Memo

To: COSO and WBSCD Leadership

From: Lorne O Joseph II, Founder - The ESG Roundtable

cc: ESG Roundtable Members

Date: June 29, 2018

Re: ESG Roundtable Response to Request for Comments on the "Applying Enterprise Risk Management to Environmental, Social and Governance Risks" Guidance

---

Introduction

We applaud the efforts by both COSO and the WBSCD, on behalf of board members, global risk practitioners and corporate citizens all over. This effort is a right step, in the right direction at the right time and we are pleased to note that the industry is taking the lead in providing the kind of transparency required to govern our collective future. Such a broad and powerful group of voices will undoubtedly provide the escape velocity required to radically alter the status quo. We believe that the single, most powerful statement delivered in this guidance was the following: "Over the past decade, the prevalence of ESG-related risks has steadily increased while the more traditional economic, geopolitical and technological risks are less dominant". As a cadre of experienced risk professionals, we could not agree more!

Background

The ESG Roundtable is a newly formed group dedicated to the persistent enumeration of the need for harmonization, transversal alignment, operationalization techniques, assimilation tools, outcome metrics, illustrative dashboards, and innovative training. This group is composed of

everyone from industry to multiple risk-assessing functions currently employed within the Global Fortune 2000 space. Member roles include: CISO, CIO, CAE, CPO, CLO, GC, Procurement, CDO, CRO and several other senior executive titles which provide both the executive view and the insight from operational management. This group is also organized to accomplish three important tasks, they are:

1. Provide guidance and support for the harmonization efforts required to organize, synthesize, and operationalize this new risk landscape. Investor interest in this critical topic will drive additional, significant streams of revenue to organizations that comply or could present an entire host of risks, not previously covered by board of directors or their respective organizations.
    a. Aggregate Framework, Guidance, Laws, Voluntary Frameworks and Commitments, and decision-making frameworks into a comprehensive and cohesive set of controls, requirements and guidance in support of task #1
2. Provide Research and support by considering various methods to support and increase the transparency and accountability goals stated herein. Best practices shall be aggregated and presented back to the larger body.
3. Provide events to allow diverse groups of corporate functions to interact and share knowledge on this very important topic. Geographic specific events should be held in order to propagate the benefits, frameworks and tools available to meet the requirements.

ePMO Framework Submission

Our founding, sponsor company, eGRC.COM, has graciously submitted their proprietary framework for operationalizing Governance Models such as the one prescribed herein. The framework is provided royalty-free and a lifetime use as an example of what they have been recommending to clients for the last ten years. This framework provides a tactical, Crawl, Walk, Run approach to implementing an oversight function which clearly demonstrates organizational Due Care. Our sponsor believes that this work effort will change the world as everyone if committed to putting some skin in the game. Please see Appendix A – eGRC Practical Management Objectives (ePMO) for additional details.

Framework Recommendation: Consider incorporating a similar methodology with the expressed intent of giving board members and executives, both experienced or newly appointed, a way to govern to the outcomes prescribed in the COSO ERM Guidance. It's simple to consume, each box in the mind map represents a group of activities required to demonstrate Due Care. The outside wheel demonstrates that the same groups of activities would occur across each domain and the red, yellow, green coding is a way to transparently report on each group.

Feedback Loop: We believe that one of the biggest risks to the successful implementation of an ESG framework will be the lack of a persistent, defined and measured feedback loop. The risks are new, the threats are new and the need for embedded risk management has never been greater. The feedback loop will provide situational awareness in the era of social media like Twitter, affecting market cap or EPS of corporations all over the world.

Feedback Loop Recommendation: Consolidated dashboards and reporting mechanisms shall be required to demonstrate risk in a side-by-side manner, given the ever-evolving threatscape. The feedback loop will consider everything from the court of public opinion to the implementation of Directive 2014/95 EU Non-financial Reporting Directive, which directs 6,000+ companies to report on environmental protections and Human Rights.

Frameworks, Benchmarks, Commitments and Standard

Given the sheer volume of Frameworks, Benchmarks, Commitments, Protocols, etc, for each of the Environmental, Social and Governance silos, the gap analysis, aggregation, synthesis of this body of work will take significant effort and will require many different types of experts to complete. This challenge is further compounded by the additional list of rules specific to each industry vertical (e.g. Bangladesh accord for apparel makers).

Frameworks Recommendation: We recommend providing the governance and oversight required to drive the aforementioned outcomes. Time, people and financial resources will all be required to help corporations continue to focus on GDP growth. Additional support will be required in two phases, the first is for the project required to establish the new operating baseline and the second phase is a clear understanding of what Business as Usual (BAU) will look like in the new world. A perfect example is the new GDPR regulation and how your loyalty websites, which generate no revenue, could present a 20 million EU penalty risk to your organization. We now have to consider the impact of that loyalty website and weigh it against the cost of customer acquisition in a measurable, repeatable format.

Milestones for Integrated Governance

Integrated Governance Protocols exist currently to provide a starting point for the ESG practitioners. The rules are currently myopic and siloed, but the foundations have been tested internationally. An example of the Integrated Governance Handbook 2016 or the King III South African King Code and Report on Governance.

IG Recommendation: We recommend broadening the scope of existing protocols once the gap analysis and harmonization process has been completed.

Annual ERM Cycle

The COSO Annual ERM Cycle and Value Chain could benefit from both a feedback loop of emerging risks and a programmatic way to measure the court of public opinion and brand sentiment. The COSO models have proven effective over the years and the feedback loop is solely to provide a path to maturation given the constant state of change and new risk landscape.

Enterprise-wide Issues Management

Develop an enterprise-wide issues management process which includes: Tone at the Top; an escalation path for issues to become material findings; and most importantly, a reporting mechanism to provide consistent guidance to board members and executives on how to separate sound from the noise generated by corporations daily. Each bucket (ESG) will have their own issues to manage, but senior management will want an aggregated and synthesized view.

Inherent versus Residual Risks

New measurements will be required to measure both inherent and residual risks. This will impact every aspect of the business from Third party risks to internal operational risks. This group shall consult with Subject Matters Experts to bring this important topic to light.

Business Context

Figure 2.2 on page 39 discusses business context and strategy. This group purports that this change in the way we do business should force all corporations to revisit several core business practices, such as:

1. Customer Acquisition Practices

2. Data Governance Practices

3. Board Governance and Reporting Practices

Each of the aforementioned practices provides both opportunities for revenue growth and significant risks waiting to impact your organization. If you don't take this opportunity you are literally putting lipstick on the pig and hoping for the best. New mandates require a new way to look at business in general and we are certain that this change will be material and impactful.

Stakeholder Engagement

Stakeholder engagement will create new opportunities to engage customers, communities and governmental agencies. This task is not insignificant and will require the use of cutting edge approaches such as social networking frameworks and communications protocols and enhanced metrics and reporting. Reputations will have to be tracked in a different way and those procedures require innovation and effort.

ESG Resources

We noted that education was not emphasized in the guidance. We consider the scope to be everything from K-12, to Collegiate and other outlets (e.g. Career and Technical Education). The shift in culture will require new training programs for each of the new types of employees that we will have to hire in the future to continue our ESG efforts.

ESG Resources Recommendations: Focus and effort should be expended to look at the education system and determine where adjustments will be necessary to produce the kind of resources that tomorrow's corporation will require.

Business Unit Risk

The group recommends a robust Organization Unit and Business Unit Risk assessment framework which will allow for direct business context and situational awareness embedded with the visibility of what revenue is being generated or the expense that is being generated. The BU -> OU risks should be assessed, aggregated, and visible to those responsible for managing risks. This challenge is further exacerbated by the complexity of corporations whom 'growth via acquisition' and is lacking in a common operating framework.

Reporting Requirements

Reporting was covered in the guidance. We agree with the need for multi-tiered reporting to ensure complete coverage and adoption. A number of the Roundtable team members are Six-Sigma trained and certified (Green and Black Belts) and we strongly recommend considering the addition of the KNOW-FEEL-DO communications planning component coupled with the three levels of reporting prescribed. The output will provide KNOW-FEEL-DO guidance for each the Board of Directors, Operational Management and the Employees working for your organization.

Timing

As mentioned in the guidance, we would be negligent if we did not briefly touch on the timing aspect of today's electronic society. The Internet, Twitter, Instagram, Facebook and all of these communications platforms which add the risk of velocity to what previously could have been purely a local issue. The ability to respond in near real-time has never been so important! When one tweet from a movie star, Rockstar or politician can affect your market cap.

Conclusion

We would like to reiterate how wonderful this effort was and how we are honored to be participating in such a great advancement in our society. The ESG Roundtable will continue with our mission to bring harmony to an otherwise fragmented set of silos representing Environmental, Social and Governance. We will report our findings publicly and shall be organized as a 501c3 non-profit organization. We thank the members of the COSO and the WBSCD Teams for all of their hard work.

Appendix A – eGRC Practical Management Objectives (ePMO)

GOAL: A methodology for measuring board or committee effectiveness at operationalizing corporate goals whilst managing the risks associated with those outcomes to an acceptable, measurable and documented level.