ESG Risk Practices

What's missing and why does it matter

Article

May 2024

May 2024

The focus and scrutiny on ESG-related risk and compliance is intensifying across regulatory agencies, fostering strong expectations for organizations to establish appropriate ESG risk and compliance programs. Can you say that your organization has an effective risk and compliance program for ESG at this moment? If not, why?

Here are some common challenging areas where organizations will need to focus in order to build and/or mature their coverage in 2024. KPMG's perspectives on each of these areas are discussed below.

1. *Developing an ESG risk framework that is not aspirational and sets the standards for ESG initiatives and accountabilities, as well as how to measure associated risks.*
2. *Integration of Double Materiality Assessment (DMA) output in ERM .*
3. *Strengthening (and documenting) ESG governance and controls.*
4. *Demonstrating ESG risk and compliance coverage across risk pillars.*
5. *Inventorying and assessing regulatory expectations/requirements (amid continued political/jurisdictional discord).*
6. *Building an effective ESG risk and compliance assessment and monitoring program that is inclusive of the organization's various ESG initiatives and assurance requirements.*

Challenge 1 Developing an ESG risk framework that sets standards for ESG initiatives

Key Question: *Should we develop and adopt a separate enterprise ESG framework?*

KPMG Perspective: A risk framework serves as a cornerstone to an organization's operations and is a foundational element to an effective risk and compliance program. Currently, the industry is struggling with what should be included in their ESG risk framework. In many cases, the question arises whether "another" policy is needed on top of existing policies that tie within the "umbrella" of ESG and sustainability. An integrated ESG risk framework should coincide with the structure of ESG teams, in many cases a "hub and spoke" with ESG at the center. Frameworks should be inclusive of policies, governance structures, and how to measure and monitor ESG risk. Benefits of an ESG framework include having a clear and transparent strategy to communicate with investors, consumers, and others on the organization's implementation of ESG/sustainability commitments and, perhaps most importantly, helping to ensure accountability across all business areas. Regulators expect organizations to:

- Develop a comprehensive ESG framework that is inclusive of ESG risk and business areas.
- Integrate ESG-related risk into their policies and procedures.
- Integrate the ESG framework into areas such as business unit strategies, risk management, third-party monitoring, and Board accountability.
- Modify their policies when necessary to reflect changes in emerging risks, operating environments, or activities.

Challenge 2 Integration of Double Materiality Assessment (DMA) output in ERM

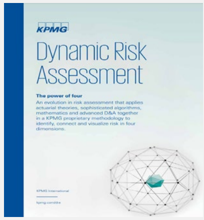
Key Question: *How can we integrate the outputs from Double Materiality Assessment (DMA) in ERM practices?*

KPMG Perspective: The European Sustainability Reporting Standards (ESRS) set out detailed reporting disclosure requirements under the Corporate Sustainability Reporting Directive (CSRD). The ESRS' introduced a new and complex concept of double materiality (multi-stakeholder approach) and also expands a company's reporting boundary to its entire value chain. The Double Materiality is the backbone of CSRD reporting. The DMA defines the reporting scope and therewith, determine the quantity and quality of disclosures of sustainability related information. The outcomes of the assessment facilitates the discussion about material topics that impacts the company from an inside-out and outside-in perspective. While the DMA identifies the material topics for an organization, for reporting purposes, an ERM function should focus on performing an entity wide risk assessment by gaining insights into the risk landscape of the organization. The output of the DMA should also be considered in the company-wide risk assessment. Such an alignment ensures that the risks can be prioritized based on their impacts & likelihood.

The steps to identify material topics in accordance with ESRS1 are as follows:

a. Desk research-based update of identified impacts and identification of main risks and opportunities.
b. Assessment of impact and financial materiality for each topic identified, including stakeholder engagement.
c. Consolidation of results and identification of material topics based on to be defined thresholds.
d. Mapping of material topics against ESRS disclosure requirements.
e. Documentation of the results and the process undertaken for impact & financial materiality assessment.

The essentials of materiality assessment



Dynamic Risk Assessment

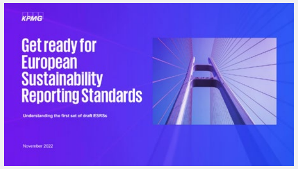
Challenge 3 Strengthening (and documenting) ESG governance and controls

Key Question: *What actions should we take to strengthen our ESG governance and controls?*

KPMG Perspective: Creating an ESG governance and control framework requires a gradual approach that is consistent and in alignment with the organization's strategies and existing internal controls. Ensuring data accuracy is vital to financial and non- financial reporting of ESG initiatives – expectations are raised even more with mandatory requirements such as those in the upcoming CSRD. Organizations face the challenge of not only managing their own data quality, but also that of their vendors and third parties.

Regulators are holding organizations responsible for lapses in oversight of their vendors and are looking for them to demonstrate accuracy, repeatability, consistency, completeness, and timeliness across governance frameworks. Risks associated with ineffective governance controls include:

- Lack of or inadequate third-party oversight, monitoring, and due diligence.
- Inhibited issue identification and resolution.
- Reporting inaccuracies, greenwashing.



Get ready for European Sustainability Reporting Standards

CSRD reporting: Application for groups with non-EU parents

Challenge 4 Demonstrating ESG as a transverse risk

Key Question: *How should we integrate components of ESG within our current risk and compliance practices?*

KPMG Perspective: ESG risks are interlinked across multiple financial and nonfinancial risk pillars and can potentially impact a wide range of risks throughout the organization, such as:

- Market risk
- Compliance risk
- Liquidity risk
- Reputational risk
- Operational risk
- Model risk
- Credit risk

The draft principles for climate risk management released by the Supervisors of financial institutions for example, outline actions that management should take when integrating climate risks into an existing risk management framework, including:

- Employing a comprehensive process for identifying emerging and material climate risks –including establishing definitions and thresholds for material risks.
- Developing processes to measure and monitor material climate risks and inform the board and management about the materiality of those risks (including physical and transitional risk).
- Incorporating climate risks into internal control frameworks, including internal audits.

Though the guidance was initially directed towards large financial organizations, regulators have called out the need for small, mid-sized and large organizations in all sectors to better understand their climate-related risks, which they suggest may include concentrated business lines and/or geographies.

Challenge 5 Inventorying and assessing regulatory expectations and requirements

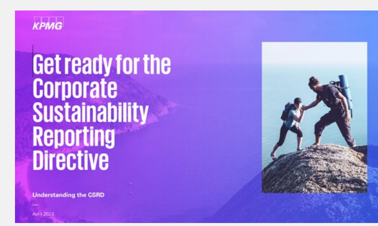
Key Question: *How do we prepare for regulatory expectations and requirements when the regulations may not yet be finalized and there is divergence across global/EU regulations?*

KPMG Perspective: ESG regulations are currently evolving amidst political and jurisdictional discord, creating some uncertainties about future regulatory requirements. This presents a challenge for organizations as they set ESG priorities based on shifting risks and regulatory expectations. Areas of regulatory scrutiny include reporting standards and frameworks, definitions/terms, scenario analysis/stress testing exercises, and third-party oversight. Highly anticipated regulations on ESG, which may introduce some clarity in coming times, are the:

- CSRD (and therefore the ESRS')
- EU Taxonomy disclosures
- SEC's climate risk disclosures

Despite these challenges, regulators expect organizations to:

- Maintain inventories of both current and emerging regulations and guidance.
- Assess risk exposures (via risk assessment processes) to pending regulations and guidance.
- Establish a strategy to implement ESG-related regulatory requirements, as well as sustainability commitments.



[Corporate Sustainability Reporting Directive]

Challenge 6 Building ongoing ESG risk and compliance assessment and monitoring

***Key Question:** Should the second line wait for the first line's decisions, actions, and innovations to implement an ESG risk and compliance program?*

KPMG Perspective: Considering that the first line of business is responsible for addressing ESG risks/issues as they pertain to product development, new technology and innovation, the second line (e.g. Risk and Compliance) faces the challenge of anticipating and applying appropriate risk management and oversight of products and services as they are built by the first line even as they begin to set Key Performance Indicators (KPIs) and risk appetite statements and undertake physical risk and scenario analysis. Integration of ESG regulatory expectations into existing risk and compliance programs must take into consideration the activities of the first line, because of the audit trail required for assurance purposes. Therefore, effective risk & compliance programs will require enhanced collaboration between both lines at the earliest stage of product development. Recent ESG-related enforcement actions against organizations underscore the importance of effective ESG monitoring and internal processes to mitigate inconsistencies in reporting, marketing, and general disclosures.

Transition plans, which should align with the organization's ESG strategy, are an important aspect of the Compliance role in establishing an effective ESG risk and compliance framework. A "good practice" transition plan should cover:

- The organization's high-level ambitions to mitigate, manage, and respond to emerging ESG risks.
- Short-, medium-, and long-term actions to achieve strategic ambitions alongside details on how those steps will be financed.
- Governance and accountability mechanisms that support the delivery of the plan and robust periodic reporting.

Measures to address material risks to, and leverage opportunities for the natural environment and stakeholders (including customers).


INCORPORATING ESG IN RISK MANAGEMENT
Transforming internal controls framework for ESG reporting
By: drs. Jeroen Bolt RC | Arushi Paliwal CA | Urvashi Aggarwala
Governance Risk and Compliance
Keywords: Assurance | Compliance And Reporting | ESG | Internal Controls | Risk

[Incorporating ESG in risk management]

Contact the authors:

Bart van Loon
Global Network Lead ERM
KPMG Netherlands
VanLoon.Bart@kpmg.nl

Emily Condack
Director, ESG Lead in GRCS
KPMG Netherlands
Condack.Emily@kpmg.nl

Arushi Paliwal
Manager, ESG in GRCS
KPMG Netherlands
Paliwal.arushi@kpmg.nl