The SOXification of ESG

ESG disclosure regulatory update and governance evolution

November 14, 2023

Environmental, social, and governance (ESG) reporting has become increasingly important for companies with a global footprint, as investors demand more transparency and accountability on ESG issues. With increasing climate regulations across jurisdictions, companies must focus on both meaningful ESG reporting and efficient internal controls that can free up their resources and drive decarbonization, social expansion, and supply chain improvements.

This webcast discussed the emerging best practices around ESG governance and its key components with a focus on internal controls.

The panelists addressed the following topics:

- The rapidly changing ESG regulatory environment
- Strengthening ESG reporting assurance
- Establishing good ESG governance principles
- Internal controls over sustainability reporting (ICSR)

The rapidly changing ESG regulatory environment

As ESG reporting requirements evolve, organizations face a growing challenge to keep up with different regulations implemented across various countries and regions. The involvement of multiple regulatory bodies, such as the International Sustainability Standards Board (ISSB), the US Securities and Exchange Commission (SEC), and California State Regulations, adds to this complexity. In particular, the SEC's climate change proposal is a key component of the regulatory agenda, alongside social and human capital, and corporate board diversity. To succeed in this uncertain environment, organizations must monitor the requirements impacting their business, while paying attention to supply chain management and procurement.

Organizations must identify people to lead ESG reporting regulations in their company and adopt a collaborative approach focused on proper disclosure preparation. Companies must also consider the assurance requirements that will drive their control responses. By having efficient internal controls in place and a clear understanding of the regulatory landscape, companies can focus on meaningful ESG reporting without sacrificing resources that could be used for decarbonization, social expansion, or supply chain improvements. As the expectations for ESG reporting continue to rise, developing a comprehensive understanding of the complexities of mandatory requirements and creating efficient internal controls is critical to responding to these changes and improving ESG performance.

Strengthening ESG reporting assurance

The world of ESG reporting is complex, but understanding the diverse external assurance standards is crucial. It is important to understand the key role of auditors in ensuring robust controls and prioritizing governance in the reporting journey.

Limited vs. reasonable assurance

To effectively implement controls, it is important to strike a balance between the need for controls and the desire to not impede the organization's initiatives. As many companies are not used to the level of controls required for ESG reporting, it may take time to implement effective controls.

Limited assurance: In limited assurance, external auditors will perform a less comprehensive examination of a company's reporting or audit, similar to a quarterly review of financial statements. This involves verifying numbers and supporting documentation without extensive testing of controls. The focus is primarily on assessing whether everything is directionally good and if any material updates are necessary. However, presenting a clear and well-articulated process and controls framework can make the audit smoother.

Reasonable assurance: In reasonable assurance, auditors will perform a deeper level of examination, similar to a 10k audit. This involves a more thorough analysis of a company's reporting and audit, including a controls-based approach and testing to reduce substantive testing requirements. To meet the reasonable assurance standard, auditors will examine a company's risk assessment processes, test controls, and monitor control processes.

Internal assurance over ESG reporting

Companies need to develop trusted processes and controls to mitigate risk and provide assurance in their ESG reporting.

Governance and strategy: The direction and level of effort for the ESG internal assurance program are set by determining its overall strategy. This involves addressing critical questions such as the level of assurance required for non-regulated metrics and the involvement of the 2nd and 3rd lines in monitoring activities.

Scope: Scoping ESG by material items, entities, and value chains will ensure that a complete picture of the ESG impact of a company is identified. Not all ESG risks are equal. The level of assurance needed will differ based on area and strategy.

Risk assessment: Risks need to be considered in several areas: strategic, financial, operational, compliance, technology, data, human capital, reputation and external. Focusing on the process alone will be insufficient.

Process and controls: Once risks are considered, processes will need to be mapped and controls identified commensurate with the risk and level of assurance needed. Ongoing execution of key controls is important to achieving investor-grade disclosures.

Tech and data: The data foundation for monitoring performance and reporting is critical to assurance. Data security, integrity, and governance need to be considered for technology enabling the collation, calculation, and reporting processes.

Monitoring: Monitoring the successful execution of key controls is an important step to examining the level of risk and control within the ESG reporting process. Develop a testing strategy to determine the level of monitoring based on risk and level of desired assurance.

Oversight: Robust reporting of any control deficiencies identified within the ESG environment is key to maturing the control environment and providing the Board and Executive management with the information they need to provide sufficient oversight.

Establishing good ESG governance principles

Understanding key governance principles is critical for promoting sound governance practices and achieving organizational goals and objectives. The following are the four essential elements of good governance:

Structure and oversight: Successful organizations establish a clear corporate strategy and objectives monitored by managerial roles with defined responsibilities. Policies, procedures, internal controls, and internal audits are established in a framework to support compliance, transparency, and effective risk management. The board has oversight responsibilities and receives appropriate training and reports to help maintain the effectiveness of governance processes.

Code and values: Organizations that prioritize code and values foster positive and ethical work environments, ensuring that their employees are engaged and incentivized to contribute to their strategic goals. They establish a strong organizational culture with shared values, beliefs, and practices that support their mission, encourage innovation and growth, and promote ethical and socially responsible behavior.

Transparency and reporting: To ensure transparency, organizations require effective governance and internal monitoring of transformation initiatives, while providing stakeholders with accurate and reliable reporting of their performance and risks. Trusted reporting is achieved through the presence of robust reporting governance structures, data governance, and proper internal controls and procedures.

Risk management: Effective risk management entails implementing an integrated framework to identify, assess, and manage all types of risks across the organization, focusing on the overall level of risk-taking rather than isolated risks from specific areas. Additionally, regulatory compliance with laws, industry standards, and governance over data, cyber, and generative AI is critical in mitigating potential risks and ensuring the organization's overall resilience.

Structuring an operating model for ESG reporting

The responsibility for ESG reporting has transitioned from sustainability leaders to finance leaders, positioning the CFOs or CIOs to directly oversee the reporting beneath them. The ESG reporting framework comprises representatives from all functions, including legal, investor relations, tax, and HR, providing inputs for efficient reporting. The target operating model is designed to ensure compliance with global regulations and create the most efficient reporting structure. Businesses can follow these three steps to structure their operating models to enable efficient ESG reporting, where each step can be configured in various ways:

Finance-led: Having a single owner for financial and ESG data can offer benefits such as comprehensive reporting and analytics capabilities, leveraging existing finance systems, and a pre-existing controls framework. However, it can also bring additional workloads for finance teams who may not have access to data sources and require up-skilling for non-financial ESG topics.

Centre of Excellence (CoE): A single central hub for all ESG capabilities can offer benefits such as cross-functional collaboration, a “single source of truth” for ESG data, and simplify ESG-related initiatives. However, there are challenges to address, such as different owners for financial and ESG reporting, the need to build reporting and controls expertise outside of finance, and variations in CoE reporting lines and locations.

Sustainability-led: Having ESG ownership from experts and functional leaders can help maintain existing finance structures, require minimal upskilling, and link ESG to overall business strategies. Yet, having separate owners for financial and ESG reporting and needing expertise beyond finance can be difficult. Overall, this approach can help companies integrate ESG into business strategies while maintaining finance structures.

Internal controls over sustainability reporting (ICSR)

ESG reporting and internal controls can be complex, but the benefits of accurate and comprehensive reporting are significant for organizations and stakeholders alike. Leaders can begin by documenting their current practices related to ESG reporting and establish minimum internal control standards. Organizations should also be transparent about assumptions and estimate approaches, and periodically assess and update their internal controls to reflect changing circumstances.

To further improve ESG reporting capabilities, a tailored internal assurance framework can be developed based on the organization's specific circumstances and challenges. By establishing entity-level controls, ESG reporting level controls, and metric collation processes, an efficient reporting process can be achieved. Adopting minimum controls standards that enforce data consistency creates a solid foundation for ESG reporting that will help organizations navigate this complex landscape and enhance their ESG reporting capabilities.

Committee of Sponsoring Organizations (COSO) components and principles

The COSO Framework is the control framework used by the majority of US public filers, and it can also be applied to ESG reporting. Although there is interpretive guidance available, it is the same framework applied to traditional reporting. To determine what "good" ESG reporting looks like, companies should leverage their existing entity-level control environment used for SOX compliance and identify any changes or new additions needed. Controls professionals should consider both existing and new ESG reporting risks when building out internal controls. Key components include:

Control environment: Conduct a comprehensive evaluation of the organizational structure, addressing areas impacted by current and pending regulations. Simultaneously, focus on hiring, training, and retaining skilled individuals, while establishing clear roles and responsibilities, and define realistic metrics to safeguard against fraudulent reporting pressures in the ESG domain.

Risk assessment: Define sustainability reporting objectives in detail for thorough risk assessment, analyze material risks, consider potential fraud risk, and continuously monitor for changes affecting the objectives.

Monitoring activities: Consider expanding the role of internal audit functions to collaborate with leadership to build an efficient, effective, risk-based ICSR portfolio and expand internal audit's role to assess the design, implementation, and effectiveness of ESG data controls before external assurance.

Control activities: Design a scalable ICSR program with controls addressing future commitments, prepare control performers for assurance requirements, and update policies, procedures, and training regularly to achieve ESG reporting objectives and support potential assurance needs.

Information and communication: Integrate sustainability data capture and controls into future system discussions to scale technology appropriately while also gauging the data's consistency, veracity, and completeness for ICSR, and implement controls to mitigate inaccuracies or missing ESG data.

Navigating the complexities of ESG reporting

As ESG factors continue to gain traction globally, organizations are under increasing pressure to improve their reporting practices. From streamlining data sourcing to strengthening internal controls, there are several approaches companies can take to effectively navigate the evolving ESG reporting landscape.

Optimizing ESG reporting through automation and data sourcing: By streamlining data sourcing processes and implementing automation, organizations can efficiently meet global ESG regulatory requirements. This approach not only ensures compliance but also reduces the burden of reporting timelines and manual efforts.

Enhancing internal controls for an effective ESG strategy: Organizations can enhance their ESG strategy by providing internal controls training to relevant teams, including ESG professionals, front-end control owners, and risk management. This approach helps build robust internal control structures, improve ESG risk management, and increase compliance and reporting effectiveness.

Streamlining ESG data aggregation through technology: Technology can help streamline data aggregation with strong internal controls and auditability measures in place. Selecting providers that offer a SOC 1 Type II report for calculations and validation controls can reduce reliance on manual processes and improve overall ESG performance.

Strengthening ESG reporting through robust internal controls: Organizations can mitigate ESG reporting risks and streamline validation efforts by prioritizing the design of robust internal controls. This approach promotes the accuracy and completeness of ESG metrics while ensuring a smooth validation process, reducing the burden on reporting teams.

Future-looking statements/ESG targets: To improve their ESG performance and reputation, organizations should adopt a future-looking approach to ESG targets and implement robust project management protocols for effective monitoring and communication of progress. This provides executives with the necessary oversight and enhances comfort when they speak to the company's ESG strategy.

Establishing policies and procedures for comprehensive ESG reporting: By establishing formal policies and procedures that define ESG metrics, organizations can enhance their ESG disclosures, including data with disaggregated finance structures. This approach improves the accuracy and completeness of ESG reporting while ensuring consistency across multinational organizations.

Assurance readiness: Organizations can improve ESG performance and reduce risks by prioritizing assurance readiness practices for efficient third-party auditing and alignment with regulatory requirements.

Navigating the evolving ESG reporting structure: Examining ownership of ESG reporting and considering bifurcated ownership between financial reporting/accounting and legacy ESG teams is critical. This approach enables appropriate delegation of responsibilities and accountability while maintaining consistency across reports.

Developing a comprehensive ESG internal assurance plan: To ensure effective internal assurance over ESG metrics, it is crucial to establish a robust strategy that includes risk assessment, documentation, and testing. This involves defining clear roles and responsibilities, determining the timing of the assessment, and ensuring the reliability of the results.

Closing comments

The landscape of ESG reporting is constantly evolving, and it is important for companies to stay informed and adapt to thrive. By establishing a strong governance structure, companies can ensure the accuracy and reliability of their ESG reporting while also meeting the demands of investors and stakeholders. Companies need to continue developing a better understanding of the changing regulatory landscape, adopt a collaborative approach, and keep their reporting and controls processes up-to-date to ensure compliance and become resilient.

Sue King
Partner and SOX
Solutions Lead
KPMG LLP

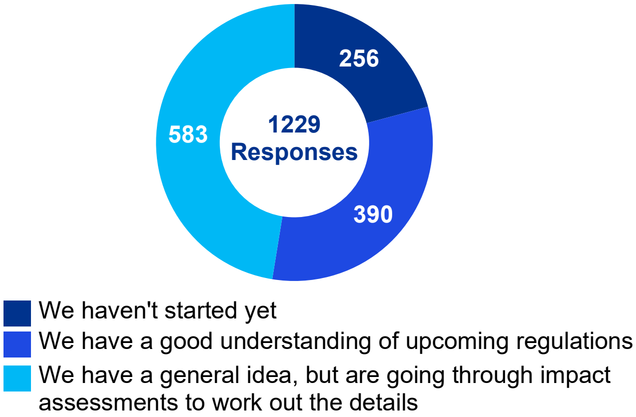
Steve Estes
Partner and Internal
Audit & Enterprise
Risk ESG Lead
KPMG LLP

Debbie Biddle-Castillo
Managing Director,
Internal Audit &
Enterprise Risk
KPMG LLP

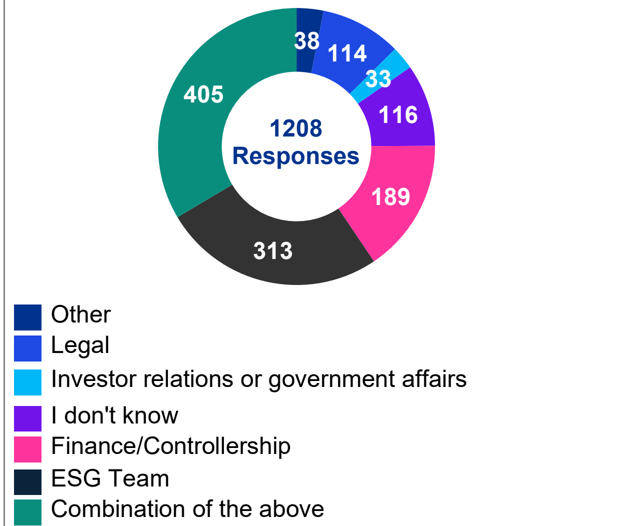
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

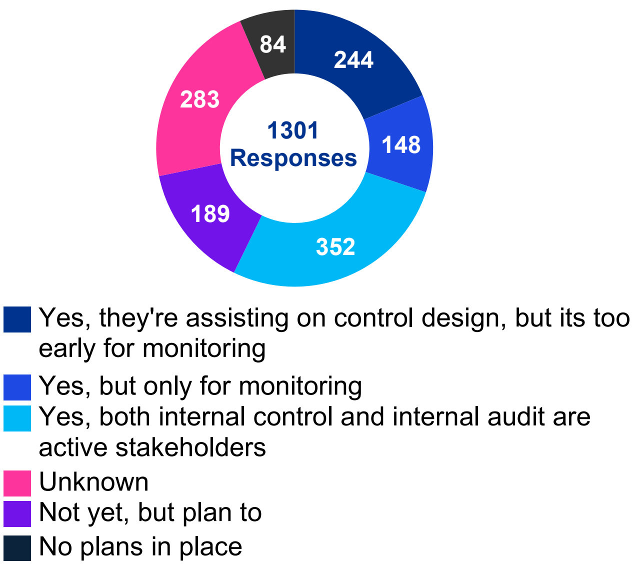
My company has a good understanding of which ESG regulations we will be required to comply with.



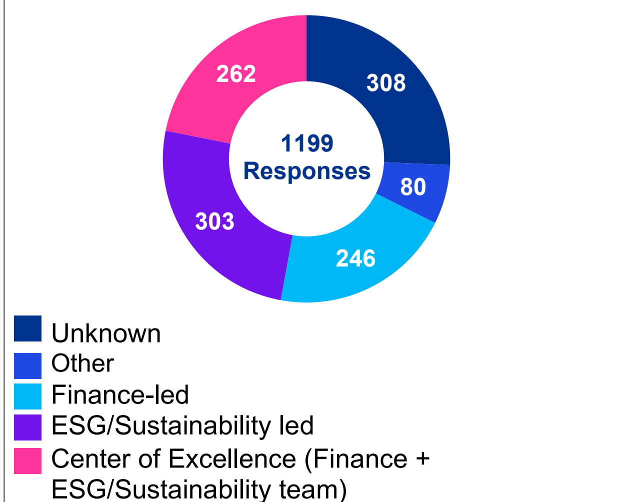
Who in your company is leading the response to ESG reporting regulations?



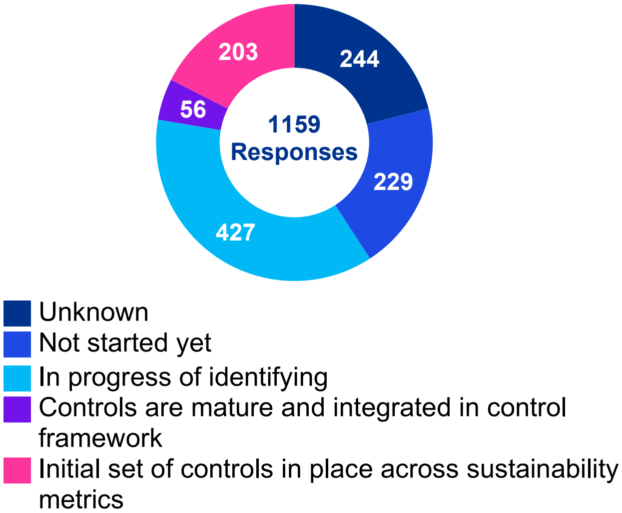
Is your internal control or internal audit function engaged to assist with the establishment of an internal assurance framework over ESG reporting, i.e. control design or monitoring activities?



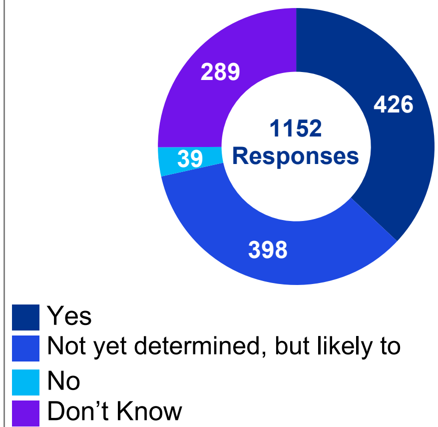
Which reporting structure is your company adopting for ESG reporting?



Where is your company in the process of establishing internal controls over sustainability reporting?



Does your company plan to use the COSO framework as the controls framework for internal controls over sustainability reporting



What are the biggest challenges that you are experiencing to a trusted ESG reporting process