Compliance Assurance: How do you stay in control of your compliance processes?

In current society, organizations increasingly need commitment to comply with relevant laws, regulatory requirements, industry codes and organizational standards, as well as standards for good governance, generally accepted best practices, ethics and community expectations. Organizations that aim to be successful in the long term have to establish and maintain a culture of compliance, considering the needs, requirements and expectations of different stakeholders. A structured compliance management approach enables an organization to create such a culture of compliance.

This raises several questions such as: What raises awareness of compliance topics? How is compliance currently anchored in your organization? How can you become familiar with relevant and new requirements? And how do you move your company to the next level of compliance and provide your stakeholders with independent assurance over your compliance function? In this article, we would like to show how you can move your compliance processes to the next level.

Drs. Jacco van Kleef RA, Digital MBA,
is partner at KPMG IT Assurance & Advisory.

Manon van Rietschoten MSc RE RA, Digital MBA,
is senior manager at KPMG IT Assurance & Advisory.

Pia Schmidt MA
is senior consultant at KPMG Integrity and Compliance, Risk & Regulatory.

INTRODUCTION

To establish a successful compliance organization, people with the right mindset and skills throughout the whole organization are needed to drive the highest possible efficiency to compete in the market. We will first introduce the importance of compliance, including the key drivers in the market, after which we will focus on the insights from KPMG's Chief Ethics and Compliance officers (CCO) survey, published in March 2022. After that, we will elaborate on KPMG's Global Compliance Framework and explain how it can help your internal organization and externally demonstrate the effectiveness of your compliance management system (CMS). We would like to close with a description of how the ISO 37301 framework can help you to achieve a higher maturity level on compliance.

IMPORTANCE OF COMPLIANCE

Compliance has become increasingly important in various areas in recent years. Continuously meeting legal requirements is an organizational challenge as overseeing and acting on all requirements is complex and costly. However, an approach to show internal and external parties that your organization is in control of compliance requirements is more important than ever, given the external challenges from society to be compliant and the competitive advantage that an organization can achieve with a good compliance system. Also, the need to provide a solid foundation which enables prevention, detection and monitoring prevention of non-compliance is more important than ever.

Several compliance incidents during the last years showed that compliance is too important to ignore. Therefore, a stronger focus on this topic is advisable. The following aspects are the key drivers to increase focus on compliance and demonstrate its importance:

- **Global public attention and demand for compliance.** A public attention and demand for conducting business in an ethical way is present globally. This triggers a search for independent assurance and certification on CMSs and environmental, social and governance (hereinafter: ESG) aspects. New regulations driving focus on human rights and adherence to social standards as well as the global sustainable development goals that include compliance concepts have the public's attention.
- **Concentration on compliance effectiveness.** Regulatory focus has expanded to maturity of compliance programs (e.g. De Nederlandsche Bank / Autoriteit Financiële Markten / Department of Justice) to improve on robustness of e.g. the monetary system.

- **Legal requirements for companies.** Corporate criminal liabilities, legislation requirements (e.g. Money Laundering and Terrorism Financing Act, US Foreign Corrupt Practices Act, UK Bribery Act) as well as the oversight of and implications for the misconduct of third parties in supply chain increasingly become a focus area.
- **Competitive advantage.** Being in control of compliance requirements can distinguish an organization from their competition. For example, a well-functioning CMS in your organization can create synergies between tasks and help to overcome departmental boundaries and meaningfully interlink different processes in the organization's workflow. Furthermore, it can show a tangible display of enhanced capabilities for a firm's reputation.

RESULTS FROM KPMG COMPLIANCE CCO SURVEY

KPMG performed a survey ([Groe22]) on compliance to gain insights in terms of the current importance of compliance. The survey includes responses from 100 Chief Ethics and Compliance Officers (CCOs), who represent some of the largest organizations across multiple industries in the Netherlands as well as acting international, about their view on the most important focus and integration areas, as well as key areas where compliance programs can improve. This survey in the Netherlands follows the same format as the KPMG US CCO Survey, last published in 2021— the most recent version focusing on risk and investment in compliance ([Mats21]). Both surveys utilize the KPMG Compliance Maturity Framework as a basis.

The organizations that participated in the survey operate in the following industries: consumer markets/ retail, energy, financial services including banking, capital markets and insurance FS (Banking and/or Insurance), healthcare and life sciences, industrial manufacturing, and technology, media and telecommunications. The outcome of the survey presents the results of the survey as well as KPMG's assessment of the most important factors and measures companies can consider bringing their compliance programs to the desired level of maturity.

With the CCO survey, the current opinion about compliance is gathered. It is shown that a majority of the organizations seek to obtain CMS certifications in the near future (66%). This shows a strong commitment to be compliant and to account for that externally. Moreover, most mature areas in the field of compliance are the areas traditionally associated with regulatory obligations (e.g. regulatory change management and reporting).

Furthermore, as key conclusions of the CCO survey, the following was noticed:

- **Training.** As a regulatory obligation, a training is still focused on completion rates and not being used as a tool for shaping a culture which is an emerging regulation in some industries (e.g. DNB soft controls). Therefore, organizations should shift their training and communication approach to view it as a tool to shape and assess their culture and conduct.
- **Driving process efficiencies.** Adequate compliance resources and digitalization / analytic support are still lacking across industries. Furthermore, organizations can do more to develop controls and indicators for emerging risks, such as ESG and third-party oversight.
- **Integrated collaboration.** More effort should be made across organizations to integrate their ethics and compliance performance metrics and indicators into wider governance, risk, and compliance (GRC) frameworks for more optimal monitoring and reporting capabilities.

Expectations of compliance professionals' knowledge and responsibilities will increase as will the need for adequate resources to match the company's ethics and compliance framework. Increasing societal pressure for strong and far-reaching corporate governance will continue to drive change in the regulatory obligations and maturity requirements. The status quo and future development of the ethics and compliance field can be summarized by the CCO survey across nine different areas: culture; governance; process; risk assessments; policies, procedures and code of conduct; training and communications; monitoring and testing; investigations; and reporting. The expected changes are already visible today (see Figure 1).

A GLOBAL COMPLIANCE FRAMEWORK

The CCO survey showed that organizations are still struggling with establishing a solid compliance framework. Therefore, and in order to achieve organizational goals, having a solid and sound compliance program in place is crucial. A combination of hard controls such as the presence of the compliance function, policies and procedures, and soft controls such as trainings and e-learnings are necessary to successfully mitigate compliance risks. In order to do so, it is crucial that the compliance function, policies and procedures align with the needs and wishes that are coming from the organization, as well as with the necessary requirements from the regulators.

Figure 1. The ethics and compliance path.

To measure the effectiveness of the compliance function, policies and procedures in place, KPMG developed the Global Compliance Framework (see Figure 2). This framework has been calibrated against applicable industry standards and regulatory expectations, requirements and guidance.

The Global Compliance Framework that tailors to your organization's needs to prevent, detect and respond appropriately to non-compliance with regulatory and contractual requirements can support you to become trusted with new requirements regarding compliance. KPMG's Global Compliance Framework can support organizations in getting a better overview and understanding of the organization's needs. It reflects an enterprise-wide risk management approach to compliance with focus on governance, policies and procedures, people (both compliance-dedicated staff and other staff) and monitoring arrangement ("three lines-of-responsibilities").

DEMONSTRATING COMPLIANCE: ISO 37301 CERTIFICATION

ISO standard certifications can help your organization to show its capability to maintain an effective CMS to a broad public, industry regulators, and your current and future clients. In particular, ISO 37301 certification, as a guideline for implementation of a CMS, is independent of the size, type and nature of the activity, as well as whether the organization belongs to the public or private sector. In this context, an ISO 37301 certification can help increase the effectiveness and optimize compliance-relevant processes. Unlike other ISO standards, the ISO 37301 standard sets the bar for an effective CMS as opposed to testing "the way of working". For organizations, an independent certification provides transparency to shareholders, clients and regulatory oversight on the appropriate working of the CMS. At the same time, it mitigates the liability risk of the organization's management.

Figure 2. KPMG's Global Compliance Framework.

KPMG supports organizations in designing, assessing and improving an organization-wide compliance system, discovering the value of compliance while fully supporting your organizational goals ([KPMG22]). An independent certification can provide transparency to shareholders and clients and regulatory oversight on the appropriate working of the CMS and mitigate the liability risk of the entity's management. As mentioned above, this is relevant given that 66% of the respondents of the compliance survey ([Groe22]) expect to obtain CMS certifications in the near future. CMS certifications such as the ISO 37301 certification can provide organizations with more assurance in this regard, where the KPMG's Global Compliance Framework can be referenced from the outset to gain a better understanding of the organization and its context.

CONCLUSION

Regulatory compliance is vital for being a successful and sustainable organization. To achieve this, organizations need to have a mature CMS that takes the needs, requirements and expectations of the different stakeholders into consideration. However, the regulatory environment is continuously changing, making it an even greater challenge to comply with all relevant legal and stakeholder requirements. A framework which shows a flexible approach to organizational needs is therefore necessary. KPMG's Global Compliance Framework is an example of such a framework. The impact of non-compliance is trivial as it not only endangers public trust but can also result in reputational damage and large fines.

These circumstances call for a solid compliance framework ensuring that an organization can prevent and remain alert to identifying (potential) breaches and follow up on any non-compliant activities. Therefore, the goal of organizations should be to familiarize themselves with their compliance program and achieve a higher maturity level. The authors in KPMG's Assurance and Advisory services can be your contact persons for further information.

References

[Groe22] Groen, L. et al. (2022). *The state of ethics and Compliance in the Netherlands - 2022 Chief Compliance Officer Survey results.* KPMG Netherlands. Retrieved from: https://home.kpmg/nl/en/home/insights/2022/02/the-state-of-ethics-and-compliance-in-the-netherlands.html?utm_campaign=PostBeyond&utm_source=LinkedIn&utm_medium=%23309247&utm_term=The+state+of+ethics+and+compliance+in+the+Netherlands

[KPMG22] KPMG (2022). *Compliance Services.* Retrieved from: https://home.kpmg/nl/en/home/services/advisory/risk-consulting/internal-audit-risk/compliance-services.html

[Mats21] Matsuo, A. et al. (2021). *KPMG 2021 CCO Survey – Sharing client perspectives on compliance imperatives.* KPMG US. Retrieved from: https://advisory.kpmg.us/articles/2021/cco-survey-2021-gated.html

About the authors

Drs. Jacco van Kleef RA, Digital MBA, is partner at KPMG IT Assurance & Advisory. He is an experienced auditor in the fields of financial audits, IT audits and ISO, working in highly regulated environments (financial services industry) with a passion for good governance and internal control.

Manon van Rietschoten MSc RE RA, Digital MBA, is senior manager at KPMG IT Assurance & Advisory. She is an IT / financial advisor and certified (ISAE) auditor (RE RA) with special affinity within the asset management and pension segments; preference for complex assignments in the field of process improvement, digitization and compliance.

Pia Schmidt MA is senior consultant at KPMG Integrity and Compliance, Risk & Regulatory. She is a compliance management system auditor, according to the German auditing standard of the Institute of Public Auditors, IDW PS 980; personal affinity for gap analyses, compliance risk (culture) assessments and risk-based internal audits.