The "SOXification" of ESG reporting

Are you ready for it?

Our world is going through immense change, driven by a global pandemic, changing work habits, differing political perspectives, and regulatory and global climate changes. Environmental, Social and Governance (ESG) encapsulates all of these and more as companies articulate their goals and efforts to address these issues via public sustainability reporting. With the broad range of topics and rate of change, having a strong process and control environment around this reporting will not come easily.

In a recent KPMG webcast, KPMG SOX Solution lead partner, Sue King, stated, "As difficult as it was to implement Sarbanes-Oxley (SOX) controls over financial reporting, implementing controls over ESG reporting will be infinitely more challenging."

When implementing Internal Controls over Financial Reporting (ICFR), the underlying financial statements had previously been audited, and there were clearly defined accounting frameworks, principles, and policies, but when it comes to ESG, most companies have not formally adopted any of the various reporting frameworks (such as Sustainability Accounting Standards Board, Task Force on Climate-Related Financial Disclosures, Global Reporting Initiative, etc.), have not developed their own policies, and those areas have not been subject to audit. "As a result, given ESG includes a lot of nonfinancial metrics, defining, measuring, and reporting on them is going to be much more difficult," King also says.

So let's take a closer look at ESG reporting—what it is, why it's become such a hot topic to companies of all sizes and across all industries, its potential impact on your internal controls framework, and what you should be doing about it.

Growing importance of ESG

There are three pillars of ESG reporting. **Environmental** deals with practices around conservation, climate change, emissions, and so on. **Social** addresses the treatment of people—customers, the public, and employees—and topics like diversity, labor standards, privacy, and human rights. **Governance** focuses on the standards of running a company, and includes board composition, bribery and corruption, political contributions, and lobbying efforts.

> **"As difficult as it was to implement Sarbanes-Oxley (SOX) controls over financial reporting, implementing controls over ESG reporting will be infinitely more challenging."**
>
> **—Sue King,**
> KPMG SOX Solution Lead

According to a recent KPMG survey, nearly 95 percent of financial and other professionals reported that they don't know enough about the topic of ESG and over 70 percent aren't comfortable with their ESG reporting program in terms of having appropriate internal controls in place.[1]

Why ESG? Why now?

Current and potential investors are asking pointed questions about a company's ESG commitments and actions. Banking institutions and investment companies like Blackstone, BlackRock, and State Street are increasingly asking questions and demanding actions from companies on their commitment to ESG. As a result, public companies are increasing the amount they are disclosing (e.g., in sustainability reports, including comments in their earnings calls, discussions in MD&A, etc.) related to their ESG commitments and achievements.

How this translates into action by the U.S. Securities and Exchange Commission (SEC) is yet to be determined, but it seems reasonable to assume that if companies are disclosing information to investors about steps they have taken to improve their environmental impact or increase diversity, the SEC expects that there are strong controls in place to ensure that the ESG data being communicated is complete and accurate and is governed by appropriate internal controls.

This is where ESG policies, processes, and an internal control framework come in.

The challenge in implementing internal controls over ESG reporting

With SOX compliance, you're dealing with financial information typically generated by finance professionals and accountants, yet it still took companies many years to implement robust ICFR programs. With ESG metrics, you are generally dealing with nonfinancial data generated by various groups that aren't as experienced being audited and implementing repeatable internal controls processes.

"We've learned from SOX implementations that the closer you are to the accounting function, the easier it is to implement internal controls. The further you move away from it—working with the supply chain, operations, or IT departments—the heavier the lift. That's because you're no longer working with accountants who are used to being audited and generally keep rigorous, complete, and accurate reconciliations and supporting documentation."

—Steve Estes, KPMG partner, Internal Audit ESG lead

[1] Survey of more than 3,000 financial and other professionals across a variety of industries during KPMG webcast, ESG and internal controls: practical advice to prepare now (September 2021).

Initial areas to focus on as you consider internal controls over ESG reporting

Consider the following list of topics that are core elements of any ICFR program and how they apply to ensuring strong internal controls around ESG reporting.

Support for estimates and assumptions. Particularly with ESG data, various estimates and assumptions are often used in preparing the calculations. The rationale and support for such estimates and assumptions should be clearly documented and supported by reliable data.

Evidence of secondary review and approval. ESG data and reporting should be subject to reviews and approvals by appropriate reviewers to validate the data, calculations, and presentation.

Controls over third-party data. Regardless of if the data is coming from a third party, the company ultimately reporting has responsibility for its accuracy and needs to define consistent measurement of data from third parties.

IT general controls. Systems used for ESG data need to have appropriate IT general controls, including appropriate access controls.

Defined policies and procedures. Similar to accounting policies that document the specific principles and procedures for preparing and presenting financial statements, companies need documented definitions for measurement and principles for how their ESG reporting is prepared and presented.

Homogeneity across processes, locations, and countries. Companies should strive for activities that are truly homogeneous and consistently measured across processes and locations. Initially arriving at common policies to define how data is defined, measured, captured, and controlled will be a challenge.

Governance over disclosures. A governance process needs to be established to define policies, oversee the end-to-end ESG process from the definition of strategy through to the disclosures being made, and ensure there are appropriate controls throughout the process.

Completeness and accuracy controls around key reports. Appropriate controls should be in place to verify that reports used for ESG data and calculations accurately capture data in a consistent, complete, and accurate manner.

These are common topics and themes for those that have been involved with ICFR for the past 20 years, but applying those same concepts across a new set of nonfinancial controls for ESG is going to be a much larger challenge.

Who should lead ESG reporting efforts?

Historically, the communication and reporting of ESG metrics typically was headed by groups such as investor relations, marketing, legal, and/or operations. But as ESG has evolved into a hot topic, with stakeholders placing more emphasis on this topic and regulators asking more detailed questions about the basis for some of the ESG claims, many companies are moving this responsibility into the finance and accounting function. Often the SOX or internal audit function is being asked to expand their role into being the trusted internal control testing function for the company, to provide input on how to enhance the internal controls around ESG reporting, and to assist in formalizing the processes for collecting the data.

Get ready for tougher ESG reporting requirements

Admittedly, we're still in the early stages of ESG reporting requirements. The SEC has not yet defined the level of scrutiny to be applied to ESG reporting, such as the potential requirement for full attestation around ESG reporting. Whether we end up with SOX-like attestation requirements or not, it's clear that since companies are already disclosing ESG objectives and metrics, there needs to be strong internal controls around the data supporting those public claims. Such data needs to be subject to the same rigors as other data currently covered by disclosure controls to verify the data provided is both accurate and verifiable.

If you haven't already started thinking about ESG, how it impacts your company, and what you will need to do in terms of data gathering, recordkeeping, and reporting, you should get started. And if you have already taken steps in that direction, you'll want to consider what else you need to do to prepare yourself for meeting future requirements.

Learn more: visit.kpmg.us/FutureOfSOX

Connect with us

For more information on establishing or improving your internal controls program related to ESG, view our webcast, ESG and Internal Controls: Practical Advice to Prepare Now, or contact one of our professionals listed below:

Steven M. Estes
Partner, Advisory,
Internal Audit ESG Lead
T: 214-840-2448
E: sestes@kpmg.com

Sue King
Partner, Advisory,
SOX Solution Lead
T: 213-955-8399
E: susanking@kpmg.com

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

kpmg.com/socialmedia