationships with many providers help to provide a cohesive experience for our clients.

## Contact

---



**Olivier Elst**  
**Director**  
**Risk & Assurance KPMG Advisory**

**M** +32 (0)485 17 83 48  
**E** oelst@kpmg.com



# Integrated GRC Target Operating Model

**A pragmatic and holistic approach to GRC**



# Integrated Governance, Risk & Compliance Target Operating Model (TOM)

Governance, Risk & Compliance (GRC) functions are facing increasingly complex risks, greater regulatory scrutiny and a more rigorous compliance environment.

Nevertheless, at KPMG we see that most organizations still have a very fragmented, silo-based approach towards GRC. This not only results in various organizational inefficiencies, but also in a lack of organizational assurance.

Other implications of this silo-based approach include: uncoordinated compliance programs and efforts, the implementation of a GRC tool before defining the proper

internal control framework, risk and control systems addressing only financial reporting risks, business continuity systems focused on IT aspects only, etc.

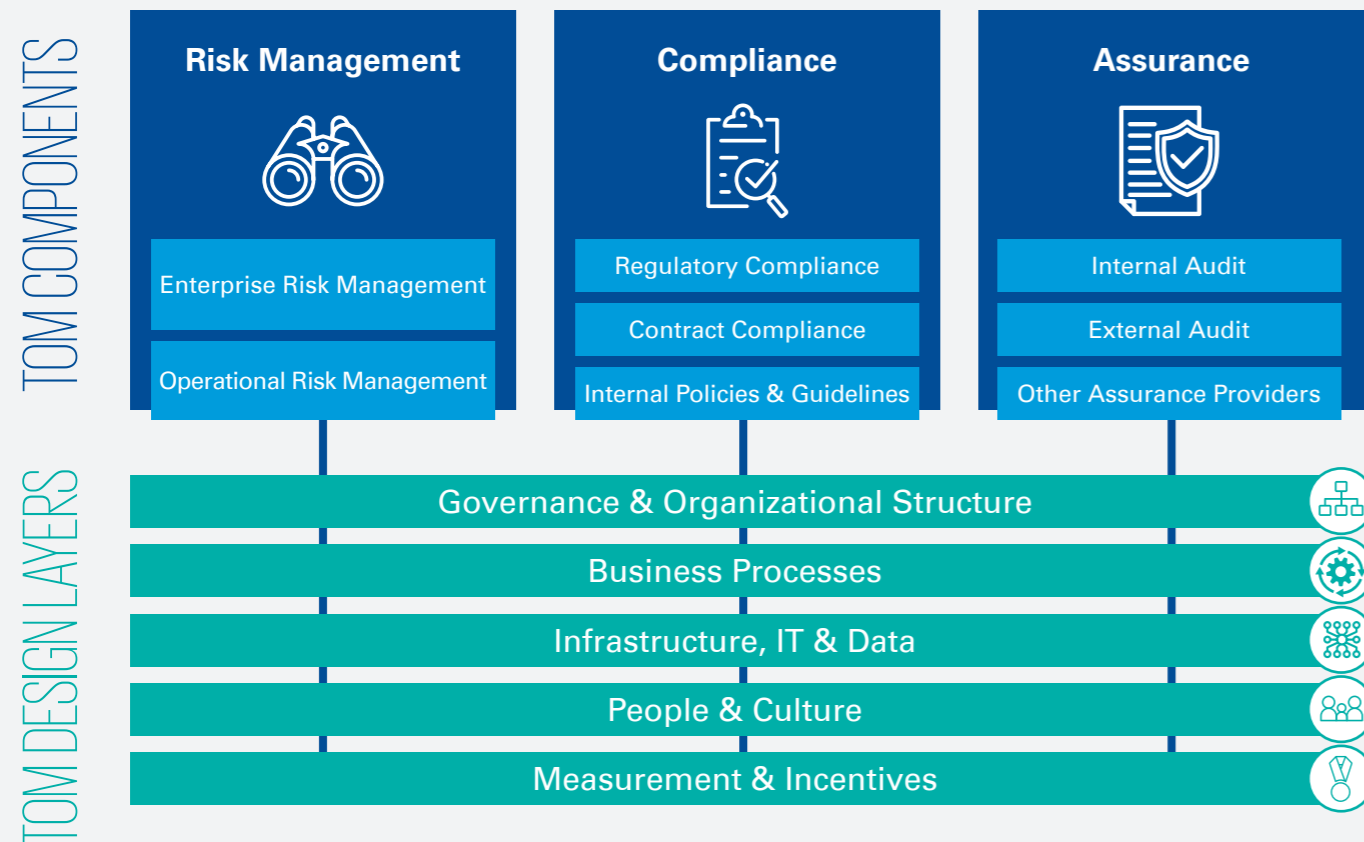
At KPMG, we understand that this fragmented approach to GRC can be explained by the fact that organizational Target Operating Models (TOM's) are rarely viewed from a GRC perspective. As such, the organization of GRC is often not designed to be well integrated.

Hereunder we propose our vision on how to achieve an integrated GRC Target Operating Model.

## KPMG's GRC TOM: A pragmatic and holistic approach

At KPMG, we believe in a pragmatic and holistic approach when it comes to GRC and have developed a generic GRC TOM based on the '9 Levers of Value KPMG Model', a proven method for defining an organization's Target Operating Model.

Our GRC TOM is built around two dimensions: the first dimension consists of three Components which cover all the GRC functions within an organization; the second dimension includes five Design Layers which need to be tailored to the risk appetite and strategy for every TOM component of the organization.



# Advantages of an integrated GRC TOM

### Protect and enhance business value:

By fostering a risk-aware culture, supporting informed decision-making and by addressing multiple compliance and assurance layers.

### Enhance operational efficiency:

By rationalizing risk management, controls and assurance structures and processes, and through the smart use of IT and data management structures.

### Provide a proactive and dynamic approach:

By enabling organizations to quickly, consistently and efficiently respond to challenges arising from evolving risk profiles and rapidly changing regulatory requirements.

### Support a linkage to strategy:

By enabling companies to meet compliance objectives while improving performance using an integrated framework in support of their strategic objectives.

## How to get there?

KPMG developed a diagnostic model consisting of 8 steps to help organizations design or refresh their GRC TOM.

Firstly, we perform a profound assessment of organizations' TOM Components with regard to the Risk & Compliance context, the strategy, and the current state. This includes:

1. The identification and scoping of the **Risk and Compliance Landscape** - the basis of the GRC TOM.
2. The defining of the **Risk & Compliance Appetite and Strategy** for each TOM component - to clarify the organization's objectives.
3. An **evaluation of the organization's current state**. The objective of this step is to understand the organization's current strengths and weaknesses in order to identify the gap between the "as is" and the "to be" situation.

Secondly, we design the future organization. Specifically, based on the GRC assessment (steps 1-3), we will adapt or set up every TOM Design Layer for each TOM Component. This entails the following 5 steps:

1. The **design of the processes** and key controls for each TOM component of the organization in order to achieve the set objectives.
2. The **design of the required IT infrastructure** in order to ensure that the design of the Risk & Compliance processes are supported by proper tooling.
3. The definition of the best possible **Governance & Organizational structure** for the future Risk & Compliance functions within the organization. This also includes the creation of an assurance map and an organizational chart.
4. KPMG will focus on **People & Culture** in order to ensure that the right people are at the right place and that the organization has a proper risk & compliance culture in place.
5. KPMG will address **Measurement & Incentives** by implementing Key Risk & Compliance Indicators that will allow the organization to monitor the performance of the Risk & Compliance framework.

