ESG Risk Practices

What's Missing and Why It Will Matter

January 2023

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 today that your organization has an effective risk and compliance program for ESG? If not, why?

Here are some common challenge areas where organizations will need to focus in order to build and/or mature their coverage in 2023. KPMG 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. *Strengthening (and documenting) ESG data governance and controls.*
3. *Demonstrating ESG risk and compliance coverage across risk pillars.*
4. *Inventorying and assessing regulatory expectations/requirements (amid continued political/jurisdictional discord).*
5. *Building an effective ESG risk and compliance assessment and monitoring program that is inclusive of the organization's various ESG initiatives.*

Challenge 1 Developing an ESG 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 effective risk and compliance programs. 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 lines of defense. Regulators expect organizations to:

- Develop a comprehensive ESG framework that is inclusive of ESG risk, lines of businesses, and lines of defense
- 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 Strengthening (and documenting) ESG data governance and controls

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

KPMG Perspective: Creating an ESG data 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 SEC climate disclosure rule. Organizations face the challenge of not only managing their own data quality, but also that of their vendors. 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 data governance frameworks. Risks associated with ineffective data governance controls include:

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

Regulators expect FS organizations to take appropriate actions including:

- Incorporating ESG risk information into internal and external reporting, monitoring, and escalation processes.
- Ensuring effective risk data aggregation and reporting capabilities.
- Monitoring developments in data, risk measurement, modeling methodologies, and reporting.
- Incorporating adjustments and updates into ESG risk management processes, as appropriate.

Climate Risk: SEC's Mandatory Climate Disclosures Proposal

Investor Protections: SEC proposed Names Rule and ESG Investment Practices Disclosure

Challenge 3 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:

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

The draft principles for climate risk management released by the federal banking agencies 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 is directed toward large organizations, the regulators (and the FDIC and NY DFS, specifically) have called out the need for small and mid-sized organizations to better understand their climate-related risks, which they suggest may include concentrated business lines and/or geographies.

Notably, the federal banking agencies also name scenario analysis as an important element in identifying, measuring, and managing climate-related financial risks. The FRB has launched a pilot climate scenario analysis with six of the largest banks. The exercise will analyze the impact of separate and independent scenarios for both physical and transition risk on specific portfolios of assets. The FRB will also collect information on the participants' climate-related governance and risk management practices, including approaches or tools other than scenario analysis used in "business-as-usual" risk management, whether climate risk is included in the "business-as-usual" risk identification process, and whether climate scenario analysis informs the organization's business decisions. The exercise will likely set more detailed expectations for the industry on strengthening quantitative climate analysis, expanding model capabilities, and establishing governance and risk management practices.

Climate Risk: FRB principles for climate-related financial risk management

Climate Risk: FRB's Pilot Scenario Analysis and Risk Management Practices

Challenge 4 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/federal/state 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 federal regulations on climate and sustainability, which may introduce some clarity in 2023, are the:

- SEC's climate risk disclosures.
- Federal Banking Agencies' (FRB, OCC, FDIC) joint guidance on principles for climate risk management.
- SEC's ESG investment practices disclosures.
- CFPB's guidance on disparate impacts.

Some of the discord stems from divergent approaches, especially related to climate and sustainability, found in voluntary disclosure frameworks such as TCFD, CSR, and Materiality (such as under GRI and SASB) as well as between state and federal laws and regulations. These divergences can potentially complicate management of ESG risk and compliance programs long after the regulatory expectations are known (inclusive of setting risk tolerances and managing reputational risk). Examples of state/federal differences include California's law to phase-out sales of new gasoline powered vehicles, and Texas' prohibition on state agencies, local governments, and state pension funds contracting with or investing in firms that divest from fossil fuel energy companies.

Despite these challenges, regulators expect organizations to:

- Inventory 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.

Scrutiny and Divergence: 2023 Regulatory Challenges

Fairness and Inclusion: 2023 Regulatory Challenges

Challenge 5 Building ongoing ESG risk and compliance assessment and monitoring

Key Question: *Should the second line of defense 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 defense 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. 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 FS organizations underscore the importance of effective ESG monitoring and internal processes to mitigate inconsistencies in reporting, marketing, and 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).

The CCO and ESG

For more information, please contact Amy Matsuo, Adam Levy, or Chris Palumbo.

Contact the authors:

Amy Matsuo
Principal and Leader
Regulatory & ESG Insights
amatsuo@kpmg.com

Adam Levy
Principal
Modeling & Valuation
adamlevy@kpmg.com

Chris Palumbo
Managing Director
FS Risk, Regulatory & Compliance
christopherpalumbo@kpmg.com

kpmg.com/socialmedia