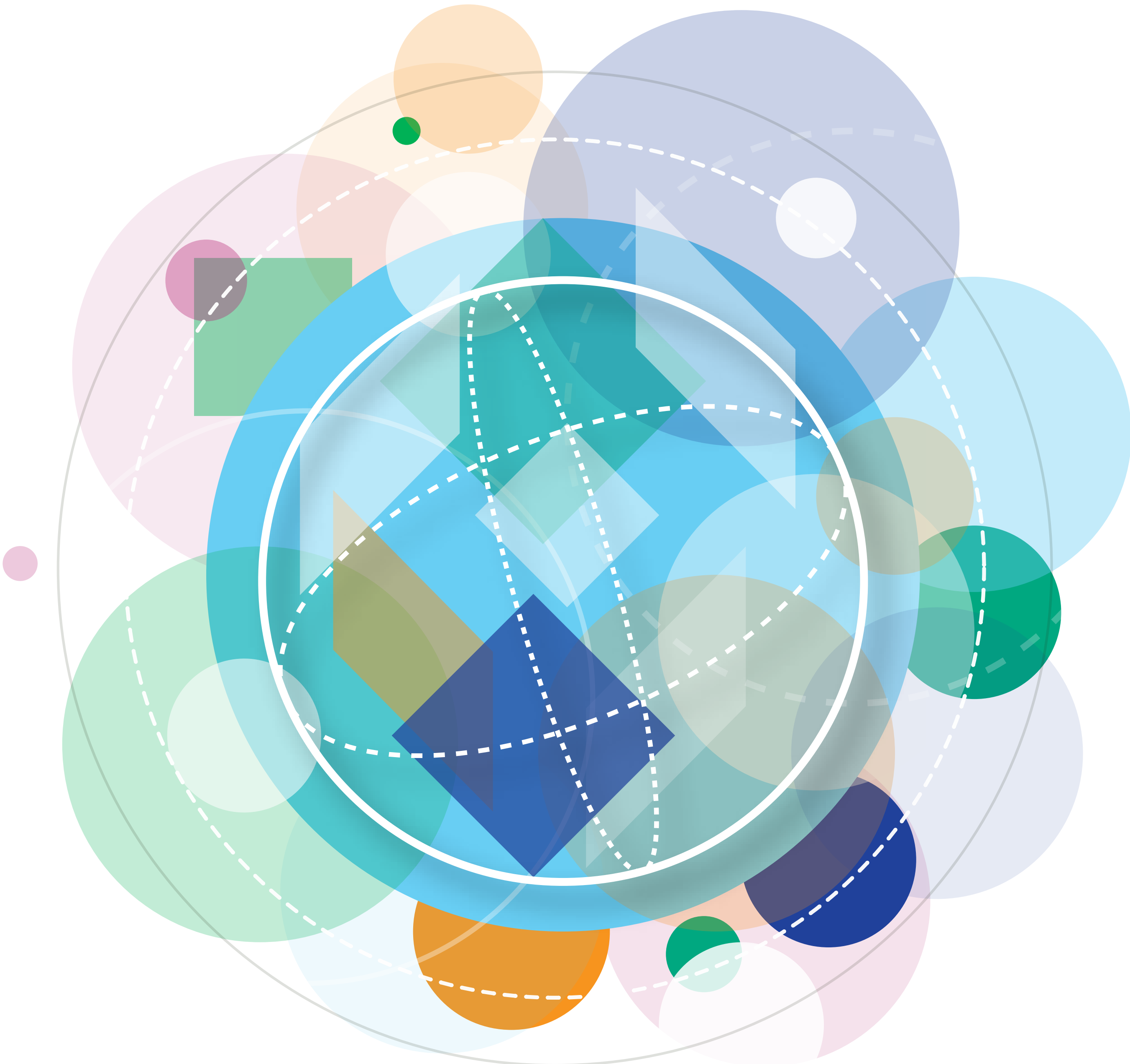
Enterprise Risk Management

Applying enterprise risk management to environmental, social and governance-related risks

Executive Summary



January 2018

COSO | wbcsd

This document was developed by the **Committee of Sponsoring Organizations of the Treadway Commission** (COSO) and the **World Business Council for Sustainable Development** (WBCSD).

This document summarizes the forthcoming draft application guidance: *Enterprise risk management framework: Applying enterprise risk management to environmental, social and governance-related risks* and is designed to supplement COSO's updated enterprise risk management (ERM) framework, *Enterprise risk management - Integrating with strategy and performance*. This guidance addresses an increasing need for companies to integrate environmental, social and governance (ESG)-related risks into their ERM processes.

COSO and WBCSD are planning for a public comment period on this material. More information will be posted at **COSO.org**.

This project is funded by the **Gordon and Betty Moore Foundation**.

About us

Originally formed in 1985, **COSO** is a voluntary private sector organization dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management and fraud deterrence. COSO is jointly sponsored by the **American Accounting Association** (AAA), the **American Institute of Certified Public Accountants** (AICPA), **Financial Executives International** (FEI), the **Institute of Management Accountants** (IMA) and the **Institute of Internal Auditors** (IIA). For more information, visit **COSO.org**.

WBCSD is a global, CEO-led organization of over 200 leading businesses working together to accelerate the transition to a sustainable world. WBCSD helps make its member companies more successful and sustainable by focusing on the maximum positive impact for shareholders, the environment and societies.

WBCSD member companies come from all business sectors and all major economies, representing a combined revenue of more than $8.5 trillion and 19 million employees. WBCSD's global network of almost 70 national business councils gives its members unparalleled reach across the globe. WBCSD is uniquely positioned to work with member companies along and across value chains to deliver impactful business solutions to the most challenging sustainability issues.

Together, WBCSD is the leading voice of business for sustainability: united by its vision of a world where more than 9 billion people are all living well and within the boundaries of the planet, by 2050. Visit **wbcsd.org**.

The Gordon and Betty Moore Foundation fosters path-breaking scientific discovery, environmental conservation, patient care improvements and preservation of the special character of the Bay Area. Visit **Moore.org** or follow **@MooreFound**.

PRELIMINARY DRAFT

Why do environmental, social and governance-related risks matter for business?

Businesses are facing an evolving landscape of emerging environmental, social and governance (ESG)-related risks that can impact a company's profitability, success or even survival.

Over the past decade, the prevalence of ESG-related risks has steadily increased while the more traditional economic, geopolitical or technological risks are less dominant.

As described by the World Economic Forum in *Global Risk Report*, in 2008, only one societal risk - pandemics - was reported in the top five risks in terms of impact. Ten years later in 2018, four of the top five risks were societal or environmental, including extreme weather events, water crises, natural disasters and failure of climate change mitigation and adaptation. The World Economic Forum also highlights the depth of the interconnectedness that exists both among the environmental risks and between them and risks in other risk categories—such as water crises and involuntary migration.[1]

Figure 1. Evolving risk landscape 2008-2018

	2008	2013	2018
Top 5 Global Risks in terms of likelihood	Asset price collapse	Severe income disparity	Extreme weather events
	Middle East instability	Chronic fiscal imbalances	Natural disasters
	Failed and failing states	Rising greenhouse gas emissions	Cyberattacks
	Oil and gas price spike	Water supply crises	Data fraud or theft
	Chronic disease, developed world	Mismanagement of population ageing	Failure of climate-change mitigation and adaptation
Top 5 Global Risks in terms of impact	Asset price collapse	Major systemic financial failure	Weapons of mass destruction
	Retrenchment from globalization (developed)	Water supply crises	Extreme weather events
	Slowing Chinese economy (<6%)	Chronic fiscal imbalances	Natural disasters
	Oil and gas price spike	Diffusion of weapons of mass destruction	Failure of climate-change mitigation and adaptation
	Pandemics	Failure of climate-change mitigation and adaptation	Water crises

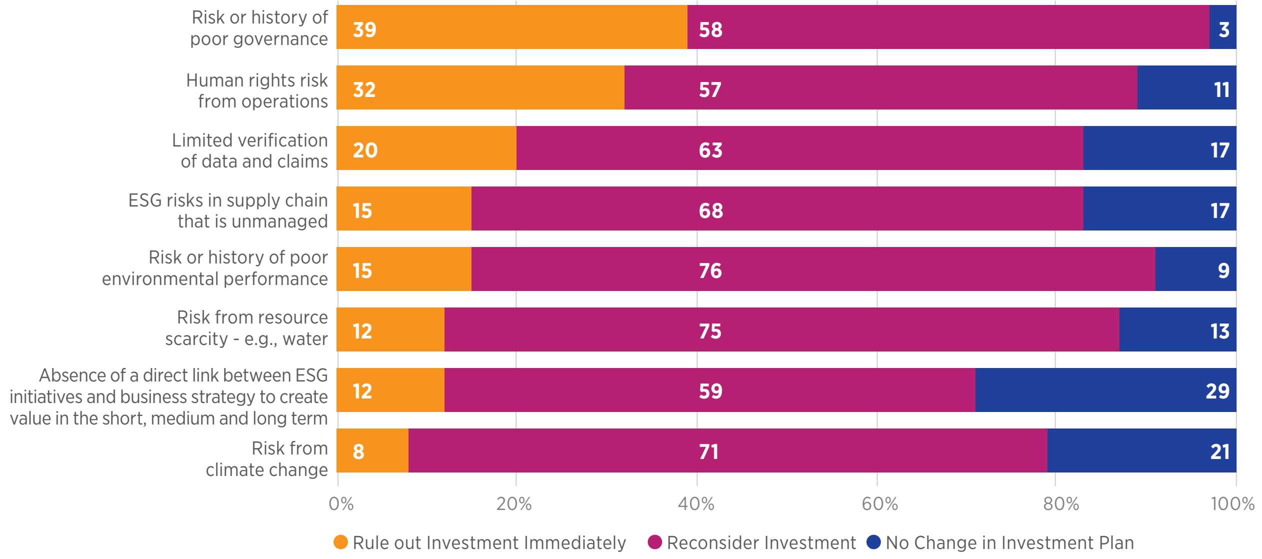
● Economic ● Environmental ● Geopolitical ● Societal ● Technological

At a global level, businesses have felt the impacts of these risks and megatrends. From small startups to large multinationals, companies have experienced instances of product safety recalls, worker fatalities, child labor, forced labor, polluting spills and weather-related supply-chain disruptions. Failure to manage these emerging risks proactively has translated into extensive financial and reputational harm – in some cases to the point of no recovery. For some companies, failure to take advantage of opportunities arising from the changing risk landscape has resulted in lost revenue or even obsolescence.

PRELIMINARY DRAFT

Investors have also expressed increased interest in ESG performance and a desire to understand how companies are managing a selection of long-term risks such as climate change and water scarcity. A survey of 320 institutional investors conducted in 2016[2] revealed that more than 80% agree that for too long companies have "failed to consider environmental and social risks and opportunities as core to their business." These institutional investors agreed ESG issues have "real and quantifiable impacts" over the long term and that generating sustainable returns over time requires a sharper focus on ESG factors. Figure 2 shows the ESG-related risks that are most likely to impact investors' decisions.

Figure 2. Corporate governance, environmental and human rights risks are most likely to alter investors' decisions



And yet, companies have struggled to bring ESG-related risks and opportunities into the risk management discussion. ESG-related risks are often managed and disclosed by a team of sustainability specialists, and in many organizations, are viewed as separate or less significant than conventional strategic operational, legal or financial risks. This is evidenced by a 2017 WBCSD member study on the integration of sustainability and ERM which reported only 29% alignment between material risks disclosed in a company's risk filings compared to those disclosed as material sustainability issues in the sustainability report.[A]

Companies pointed to several reasons for this misalignment. Most common is the challenge of quantifying the potential monetary impact of ESG-related risks to enable the prioritization and allocation of resources. Contributing to this challenge are the long-term nature and uncertainty of expected impacts for ESG-related risks. Many companies also lack the knowledge about ESG-related risks at the management or executive level, which is exacerbated by limited cross-functional collaboration between sustainability managers, risk managers and risk owners.[3]

[A] Included the risks disclosed in the"risk factors" section of a SEC 10-K, Form 20-F or an equivalent annual report. The desktop research methodology used a word search seeking exact language matches.

How can enterprise risk management support management of ESG-related risks?

Leveraging a company's enterprise risk management (ERM) governance and processes can support identification, assessment and mitigation of ESG-related risks at an enterprise level.

A robust risk management framework not only preserves value and reduces downside exposure but can also help connect risk, strategy and decision-making while enhancing corporate performance. One study found that companies with superior risk management maturity (top 20%) reported earnings three times higher than companies in the bottom 20%.[4]

Although many ESG-related risks are new or emerging, complex and longer-term, leveraging and enhancing a company's enterprise risk management framework are effective for reducing potential risk and capturing opportunities arising from ESG issues. ESG-related risks are business risks and should therefore be integrated into strategy and ERM.

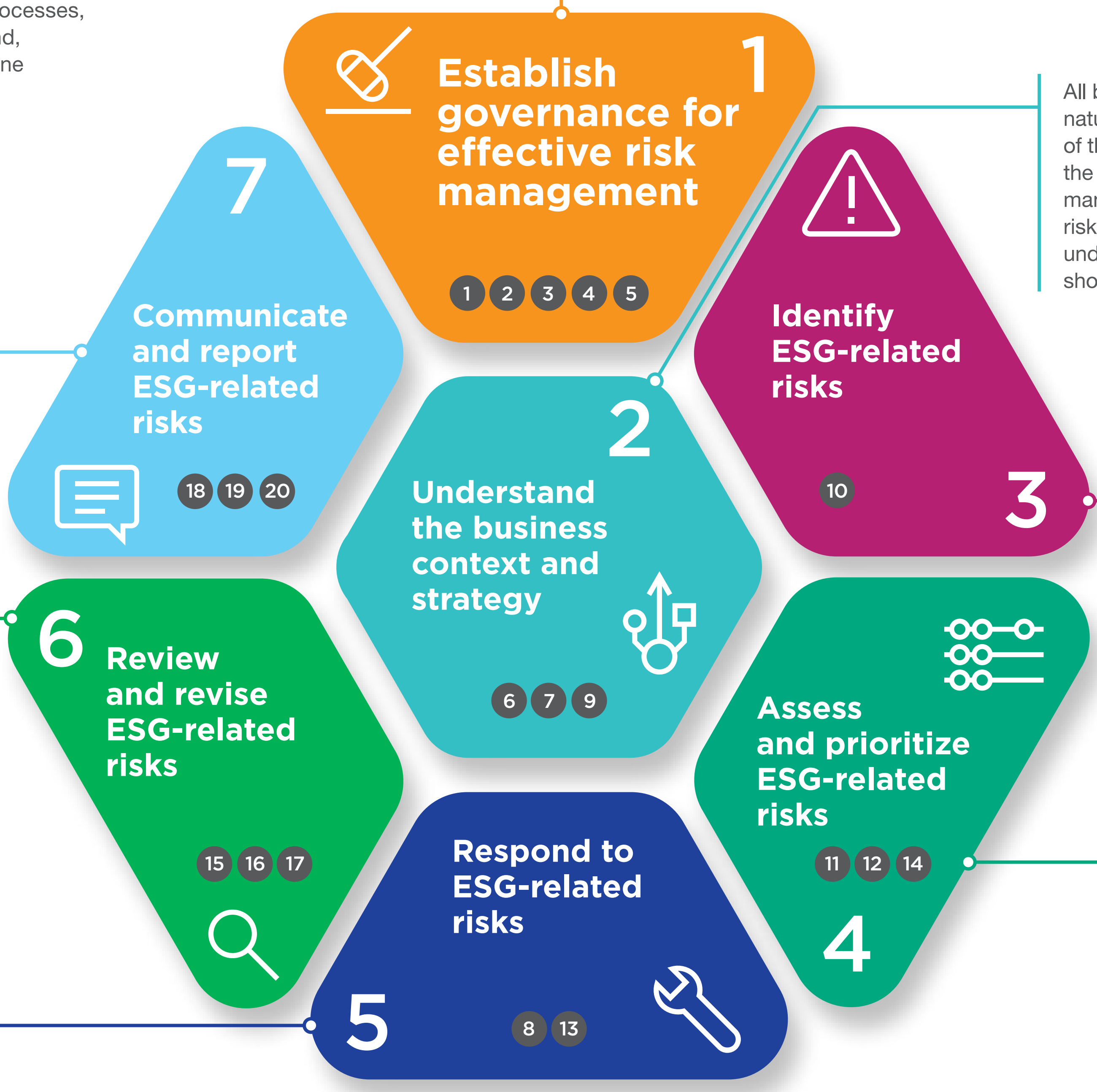
In September 2017, COSO released an updated framework *Enterprise Risk Management - Integrating with Strategy and Performance*, which details five components and 20 principles that support companies in establishing ERM governance and processes to think strategically about how to manage increasing volatility, complexity and ambiguity of the business environment – internally and externally.

Both COSO and WBCSD believe that enterprise risk management is the most powerful conduit to address ESG-related risks.

Figure 3. COSO's Enterprise Risk Management Framework

Guidance for applying ERM to ESG-related risks

To supplement COSO's updated framework, COSO and WBCSD have come together in a unique collaboration to develop application guidance for companies to integrate ESG-related risks into the ERM process. This guidance leverages existing decision-useful frameworks, company examples and tools to provide sustainability and risk managers with practical approaches for managing ESG-related risks. The guidance is set out in seven modules, starting with establishing governance structures and processes, then moving through the ERM process to identify, assess, respond, review and communicate ESG-related risks, while maintaining a line of sight to the business context and strategy. This guidance will be subject to a robust consultation process in 2018.



● COSO's Enterprise Risk Management Framework 20 Principles

Governance, or internal oversight, establishes the manner in which decisions are made and how these decisions are executed. Applying ERM to ESG-related risks includes supporting the board and executive management's awareness of ESG-related risks - supporting a culture of collaboration among those responsible for risk management and challenging organizational bias against ESG-related issues.

All businesses have impacts and dependencies on nature and society. Therefore, a strong understanding of the business context and strategy serves as the anchor to all ERM activities and the effective management of risks. Applying ERM to ESG-related risks includes examining the value creation process to understand these impacts and dependencies in the short, medium and long term.

Risks and opportunities can arise from changes to the business strategy, objectives, context or risk appetite. Applying ERM to ESG-related risks includes analyzing ESG materiality assessments, megatrend analysis and other approaches.

Companies have limited resources to mitigate all risks identified across the entity. For that reason, it is necessary to assess risks for prioritization. Applying ERM to ESG-related risks includes assessing risk severity in terms management can use to prioritize risks. Assessment approaches for ESG-related risks include forecasting and scenario analysis among others.

For all risks in the risk inventory, management selects and deploys an appropriate risk response based on the prioritization. Companies can apply a variety of existing ESG-related resources (e.g., industry working groups and ESG-related protocols) to develop innovative and effective responses to ESG-related risks. These responses can create business solutions that can lead to new value creating activities.

Management monitors ESG trends and indicators for changes to the business context and strategy and establishes metrics to monitors risk response activities.

Applying ERM to ESG-related risks includes consulting with the risk owners to identify the most appropriate measures for evaluating and communicating performance internally and externally.

PRELIMINARY DRAFT

Benefits of integrating ESG-related risks into ERM

Applying this guidance along with the ERM principles and processes detailed in COSO's ERM framework (or other frameworks) can provide a starting point for effectively understanding, managing and disclosing the full spectrum of risks. By doing so, a company can achieve:

- **Enhanced company resilience**
  A company's medium- and long-term viability and resilience will depend on the ability to anticipate and respond to risks that threaten its strategy and business objectives.
- **A common language for articulating risks**
  ERM identifies and assesses risks for potential impact to the business strategy and objectives. Articulating ESG-related risks in these terms enables ESG issues to be brought into mainstream processes and evaluations.
- **Improved resource deployment**
  Obtaining robust information on ESG-related risks allows management to assess overall resource needs and helps optimize resource allocation.
- **Enhanced pursuit of opportunity**
  By considering both positive and negative aspects of ESG-related risks, management can identify ESG trends that lead to new business opportunities.
- **Efficiencies of scale**
  Managing ESG-related risks centrally and alongside other entity-level risks helps to eliminate redundancies and better allocate resources to address the company's top risks.
- **Improved disclosure**
  Improving management's understanding of ESG-related risks can provide the transparency and disclosure investors expect and ensure consistency with jurisdictional reporting requirements.

Assessing company readiness for ESG-related risks

The following questions can help assess a company's readiness to identify and manage the ESG-related risks of today while maintaining resilience to adapt and respond to the megatrends of tomorrow.

	Questions	Module
☐	Are the board and executive management familiar with ESG-related risks that may impact the company's ability to achieve its corporate strategy now and in the future?	1. Establish governance for effective risk management
☐	Is management aware of its responsibilities for existing or proposed ESG reporting requirements?	
☐	Has the company defined its risk appetite including consideration of ESG-related risks?	
☐	Has an appropriate risk owner been assigned to each ESG-related issue or risk?	
☐	Do risk owners, sustainability managers and risk managers collaborate on a regular basis?	
☐	Do risk owners understand the impacts and dependences of their business on nature and society? (Refer to Module 2.)	
☐	Does the company use established mechanisms (e.g., *Natural Capital Protocol* and *Social Capital Protocol*, megatrend analysis, materiality assessments) to understand the impacts and dependencies of social and natural capital on value creation?	2. Understand the business context and strategy
☐	Does the company maintain a line of sight to the business context, strategy and risk appetite throughout its ERM activities?	
☐	Are sustainability managers, risk owners and other ESG experts included in the risk identification process?	3. Identify ESG-related risks
☐	Are ESG-related risks captured in the risk inventory?	
☐	Does the company use sustainability and risk assessment tools to express ESG-related risks in a language that promotes comparability and prioritization?	4.Assess and prioritize ESG-related risks
☐	In addition to impact and likelihood of a risk, does the company consider aspects such as resilience to prioritize risks?	
☐	Does the risk management process ensure that longer term ESG-related risks are not excluded from the risk identification and prioritization process?	
☐	Does management provide stakeholders (e.g., the board, shareholders) with appropriate and timely responses for ESG-related risks?	5.Respond to ESG-related risks
☐	Does management use indicators and thresholds to review the effectiveness of management for ESG-related risks?	6.Review and revise ESG-related risks
☐	Does the company understand and meet the ESG disclosure expectations of internal and external stakeholders?	7. Communicate and report ESG-related risks

Notes

References

1 World Economic Forum. (2018, January 17). The Global Risks Report 2018, 13th Edition. Retrieved from World Economic Forum: **reports.weforum.org/global-risks-2018/**

2 EYGM Limited. (2017). Is your nonfinancial performance revealing the true value of your business to investors? Retrieved from EY: **ey.com/Publication/vwLUAssets/EY_-_Nonfinancial_performance_may_influence_investors/$FILE/ey-nonfinancial-performance-may-influence-investors.pdf**

3 WBCSD. (2017, January 18). Sustainability and enterprise risk management: the first step towards integration. Retrieved from WBCSD: **wbcsd.org/Projects/Non-financial-Measurement-and-Valuation/Resources/Sustainability-and-enterprise-risk-management-The-first-step-towards-integration**

4 EYGM Limited. (2013). Turning risk into results: How leading companies use risk management to fuel better performance. Retrieved from EY: **ey.com/Publication/vwLUAssets/Turning_risk_into_results/$FILE/Turning%20risk%20into%20results_AU1082_1%20Feb%202012.pdf**

PRELIMINARY DRAFT

PRELIMINARY DRAFT

Enterprise Risk Management

Applying enterprise risk management to environmental, social and governance-related risks

Executive Summary

January 2018

coso.org

wbcsd.org

PRELIMINARY DRAFT