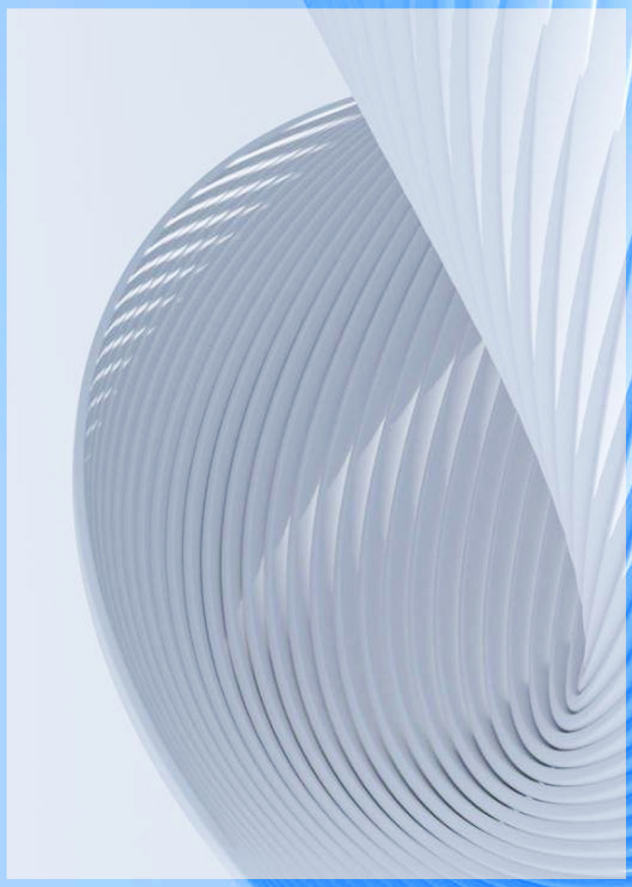
KPMG

Compliance function transformation

A strategic opportunity



KPMG Middle East

November 2025

Contents

Introduction

In an era marked by rapid change and unprecedented complexity in Saudi Arabia, the landscape of regulatory compliance is evolving at an extraordinary pace driven by Vision 2030 initiatives and programs, economic diversification efforts, regulatory reforms, along with the focus to align with international standards.

As Saudi Arabia's economy expands further, more organizations have been established within the public and private sectors and many multinational businesses have established their presence in the Kingdom. Thus, the oversight role of regulators has become more critical to interpret the legal requirements and regulations in addition to the enforcement of compliance with such regulations.

Compliance management activities are mandated by regulators, closely monitored by rating agencies, and increasingly expected by stakeholders across major sectors and industries including financial services, government and public sector, energy, healthcare, tourism and entertainment, FMCG and retail, insurance, telecommunications, manufacturing, education, transport and logistics, and infrastructure.

Historically, the responsibility for compliance was scattered across various departments, with each function handling compliance matters relevant to their specific areas, with limited coordination or enterprise-level oversight, which led to inconsistencies, inefficiencies, and increased risk exposure. As regulations expanded and regulatory environments grew more complex and demanding, organizations began to formalize and centralize these efforts, leading to the establishment of dedicated compliance functions.

Compliance functions today are driven by more than regulations and external forces. Managing compliance risks efficiently and effectively helps organizations achieve strategic and operational objectives and protect against non-compliance which ultimately enhances stakeholder confidence.

In the early emergence of compliance functions, focus was merely on regulatory related checks to ensure adherence to applicable laws and regulations, relying heavily on manual and reactive processes. As laws and regulations expanded, there became a need to to formalize compliance practices through standardize compliance management frameworks.

> “Managing compliance risks efficiently and effectively benefits organizations to achieve operational and strategic objectives and protect against noncompliance which ultimately benefits stakeholders.”

To enhance efficiency, a shift toward a risk-based and integrated approach has emerged, supported by technology enablement. Integrating compliance and risk management, and the use of data analytics and AI have become increasingly important to enhance predictive compliance and also support teams in proactively detecting red flags and potential violations.

This publication focuses on the need for organizations and more specifically compliance functions to transform in response to the rapid changes in the regulatory landscape and the evolving compliance frameworks and practices. In doing so, entities in the private and public sectors are evaluating their current compliance practices to define and initiate their transformation journey.

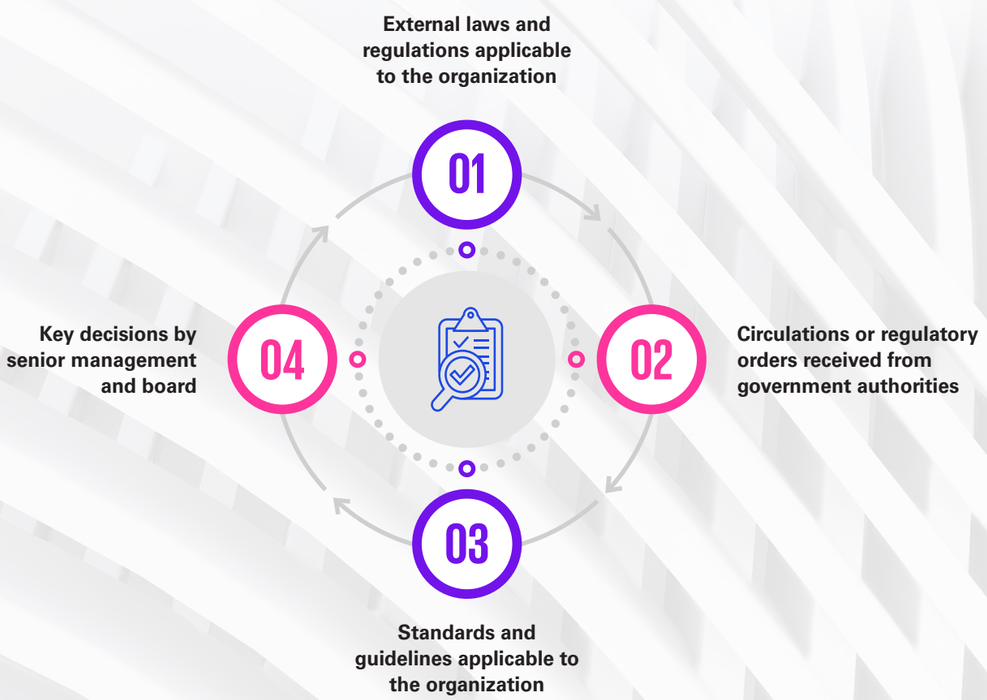
Craig Wright
Partner, Head of Enterprise Risk Services

The case for compliance transformation

Key challenges

- The number of laws and regulatory requirements continues to increase rapidly across sectors.
- Rapid regulatory changes require more agile approaches to handle compliance agenda.
- Regulations are emerging/expanding in new areas such as ethical business practices, sustainability, and corporate social responsibility.
- Digital transformation and challenges related to cyber threats, data management, and AI, including local requirements issued by authorities such as the National Cybersecurity Authority (NCA) and the Digital Government Authority (DGA), as well as international regulations such as the European Union's General Data Protection Regulation (GDPR).
- Recent establishment of new entities in the public sector to drive the execution of Vision 2030 initiatives and programs, increasing pressure on governance and stakeholders management within clear frameworks.
- Clear accountability and robust enforcement are critical, as the consequences of non-compliance, whether financial, reputational, or operational, have become too severe to overlook.

Key sources of compliance requirements



The importance of compliance

Compliance is an ongoing process and the outcome of an organization meeting its compliance requirements through conforming to laws, regulations, and standards.

Building and maintaining an effective compliance function can benefit organizations through ensuring smooth operations, avoiding costly litigations and legal consequences, fostering a trusted reputation and strong relationships with local communities, authorities and all stakeholders.

The concept and importance of compliance has evolved through the years to eventually gain the meaning and importance it has today. There are two main types of compliance according to ISO 37301 – Compliance Management System. These types include:

Regulatory compliance

Focuses on organizations' compliance with the local and international laws and regulations that are relevant to its operations. Depending on the business and the industry in which it operates, the requirements of regulatory compliance will vary. Regulatory compliance ensures the organization is following the laws and regulations so that trust can be established and eventually the organization's reputation improves and grows.

Voluntary compliance

Focuses on organizations' compliance with internal policies, procedures, code of conduct, and best practices.

Risks of non-compliance

Risk management process is a systematic recurring cycle for continuous identification, assessment, treatment, and monitoring of risks. It can be applied across strategic, legal and compliance, operational, technology, and other risks.

Risks associated with non-compliance with regulations include, but are not limited to, significant financial losses arising from penalties, fines, and increased costs related to remediation and legal proceedings. Reputational risks can also be severe, as regulatory breaches may damage stakeholder trust, confidence, and negatively impact market perception. In addition, non-compliance can lead to business interruptions, such as suspension of operations, loss of key licenses or permits, restrictions on business activities, and delays in critical projects, which can have lasting operational and financial consequences.

Such risks are addressed and mitigated across the organizations through integrated models, one of which is the three-lines model explained in the next section.

Compliance and the three lines model

The three lines model is the cornerstone of the most successful compliance management systems in any organization. The basic structure of the model was published by the Institute of Internal Auditors (IIA).

First line

The **first line** is comprised of the day-to-day management operations and activities. The first line fills the dual role of performing the general operations as well as the baseline controls to prevent loss, fraud, failure, etc.

Second line

The **second line** is made up of independent compliance and risk management functions that support and advise the first line on compliance, risk, and controls. These functions also report to senior management and the board or its committees on compliance and risk management activities.

Third line

The **third line** is generally an internal audit function (or an outsourced audit function for smaller institutions) that provides independent assurance over the compliance functions in place in the first and second lines.

The table below shows implications of the three lines model in a compliance function:

Compliance owners	Compliance professionals	Internal audit
Gather the data to perform the tasks to ensure compliance.	Review compliance activities performed by compliance owners in accordance with the established compliance management system.	Review the activities of compliance performed along with the evidence recorded.
Perform the tasks and confirm their completion.	Ensure that the evidence recorded is updated and accurate.	Report non-compliances and assess the steps taken to mitigate the risk of non-compliance.
Record evidence of compliance-related tasks performed.	Review periodically status of compliance.	Assess the compliance framework including the automated portals and policies.
Update MIS/other records as per the internal requirements.	Assess risk of the non-complied tasks and structure action plans and set the target date of completion.	

Enterprise versus regulatory compliance

Compliance functions are typically focused on ensuring adherence to regulatory requirements and obligations which are applicable to the organization's mandate. Complying with external obligations (such as laws, regulations, royal decrees and other directions from regulatory bodies) is considered mandatory.

Organizations may also opt for compliance functions to focus on ensuring adherence to internal compliance matters such as the policies, procedures and processes. However, this is not considered a common practice and is classified as 'voluntary' compliance rather than mandatory as per ISO 37301 – Compliance Management System.

To decide on the coverage of compliance function mandate, few points should be considered and those include:

Specialization

Having a specialized team focusing on regulatory compliance and operational team focusing on policies, procedures and processes will enhance credibility, accuracy and relevance of conclusions on status of compliance.

Efforts overlap

If compliance takes on regulatory and enterprise-wide compliance including policies and procedures, there might be efforts overlapping with other assurance functions such as risk management, quality and operational excellence, internal audit, etc.

Effective utilization of resources and time

Absence or ineffective management of overlapping possibilities will lead to ineffective utilization of resources and time across assurance providers. In addition, this will also potentially lead to extensive time investment from management to address requirements on similar subjects.

ISO 37301:2021 Compliance Management System

ISO compliance status remains intact if the compliance function primarily takes responsibility for ensuring adherence to external obligations, while the quality or operational excellence functions remain responsible for ensuring adherence with internal policies, procedures and processes.

Compliance enablers

Compliance management plays a vital role in organizations. The failure in compliance governance or processes may lead to fines, legal and reputational risks, and even business interruptions that hinder organization's ability to achieve its goals and objectives.

Ongoing reviews and assessments of compliance help avoid non-compliance incidents. Other barriers to compliance include the structural complexity of the organization, inability to understand and interpret laws and regulations, and their implications on operations.

Effective compliance management generally encompasses the target operating model, framework, policies, procedures, monitoring plans and reporting tools that ensure the organization's regulatory obligations are identified, monitored, and the status of compliance is reported in a systematic and timely manner. In addition, one important component of effective compliance is culture. A strong culture supports trust in the system, and ultimately leads to more effective compliance.

To ensure that compliance development, enhancement and transformation are sustainable, organizations should focus on key components of an effective compliance management system. Those components fall into three main pillars which include; governance and culture, operations. and monitoring and continuous enhancement.

Governance and culture

Compliance Target Operating Model (TOM) including organizational structure, roles and responsibilities, manpower plan and KPIs.

Compliance framework along with policies and procedures.

Reporting structure to direct management reporting, and enable access to the board of directors and relevant board committee(s).

Culture and awareness to have the buy in of all stakeholders and gain trust for more effective implementation.

Operations

Regulatory requirements: identify relevant rules, regulations and mandates that the organization must comply with.

Conduct periodic risk assessments and prioritize monitoring activities based on results

Deliver continuous training to personnel, compliance professionals and relevant stakeholders.

Monitoring and enhancement

Monitor compliance through self-assessments and execution of inspection visits based on the annual risk-based approach.

Compliance reporting and automation: implement digital assets and AI that can enhance work efficiency, accuracy and timeliness.

Recommend controls and remedial actions for non-compliance, and follow-up to ensure effective implementation.

Compliance enablers are tools, practices and processes that facilitate an organization's ability to operate and maintain effective compliance programs. Such enablers include:

- **Tone at the top:** Leadership commitment sets the tone for ethical behavior and compliance across the organization.
- **Clear policies and procedures:** Well-defined, accessible policies and procedures provide employees with guidance on expected behaviors and compliance requirements.
- **Continuous training and education:** Continuous training helps employees understand compliance expectations, risks, and how to address them.
- **Communication:** Open dialogue with stakeholders fosters transparency and collective accountability.
- **Enforcement and discipline:** Applying consistent consequences for violations reinforces the importance of compliance.
- **Technology and automation tools:** Compliance software and systems help streamline processes, track activities, and manage documentation efficiently.
- **Review and improvement:** Assessing and updating compliance programs ensures they remain effective and aligned with evolving regulations and business needs.

By integrating these enablers into the organizational culture and operations, organizations can strengthen compliance efforts and promote an environment of integrity and responsibility.

Compliance culture

To build and sustain a strong compliance culture, organizations must adhere to the elements of driving trust. Trust is built on consistent, predictable action in the moments that matter—like keeping data safe, using ethical business practices, complying with regulations, and partnering with credible third parties.

KPMG's Trusted Framework sets forth the following six elements that entities can embed into their business to earn and sustain the trust of stakeholders:

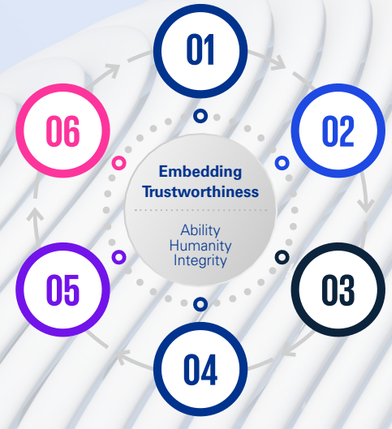
- Purpose and strategy
- Culture
- Leadership and management
- Governance and structure
- Systems and processes
- Products, services, and operations

A strong ethics and culture of compliance is one that fosters and celebrates doing the right thing—an environment that constantly looks to enhance integrity and earn/maintain trust.

Purpose and strategy
Clear purpose and strategy with trust-inducing core values that creates value for society and accommodates stakeholder's interests.

Products, services, and operations
Processses that ensure stakeholder needs and expectations are met, legislation adhered to, and values upheld.

Systems and processes
Leverage and align planning, management, HR, reporting, and compliance systems to reinforce trustworthy behavior in line with the legal and regulatory context.



Culture
Shared values, beliefs, and norms that foster constructive trust-including behavior aligned with the organization's purpose.

Leadership and management
Leaders who embody the company values and purpose, and hold themselves and others to account for trustworthy conduct.

Governance and structure
Formal organization and governace that set clear roles and accountability and provide discretion within prudent oversight.

Beyond compliance

To remain competitive, innovation in compliance is a necessity. Organizations must strategically invest in the integration and automation of their compliance management activities to promote greater agility, sustainability, resilience, and effectiveness.

Design and implementation

- Revised compliance policies, procedures, code of conduct, processes and controls.
- New risk assessment methodologies, standards and protocols.
- Updated compliance hotlines and reporting (root cause analysis, metrics, dashboards).
- Data remediation to address strategic compliance needs for information.
- Regulatory change management mechanism to identify, track and respond to compliance obligations in order to link them to applicable internal policies, procedures, processes and controls.

Integrate

- Design enterprise-wide compliance controls and processes to eliminate silos, coordinate compliance efforts, recognize synergies and achieve greater consistency and agility.
- Integrate and centralize governance structures and processes.

Automate

- Implement technologies to support compliance efforts that align to the organization's strategy and operations.
- Design new functionality in existing technology to automate metrics, manage regulatory changes, due diligence, dashboards, investigations, and policy management and more.
- AI plays a vital role in compliance by enhancing efficiency, accuracy, and proactive monitoring. It can automate routine tasks such as data collection, document review, control mapping and reporting, reducing human error and saving time. AI tools can also analyze data to identify potential risks, and flag non-compliance.
- Overall, integrating AI into compliance processes helps organizations adapt to new regulations, monitor and map relevant controls, maintain high standards of integrity, and foster a culture of continuous improvement.

How KPMG can help

Industry relevance

KPMG helps organizations enhance and align their compliance program with the current regulatory environment specific to their industry and geographic jurisdictions. We also help organizations anticipate regulatory changes and better understand peer practices in their respective sector.

Client-specific target operating models

KPMG, using its propriety methodology, assesses the organization's business activities, regulatory obligations, and requirements to develop a compliance target operating model that is aligned with local regulatory requirements, international standards (ISO 37301:2021), and relevant industry-leading practices and standards.

A global compliance risk assessment framework

KPMG's global regulatory and compliance framework has been developed through numerous advisory engagements and is continuously calibrated against applicable regulatory expectations, requirements, and guidance, as well as industry-leading practices and standards.

This KPMG proprietary framework allows the stakeholders to integrate and automate their compliance obligations to respond to control gaps, regulatory changes, trends, and risk assessment results in an effective and timely manner.

KPMG's compliance framework includes eight key elements that drive prevention, detection, and response, with governance and culture at the core. Compliance accountability starts with a strong compliance culture that sets the tone at the top and reaches across the three lines.

KPMG's Compliance Methodology

- Staft fitness and propriety
- Defined JDs, KPIs, clear reporting lines
- Third party due diligence

- Risk-based assessment approach
- Inherent and residual risks
- Regulatory universe

- Internal reporting to board and management
- External reporting to regulators and supervisory authorities
- Record-keeping

- Issues management and remediation
- Voluntary disclosure protocols/self-reporting
- Regulatory investigations
- Investigation policy and protocol

- Entity-wide embedding of compliance requirements and values
- Policies and procedures management

- Training and awareness
- Regulatory updates
- Tone at the top: regular management communication

- Compliance automation
- Due-diligence screening tools

- Monitoring and testing program
- Regulatory change monitoring
- Self-assessments
- Independent audits

About KPMG Middle East

KPMG Middle East is a part of the KPMG global organization of independent member firms that operate in 142 countries and territories and are affiliated with KPMG International Limited. We provide audit, tax and advisory services to public and private sector clients across Saudi Arabia, United Arab Emirates, Jordan, Lebanon, Oman, and Iraq, contracting through separate legal entities. We have a strong legacy in the region, where we have been established for over 50 years. KPMG Middle East is well-connected with its global member network and combines its local knowledge with international expertise.

KPMG serves the diverse needs of businesses, governments, public-sector agencies, not-for-profit organizations, and the capital markets.

Our commitment to quality and service excellence underpins everything we do. We strive to deliver to the highest standards for our stakeholders, building trust through our actions and behaviors, both professionally and personally.

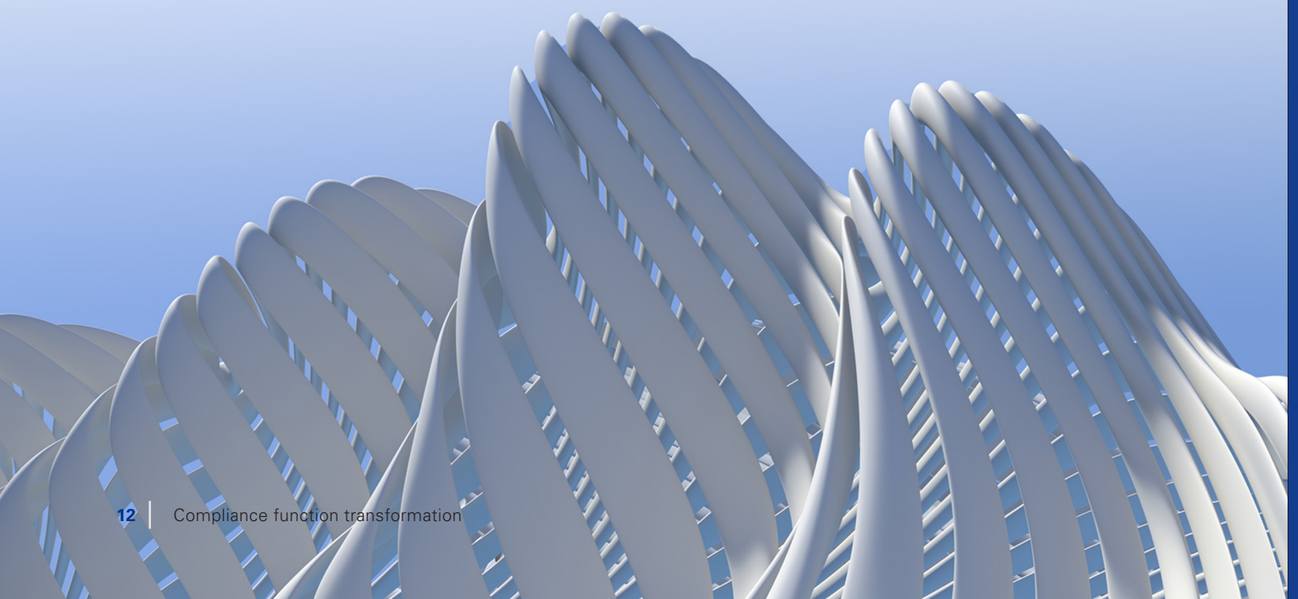
Our values guide our day-to-day behavior, informing how we act, the decisions we make, and how we work with each other, our clients, and all our stakeholders. Integrity: We do what is right. Excellence: We never stop learning and improving. Courage: We think and act boldly. Together: We respect each other and draw strength from our differences. For Better: We do what matters.

Our purpose is to inspire confidence and empower change. By inspiring confidence in our people, clients and society, we help empower the change needed to solve the toughest challenges and lead the way forward.

KPMG's Impact Plan guides our commitments to serving our clients, people and communities across four categories: Planet, People, Prosperity, and Governance. These four priority areas assist us in defining and managing our environmental, social, economic and governance impacts to create a more sustainable future. We aim to deliver growth with purpose. We unite the best of KPMG to help our clients fulfil their purpose and deliver against the United Nations Sustainable Development Goals, so all our communities can thrive and prosper.

We are dedicated to delivering growth with purpose, helping our clients achieve their goals, and advancing sustainable progress to ensure that all our communities thrive. Empowered by our values, and committed to our purpose, our people are our greatest strength.

Together, we are building a values-led organization of the future. For better.



Contacts

Sudhir Arvind
Partner, Head of Governance,
Risk and Compliance Services
sarvind@kpmg.com

Mohammad Abudalo
Partner, Governance,
Risk and Compliance Services
mabudalo@kpmg.com

Mohammad Fahad Shaikh
Director, Governance, Risk and
Compliance Services
shaikhfahad@kpmg.com

Sarah Althahabi
Manager, Governance, Risk
and Compliance Servicess
salthahabi@kpmg.com

kpmg.com/sa

kpmg.com/ae

kpmg.com/om