Strengthen internal controls to navigate the "SOXification" of ESG reporting

kpmg.com

Introduction

Performance on environmental, social, and governance (ESG) factors has become a significant issue for companies, impacting financial resilience, growth, and stakeholder value. As ESG has grown in importance, reporting requirements are proliferating. Indeed, some internal audit leaders now talk about the "SOXification" of ESG"—impacting organizations the way Sarbanes-Oxley did in 2002.

The European Union has implemented broad reporting requirements on environmental, social, and governance performance. In October 2023, California adopted broad climate reporting laws that will require large businesses (both publicly traded and privately held) to report on greenhouse gas (GHG) emissions and climate-related financial risk.[1] These laws join a suite of sustainability reporting requirements covering GHG emissions and climate-related financial risks and may shape climate reporting in other states and influence regulation at the federal level. According to a KPMG study, by 2022, 96 percent of the world's top 250 businesses and all of the top 100 U.S. companies were producing voluntary annual sustainability reports.[2]

By 2022, virtually all large U.S. companies were producing voluntary sustainability reports.

However, most organizations struggle to address the higher levels of transparency and integrity required with new regulations. This has placed pressure on companies to focus on the robustness of process and controls to meet these higher expectations and to communicate their strategies.

In this paper we describe how companies can apply the internal controls used for other financial reporting to efficiently meet ESG reporting requirements and effectively carry out ESG strategies.

[1] See, KPMG Regulatory Alert, October 2023

[2] KPMG, "Big shifts, small steps: KPMG's 2022 global survey of sustainability reporting," 2022.

The growing reporting challenge

Corporations face a growing list of reporting requirements from regulators, even as investors press for more thorough and verifiable voluntary reporting. In January 2023, the European Union finalized the Corporate Sustainability Reporting Directive (CSRD), which requires in-scope companies to disclose data on a broad set of sustainability topics. In July 2023, the EU enacted the European Sustainability Reporting Standards (ESRS), one of the most far-reaching regulations to date, which applies to organizations subject to the CSRD. Multinationals that are not listed on European exchanges may need to meet the CSRD requirements and, according to one estimate, 3,000 U.S.-based companies could be affected.[3]

In the U.S., the Securities and Exchange Commission issued proposed sustainability reporting rules in 2022, but the final rules are still pending. Meanwhile, a new Federal Supplier rule requires sustainability reports from public and private suppliers whose annual billing exceeds a specified threshold.[4] Then, in October 2023, the State of California became first in the nation to adopt greenhouse gas emission reporting laws that will require large public and private companies to disclose climate-related financial risks and publicly disclose GHG emissions.

Organizations outside the scope of the SEC and CSRD may be required to adopt sustainability disclosure standards issued by the International Sustainability Standards Board (ISSB). The ISSB is an independent, private sector organization that collaborates with national leaders to develop and approve International Financial Reporting Standards (IFRS) sustainability disclosure expectations. So far, the ISSB has released two IFRS for sustainability disclosure, establishing a new reporting standard that integrates sustainability reporting with traditional financial reporting.

Adhering to complex disclosure requirements can be daunting for companies. Many businesses are unsure which regulations apply to them, whether they are tracking appropriate sustainability-related information, or if their data is accurate.

The stakes for inaccurate reporting will rise dramatically when companies file sustainability reports with the SEC alongside other financial reports. Failure to comply with SEC reporting rules can result in fines. In 2022, the SEC collected a record $4.2 billion in penalties.[6] Penalties for failure to properly disclose in California can be as high as $500,000 per year. Fines can also result in negative publicity, brand damage, or loss of stakeholder trust. With mandatory ESG reporting deadlines fast approaching, organizations must prepare now by assessing their existing internal controls and ensuring a compliant architecture. Internal processes must adhere to current regulations and be flexible enough to satisfy future ESG reporting requirements.

> **“Proactively addressing emerging disclosure gaps that threaten investors and the market has always been core to the SEC’s mission.”**
>
> —Kelly L. Gibson, SEC Deputy Director of the Division of Enforcement

[3] Avery Ellfeldt, “U.S. companies scramble ahead of EU climate disclosure rules,” Climatewire, Oct. 17, 2023

[4, 5] “FACT SHEET: Biden-Harris administration proposes plan to protect federal supply chain from climate-related risks,” The White House, November 10, 2022

[6] “The effects of mandatory ESG disclosure around the world,” Harvard Law School Forum on Corporate Governance, May 10, 2021

Internal controls for sustainability reporting

Many businesses are reviewing their sustainability reporting processes to meet new requirements. They are looking to improve internal controls over sustainability reporting and align that reporting more closely with the approach used in financial reporting. However, there are significant pitfalls to avoid and pain points to address.

Pitfalls and pain points

- Inadequate or incomplete risk assessment
- Disconnect between ESG targets and business strategies
- Insufficient commitment from board members, leadership, and employees
- Unclear roles, responsibilities, and delineation of duties
- Difficulty establishing materiality
- Inadequate processes and controls for data gathering, validating, and reporting
- Too much time and resources spent on data collection and verification
- Incomplete documentation and communication
- Limited monitoring and oversight
- Participants in the reporting process lack knowledge or experience with robust internal controls

Organizations that understand these potential obstacles can address them pre-emptively when implementing a more robust and resilient control environment.

The ESG internal controls maturity continuum

Businesses should start by reviewing existing controls for financial reporting to see which can absorb new ESG requirements. Organizations must design and implement new controls if current protocols do not cover ESG metrics before regulatory deadlines occur. Companies also need to determine if existing procedures can report ESG data accurately. Since control processes vary in resource requirements, organizations should refine them to accommodate changing regulations or executive expectations. ESG controls today range in maturity as described below:

01 Fragmented

- Manual data collation for ESG metrics with little or no focus on controls
- Undefined or inconsistently retained documentation for metrics

02 Detective

- ESG control environment depends on manual validation by an ESG reporting or internal auditing team
- Controls and supporting documentation are not considered or defined

03 Compliance-based

- ESG metrics against regulatory requirements adhere to controls throughout the data collation process
- Supporting documentation is consistently defined and retained for regulated metrics only

04 Risk-based

- Implementation of a control strategy across the ESG reporting landscape
- ESG metrics are risk-assessed and supported by controls in the data collation process. Regulated and unregulated metrics have proper documentation

05 Integrated

- ESG controls exist within the organization's process and monitoring frameworks
- Documentation maintenance meets company standards and operating procedures
- The monitoring process adheres to controls defined by an organization's monitoring strategies

A roadmap to internal controls sustainability reporting (ICSR) compliance

Whichever maturity level an organization desires, setting up internal controls for sustainability reporting requires a systematic approach that aligns with the organization's overall ESG objectives, strategy, and risk management framework. Organizations can take several steps to establish an effective internal control environment for ESG reporting and compliance.

Roadmap to ICSR compliance

1. Pre-readiness assessment to understand all regulations that apply to the organization.

2. Materiality assessment to determine ESG focus areas based on regulatory requirements and priorities for the organization and its stakeholders. Organizations should use the results of the materiality assessment to establish an ESG strategy that outlines its vision, goals, and priority topics for designing and implementing internal controls.

3. Gap analysis against regulations and priority topics identified in the materiality assessment to understand the organization's reporting requirements and readiness. The study can serve as a roadmap for gap remediation, including those in the control environment.

4. Appoint governance and resources over ESG reporting in an organizational structure that supports accountability and decision making related to upcoming reporting requirements.

5. Processes and data mapping should be documented to support measurement and reporting.

6. Audit readiness of ESG reporting should be assessed regularly by an internal audit that encompasses ESG data, controls, and reporting to identify gaps, weaknesses, or inconsistencies. Organizations should use these assessments to drive continuous improvement in ESG reporting practices.

7. Integration with management reporting must give organizational leadership confidence in the accuracy of ESG-related metrics and assertions published by the company.

In 2023, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released guidance on how to apply its internal controls framework to ESG information. COSO is well known for its Internal Control–Integrated Framework (ICFR), a leading choice for designing and implementing internal controls. The proven success of COSO ICIF in both financial and non-financial reporting, as detailed in our paper COSO ICIF for ESG Reporting: Building confidence in sustainable business information through the COSO framework, describes why it is an ideal tool for creating and implementing a solid control structure for ESG reporting.[7]

[7] KPMG LLC, "COSO ICIF for ESG Reporting," April 2023.

Becoming assurance ready

Organizations must prepare for ESG reporting scrutiny by external assurance programs, which impending regulations require. External assurance enhances the credibility and reliability of the organization's reporting and helps identify when a business should dedicate additional resources to that process.

Internal assurance and confidence in sustainability reporting need to exist before companies pursue external assurance.[8] Organizations can start by engaging their internal audit or compliance teams to evaluate the control environment for ESG reporting independently.

Companies should assess whether controls can mitigate relevant ESG risks, determine their operational effectiveness, and make recommendations for improvement. Any findings can help a business to improve its control environment by preventing or detecting errors and irregularities and achieving compliance with legal, regulatory, and ethical standards. Internal assurance can help executives increase their confidence that the ESG reporting is factual, complete, and accurate before bringing in a third party to provide external validation.

> Internal assurance and confidence in sustainability reporting need to exist before external assurance.

[8] See: "COSO ICIF for ESG Reporting," KPMG LLP, April 2023.

Limited vs. Reasonable Assurance

Regulations will increase the level of assurance required for ESG reporting, starting with **limited assurance** and moving to **reasonable assurance**. The level of assurance reflects the confidence that auditors have over the data. The phase-in approach gives companies time to improve their data and underlying processes to demonstrate compliance.

Limited Assurance	VS	Reasonable Assurance
Provides a lower degree of confidence but is easier to achieve compared to reasonable assurance. Auditors should perform limited procedures to identify material inconsistencies or instances that might cause data reporting accuracies.		**Provides a higher degree of confidence** in the effectiveness of internal controls, making it the primary choice for financial statement audits. Reasonable assurance involves more extensive audit procedures to reduce the risk of material misstatement, efforts, or fraud in reporting to an acceptably low level. The scope of the assurance can vary depending on the regulation and the auditor. However, an organization needs to have confidence in its system of internal controls before pursuing third-party validation.

How KPMG help

The evolving expectations around ESG reporting can be daunting, and most organizations have a significant amount of work ahead to prepare verifiable data for compliance. While some organizations can leverage existing internal controls for financial reporting to absorb new ESG requirements, many need to establish new internal controls over the ESG data. Organizations must start preparing to design and implement comprehensive internal controls to meet regulatory deadlines. Building and maturing the internal control environment will take time and needs to be supported by adequate change management as well as ongoing training and support. Setting up an effective system of internal controls will enhance the credibility and reliability of ESG data and bring value to the business.

KPMG can assist organizations every step of the way as they prepare for pending ESG regulations.

Our professionals can help you by:

01 Identifying which ESG regulations apply to organizations

02 Understanding the specific requirements and phase-in timelines

03 Reviewing the existing internal controls in place over ESG data and providing recommendations for improvement

04 Determining an organization's desired maturity level for ESG controls

05 Setting up a robust internal control environment, leveraging existing internal controls in place for financial reporting and external guidance where desired

06 Supporting an organization's Internal Audit function with subject matter expertise as it reviews the ESG control environment to prepare for external reporting

Effective internal controls can shield organizations from exposure to fines or other regulatory sanctions and help improve stakeholder trust and confidence.

Contact us

Ric Kimball
Service Network Leader, Internal Audit and Enterprise Risk, KPMG LLP
404-222- 3407
ekimball@kpmg.com

Steve Estes
Partner, Internal Audit ESG Solutions Leader, KPMG LLP
972-896-9476
sestes@kpmg.com

Sue King
Partner, SOX Solutions Leader, KPMG LLP
310-480-2145
susanking@kpmg.com

Aila Pallera
Principal, Internal Audit and Enterprise Risk, KPMG LLP
818-571-1165
cpallera@kpmg.com

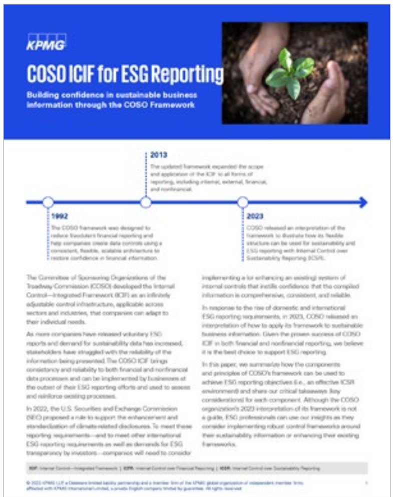
Debbie Biddle-Castillo
Managing Director, Internal Audit and Enterprise Risk, KPMG LLP
213-533-3375
dlbiddle@kpmg.com

Ivor O'Neill
Managing Director, Internal Audit and Enterprise Risk, KPMG LLP
614-241-4636
ioneill@kpmg.com

Rachel Horne
Director, Internal Audit and Enterprise Risk, KPMG LLP
305-913-3637
rehorne@kpmg.com

Special thanks to Matt Musgrave for supporting contributions.

Related thought leadership



COSO ICIF for ESG Reporting

ERM's role in ESG

Internal audit's role in ESG

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

kpmg.com/socialmedia

DASD-2023-13836