Douglas Hileman Consulting, LLC
Van Nuys, CA 91405-4235
www.douglashileman.com

June 9, 2025

Committee of Sponsoring Organizations (COSO)
www.coso.org
Submitted online, with comments

Subject: **Corporate Governance Framework**
Public Exposure Draft, released May 27, 2025
DHC Comments

I have worked in the field of compliance, risk, reporting and disclosures, auditing, and assurance over my career of more than four decades. I worked at a Big 4 firm for six years, and was on the Volkswagen Monitor Team for three years. I have specialized in environmental, safety, sustainability (including most recently climate/ GHG emissions). I am also an author of COSO's "Achieving Effective Internal Controls over Sustainability Reporting (ICSR)", released to wide acclaim in 2023. Douglas Hileman Consulting LLC (DHC) is pleased to submit comments on this document. These comments are my own, and do not necessarily reflect those of any client or professional association.

COMMENDATIONS

The draft CGF is an extraordinary document. It is a much-needed companion to COSO's Internal Controls Integrated Framework (ICIF) and the Enterprise Risk Management (ERM) Framework.

Professionals have spoken of "GRC" for many years; the Governance Framework is a worthy addition to round out the set.

- As with COSO's other marquee documents, the CGF is organization-neutral. It can be scaled to apply to organizations large or small, for-profit or non-for-profit, or public or private.
- The CGF organization is thoughtful and logical. The graphic is distinct from the time-honored COSO "cube" (ICIF) and the latest iteration of COSO's ERM guidance graphic. The nature of governance is different, so it must be so.
- The CGF is comprehensive. It is written in a style accessible to board members, executive management, and anyone involved or interested in governance.
- The convention of providing Deeper Insights and Leading-Edge Considerations as call-out boxes is an excellent way to provide additional insights. They are all practical examples.

SUGGESTIONS

DHC offers no suggestions as corrections to the draft CGF.

DHC offers some suggestions to enhance the quality and usefulness of the document. All of these could be achieved via Deeper Insights or Leading-Edge Considerations call-out boxes.

Business Case for COSO's Corporate Governance Framework (p. viii)

Suggestion: Provide more context regarding the dynamic, more complicated way of business.

Draft text: New section heading: The Nature of Business is Complex and Dynamic

The very nature of business has changed in recent decades; the pace of change shows no signs of slowing down. The majority of market capitalization is intangible value. Supply chains have become more complex, and span the globe. So do the value chains. Organizations no longer simply procure a part or a service from suppliers; they are expected (and in some cases required to) exert influence or monitor how third parties conduct their business. The scope and applicability of laws and regulations extend beyond the geography where an organization does business. There has been a proliferation of voluntary standards and frameworks; some have become widely accepted and are now incorporated by reference into regulations. Emerging issues become mainstream risks, requirements and opportunities in ever-shrinking timeframes: climate risk; cybersecurity; and now AI. Processes for compliance and risk management can no longer be linear. They are complex, and changing. A common, comprehensive governance model can be an effective way to ensure organizational continuity and value.

Rationale: The rationale is embedded in the draft text. The business landscape is a precursor to the risk landscape, and supports the point that issue-specific governance is increasing in complexity. The nature of business has changed considerably since COSO published ICI and ERM. Even I organizations have adopted ICIF (and even if they have embraced ICSR) and ERM, this is no longer sufficient. DHC suggests this context will make adoption of the CGF more compelling and far-reaching.

Principle 5, Communication; Introduction and elsewhere.

Suggestion: Add content to differentiate of "disclosures" and "reporting".

Draft Text: Defer to the CGF author team.

Rationale: The exposure draft includes mentions of "disclosures" and/or "reporting" – sometimes individually, sometimes together. The document does not explain the difference between the two.

- "While some **disclosures** are required by regulations …" (introduction to Communication component, p. 34). [emphasis added]
- POF 17.1 expands, with "The board or responsible committee reviews … accuracy of financial **reports**, strategic updates and operational **disclosures**."
- POF 20.1 says "Executive management oversees … external **reports, disclosures**, and communications." (p. 39).
- POF 20.2 [Board oversight of external communications] says "Directors understand their oversight role with respect to the entity's various types of external communications, from regulated filings to **disclosures** such as sustainability reports …" (p. 40). DHC notes that Sustainability reports and disclosures can also be mandatory, as compelled by industry standards, business partners, or customers.
- POF 20.3 (Disclosure committee) says "Executive management establishes a dedicated committee that oversees the entity's external **reporting and disclosure** practices …" The Leading Edge Considerations text box on this page is an excellent call-out for board to expand the role of Disclosure committees to go beyond financial topics.

DHC observes that professionals in the Sustainability field routinely conflate the two. This poses challenges for preparers, analysts, groups establishing standards or frameworks, other users, internal management (second line) auditors, Internal Audit, and external validators, verifiers and assurance providers. Conflation extends to understanding the financial side. Financial auditors, public accountants and finance professionals may understand the difference between "reporting" and "disclosures". Others do not.

My AI friend Gemini notes that "while often used interchangeably in everyday language, "reporting" and "disclosures" have distinct meanings in the context of financial accounting *and corporate governance*." The CGF Glossary includes an outstanding definition of "disclosures." It expressly notes that disclosures can be mandatory or voluntary, "such as sustainability reports." However, there is no definition of "report" or "reporting." COSO is the ideal entity to highlight the distinction. The CGF is the ideal place to do it.

Please add a definition of "report/ reporting" to the CGF. Please give another look where either/ both terms are used throughout the document, and modify as appropriate.

Principle 1 (Oversight), Point of Focus (POF) 1.5 – Board Committee structure, roles …

Suggestion: Include Sustainability reporting and disclosures among the roles and responsibilities that should be assigned to an appropriate the board. This could be an addition to the Deeper Insight "Additional Board Committees" or a new Leading Edge Consideration box.

Draft text: [as a bullet point] A Sustainability Committee to monitor drivers, risk management, compliance, reporting and disclosure of Sustainable business information. This Committee can also oversee the entity's approach to leveraging Sustainable business information to create value.

Rationale: Sustainability reporting began as voluntary reporting done by a few leading companies. It has evolved to be mandatory reporting required by law or regulation, as well as an array of voluntary reporting and communications. The scope of disclosure topics has grown; climate-related disclosures apply universally; others (human rights, product conformity, cybersecurity) vary by sector and industry. Furthermore, there is a range of reporting and disclosure channels, including public (to government entities, required disclosures on company websites) and non-public (B2B reporting and communications channels). The organization's ability to inspire confidence in investors and to engage in business activities depends on accurate, reliable and timely reporting and disclosures. Some companies have created positions for a Sustainability Controller; many others now place some Sustainability responsibilities with the existing Controller function. Indeed, COSO addressed this need with "Achieving Effective Internal Controls over Sustainability Reporting", released to wide acclaim in 2023[1]. The sprawling nature of Sustainability reporting and disclosure requirements, risks and opportunities make thoughtful governance an imperative.

Principle 22, Manage Compliance Responsibilities; Point of Focus 22.1, Establish a structured compliance program.

Suggestion: Mention the full scope of "compliance" requirements as they arise, including those that originate via channels other than statutory and regulatory requirements.

Draft text: "… a compliance program that is tailored to the entity's risk profile, regulatory environment, *and full scope of compliance obligations*." [suggested addition in italics]

"Due to the volume and complexity of legal and regulatory requirement, *and other enforceable and binding compliance obligations* to which entities are subject …"

[1] Douglas Hileman is an author of this document.

Rationale: Compliance obligations arise via many channels. Statutory and regulatory obligations are, of course, the most obvious. It is standard fare for companies to have efforts in place to identify, assess, and pursue compliance with laws and regulations. There are many commercial options to support these efforts.

Compliance obligations arise via other mechanisms.

- Contractual obligations with "tier 1" business partners, where the entity has a direct relationship. Examples include purchase and sale agreements of businesses or assets; requirements embedded in grant agreements or loan agreements; conditions of insurance policies.
- Contractual obligations with other business partners. Companies are subject to requirements that extend beyond parties they control. Laws, regulations, disclosures, and industry groups have developed frameworks to address forced labor/ human trafficking, ethical sourcing of products (palm oil, seafood, coffee), business conduct and ethics. Companies must indicate compliance with this array of requirements to fulfill regulatory requirements, and/or to engage in commerce with business partners.
- Industry, product, or topical standards. NIST has published Cybersecurity Framework, a voluntary framework consisting of standards, guidelines and best practices. Companies may obtain certification to ISO 9001 Quality Management Standards to inspire gain customer confidence in their operations or products. Companies may obtain Energy Star ratings for appliances. Companies must navigate regulatory an voluntary certifications if they wish to label a food product as "non-GMO".

Regulatory compliance obligations typically enter the organization via Legal or Compliance. There are mature processes to determine applicability, risk, and requirements. Other compliance obligations may be conveyed to Sales, R&D, Real Estate, Quality, Finance, Operations, or Risk. Compliance processes may not less mature, such that others in the organization do not fully recognize the impact of the requirements or resources required. Nonetheless, they impose requirements, and can pose risks – and opportunities. The complicated array of requirements, affected groups within the entity, and the lack of consistent alignment with traditional processes, controls, and service offerings means that governance is critical.

CONCLUSION

DHC looks forward to COSO's final Corporate Governance Framework. Broad adoption should improve the effectiveness and efficiency of boards, and stakeholders who depend on them fulfilling their obligations.

Respectfully submitted,

Douglas Hileman, FSA, CRMA, CPEA, P.E.
President, Douglas Hileman Consulting LLC
doug@douglashileman.com
or djhielman@gmail.com