

# Discussion guide for internal control over sustainability reporting

No matter where a company sits in its maturity in establishing internal control over sustainability reporting, the points of focus and insights within the COSO guidance provide actionable tips to enhance the design and operating effectiveness of controls

**Below are key questions organizations and auditors (internal and external) can ask to assess the extent to which the existing controls address each of the five components and 17 principles of the integrated framework:**

Component: Control Environment	
Principles	Key questions
1. Demonstrates commitment to integrity and ethical values	<ul style="list-style-type: none"> <li>▶ How is the organization demonstrating its commitment toward integrity and ethical values with respect to sustainability?</li> </ul>
2. Exercises board of directors' oversight responsibilities	<ul style="list-style-type: none"> <li>▶ How does the entity ensure that considerations about climate change and other sustainability risks and opportunities are embedded into the entity's strategy and management of risks (or opportunities)?</li> </ul>
3. Establishes structures, authority, and responsibilities	<ul style="list-style-type: none"> <li>▶ Is the board of directors operating independently from management, and does it have the requisite expertise with respect to oversight and responsibilities for decision-making on ESG and sustainability issues?</li> </ul>
4. Demonstrates commitment to competent human resources	<ul style="list-style-type: none"> <li>▶ What structures, such as a designated committee or subcommittee, has the board of directors established to oversee the organization's ESG and sustainability activities and reporting, including the system of internal control? How is the audit committee involved in the oversight of external reporting?</li> </ul>
5. Enforces accountability	<ul style="list-style-type: none"> <li>▶ Is there a specific director, department or committee that is responsible for addressing and managing sustainability risks and reporting directly to the board/those charged with governance?</li> <li>▶ Has the organization developed and implemented policies and practices that communicate expectations regarding its personnel's competence with sustainable business management and information?</li> <li>▶ How do those charged with governance ensure that a sufficient level of skill, focus and resources is allocated to identifying climate-related and other sustainability risks (or opportunities)?</li> <li>▶ How does the organization hold individuals accountable for their internal control responsibilities related to ESG and sustainability objectives?</li> </ul>

## Component: Control Environment

- ▶ Do remuneration policies and agreements with key management personnel link explicitly to climate-related targets or other commitments? Are members of management's reward and incentive schemes based on their progress on reducing emissions/other commitments, or do they promote sustainable value creation? How does incentive-based compensation account for short, medium and long-term progress against goals?

## Component: Risk Assessment

Principles	Key questions
6. Specifies suitable objectives	<ul style="list-style-type: none"> <li>▶ Has the organization clearly specified its ESG and sustainability objectives and risk tolerances to enable the identification and assessment of related risks?</li> </ul>
7. Identifies and analyzes risks to meeting sustainable business objectives	<ul style="list-style-type: none"> <li>▶ Does the organization consider sustainable business risks both in terms of the potential effects on the company's operational and financial performance, as well as the effects on external parties (i.e., the concept of "double materiality")?</li> <li>▶ How does the organization identify and analyze risks to achieving its ESG and sustainability objectives and determine the appropriate response?</li> </ul>
8. Assesses fraud risk	<ul style="list-style-type: none"> <li>▶ Has the entity performed an assessment of the climate-related risks and opportunities over the short, medium and long term?</li> </ul>
9. Identifies and analyzes significant changes and emerging trends	<ul style="list-style-type: none"> <li>▶ How is the company identifying and assessing sustainability risks associated with third parties and suppliers in particular? How does the organization identify and assess risks regarding the accuracy and validity of claims related to sustainably within the supply chain?</li> <li>▶ Is the organization assessing its compliance with all applicable statutes, regulations and obligations, including not only mandatory disclosures under securities regulations but also compliance in a range of ESG areas, for example, energy, water, waste, health and safety, equal opportunity, anti-corruption, and modern slavery? How does the organization monitor for changes in legislation and regulations that are required within all operating jurisdictions for sustainability matters?</li> <li>▶ Does the organization estimate the potential effects of various scenarios on its sustainable business objectives, including both qualitative identification and, as appropriate, a quantitative assessment that monetizes the potential effects of the risks?</li> <li>▶ How is the organization assessing the pressures, attitudes/rationalizations and incentives for potential fraud risk factors aligned with the Association of Certified Fraud Examiners fraud taxonomy for sustainability?</li> <li>▶ How is the organization considering the SEC's anti-fraud provisions of the Securities Exchange Act of 1934 and related regulations (Section 10(b); SEC Rule 10b-5) and applicable state regulations related to material errors and omissions within sustainability reporting that would subject a company or its directors and officers to be held legally liable (regardless of whether the information is part of a regulatory filing or otherwise disseminated to the market, including on a company's website, press releases, product information, or other material)?</li> <li>▶ As conditions change, are the metrics or assessments of what information is material (under regulatory definitions) or decision is useful for management and other stakeholders reassessed?</li> <li>▶ What evidence demonstrates that the processes and controls are present and functioning?</li> </ul>

### Component: Control Activities

Principles	Key questions
10. Selects and develops control activities	<ul style="list-style-type: none"> <li>▶ How effective is the organization's system of internal control in countering risks and ensuring that oversight activities are responsive to ESG and sustainability business objectives?</li> <li>▶ To what extent does the organization rely on technology, including leveraging existing IT systems, for the collection, processing, reporting and security of sustainability information, and are there effective IT controls over these systems?</li> <li>▶ Is the organization over-relying on spreadsheets, email or cutting and pasting from one system to another, which poses risks to the preservation and integrity of information as it flows from the original source through categorizing, sorting, and analyzing until it reaches the ultimate user?</li> <li>▶ To what extent is the organization relying on third parties or outsourcing functions? Is the entity aware of its responsibilities for the accountability related to the use of third parties regardless of the size, sophistication, innovativeness or reputation of the vendor?</li> <li>▶ Has the organization created policies that facilitate management's decision-making on how it utilizes the control environment to respond to risks?</li> <li>▶ Is there documentation that is communicated internally to support the flow of information from source to report, and how often is the documentation updated for changes?</li> <li>▶ How often does the organization revisit the policies and procedures to respond to changing circumstances, objectives and risks?</li> <li>▶ What evidence demonstrates that the processes and controls are present and functioning?</li> </ul>
11. Selects and develops general controls over technology	
12. Deploys oversight through policies and procedures	

### Component: Information and Communication

Principles	Key questions
13. Uses relevant information	<ul style="list-style-type: none"> <li>▶ Does the organization have high-quality data that informs whether its processes are facilitating its ability to meet its ESG and sustainability objectives, goals, targets and commitments?</li> <li>▶ How are the structures and policies communicated throughout the organization to facilitate the understanding of roles and responsibilities for meeting ESG and sustainability objectives, goals, targets and commitments?</li> <li>▶ Is the sustainability information communicated to external parties, such as debt and equity investors, regulatory bodies, customers and other stakeholders, reliable and sufficient to meet their needs?</li> <li>▶ What evidence demonstrates that the processes and controls are present and functioning?</li> </ul>
14. Communicates internally	
15. Communicates externally	

### Component: Monitoring Activities

Principles	Key questions
16. Conducts ongoing and/or separate evaluations	<ul style="list-style-type: none"> <li>▶ What types of reviews are conducted to assess how well the organization's oversight systems regarding its ESG and sustainability activities are functioning?</li> <li>▶ Is the frequency of review activities sufficient to identify emerging demands and drivers for change that may require a reassessment of the effectiveness of existing processes?</li> <li>▶ Does the entity have any new technology enablement or data analytics to help facilitate the monitoring of any planned changes to commitments or disclosures?</li> <li>▶ How is the company monitoring sustainability risks associated with third parties and suppliers in particular?</li> <li>▶ How does the organization communicate control deficiencies and observations identified to drive corrective action and continuous improvement?</li> <li>▶ What evidence demonstrates that the processes and controls are present and functioning?</li> </ul>
17. Evaluates and communicates deficiencies	

## **EY | Building a better working world**

**EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.**

**Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.**

**Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.**

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2023 Ernst & Young LLP.  
All Rights Reserved.

US SCORE no. 20121-231US

2305-4247540  
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

**[ey.com](https://ey.com)**