

# Enterprise Risk Management

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



EXECUTIVE SUMMARY

October 2018



This document is an executive summary of *Enterprise risk management—Applying enterprise risk management to environmental, social and governance-related risks*. This guidance is designed to apply to COSO's enterprise risk management (ERM) framework, *Enterprise Risk Management—Integrating with strategy and performance*. It addresses an increasing need for companies to integrate environmental, social and governance-related risks (ESG) into their ERM processes.

#### **Committee of Sponsoring Organizations of the Treadway Commission (COSO)**

- Paul J. Sobel, COSO Chair
- Douglas F. Prawitt, American Accounting Association
- Charles E. Landes, American Institute of Certified Public Accountants
- Daniel C. Murdock, Financial Executives International
- Jeffrey C. Thomson, Institute of Management Accountants
- Richard F. Chambers, The Institute of Internal Auditors

#### **World Business Council for Sustainable Development (WBCSD)**

- Peter Bakker, President and CEO
- Peter White, Vice President and Chief Operating Officer
- Rodney Irwin, Managing Director, Redefining Value

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](https://www.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 USD\$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](https://www.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 San Francisco Bay Area. Visit [Moore.org](https://www.moore.org) or follow @MooreFound.

# Introduction

Entities, including businesses, governments and non-profits, face an evolving landscape of environmental, social and governance (ESG)-related risks that can impact their profitability, success and even survival. Given the unique impacts and dependencies of ESG-related risks, COSO and WBCSD have partnered to develop guidance to help entities better understand the full spectrum of these risks and to manage and disclose them effectively.

The guidance is designed to help risk management and sustainability practitioners apply enterprise risk management (ERM) concepts and processes to ESG-related risks.

## What are ESG-related risks?

ESG-related risks are the environmental, social and governance-related risks and/or opportunities that may impact an entity. There is no universal or agreed-upon definition of ESG-related risks, which may also be referred to as sustainability, non-financial or extra-financial risks.<sup>a</sup> Each entity will have its own definition based on its unique business model; internal and external environment; product or services mix; mission, vision and core values and more. The resulting definition may be broad (for example, may include all aspects of the International Integration Reporting Council's (IIRC) six capitals, discussed in Chapter 2) or narrow (for example, may include only a selection of priority environmental and social issues) and may evolve over time.

For the purposes of the guidance, the term ESG-related risks encompasses the issues that are prominent on investors' and other stakeholders' agendas, such as those described by MSCI<sup>1</sup> and Robeco<sup>2</sup> in Table 1:

**Table 1: Definitions of ESG**

	MSCI definition	Robeco definition
<b>Environmental</b>	Climate change, natural resources, pollution and waste and environmental opportunities	The contribution an entity makes to climate change through greenhouse gas emissions, along with waste management and energy efficiency. Given renewed efforts to combat global warming, cutting emissions and decarbonizing have become more important.
<b>Social</b>	Human capital, product liability, stakeholder opposition and social opportunities	Human rights, labor standards in the supply chain, any exposure to illegal child labor and more routine issues such as adherence to workplace health and safety. A social score also rises if a company is well integrated with its local community and therefore has a "social license" to operate with consent.
<b>Governance</b>	Corporate governance and corporate behavior	A set of rules or principles defining rights, responsibilities and expectations between different stakeholders in the governance of corporations. A well-defined corporate governance system can be used to balance or align interests between stakeholders and can work as a tool to support a company's long-term strategy.

Organizations such as the Sustainability Accounting Standards Board (SASB)<sup>b</sup> and the Global Reporting Initiative (GRI), among others, also provide lists of the potential issues that may be captured in the definition of ESG.

COSO's *Enterprise Risk Management—Integrating with Strategy and Performance* (COSO ERM Framework) defines risk as "the possibility that events will occur and affect the achievement of strategy and business objectives."<sup>3</sup> This includes both negative effects (such as a reduction in revenue targets or damage to reputation) as well as positive impacts (that is, opportunities – such as an emerging market for new products or cost savings initiatives).

<sup>a</sup> Although these terms are used interchangeably, the guidance has adopted the term *ESG*, as it is currently the term commonly used by the investor community and captures the range of criteria to generate long-term competitive financial returns and positive social impact. The term *related risks* has been adopted to account for non-ESG risks that may have ESG-related causes or impacts. For example, the risk of raw material price fluctuations may be exacerbated by an environmental cause, such as flooding or droughts that not previously considered by the organization.

<sup>b</sup> SASB's sustainability topics are organized under five broad sustainability dimensions: environment, social capital, human capital, business model and innovation and leadership and governance.

### Example: Unilever's purpose, vision and ESG issues

Unilever's identified ESG issues stem from its purpose "to make sustainable living commonplace" and its vision "to grow [its] business while decoupling [its] environmental footprint from [its] growth and increasing [its] positive social impact."<sup>4</sup> The table below highlights Unilever's identified ESG topics that may affect achievement of this purpose or vision.<sup>5</sup>

Improving health and well-being	Reducing environmental impact	Enhancing livelihoods	Responsible business practices	Wider sustainability topics
<ul style="list-style-type: none"> <li>• Nutrition and diets</li> <li>• Sanitation and hygiene</li> </ul>	<ul style="list-style-type: none"> <li>• Agricultural sourcing</li> <li>• Climate action</li> <li>• Deforestation</li> <li>• Packaging and waste</li> <li>• Water</li> <li>• Non-agricultural sourcing</li> </ul>	<ul style="list-style-type: none"> <li>• Human rights</li> <li>• Women's rights and opportunities</li> <li>• Economic inclusion</li> <li>• Employee well-being</li> <li>• Fair compensation</li> </ul>	<ul style="list-style-type: none"> <li>• Ethics, values and culture</li> <li>• Data security and privacy</li> <li>• Governance and accountability</li> <li>• Responsible marketing and advertising</li> <li>• Tax and economic contribution</li> <li>• Responsible use of innovation and technology</li> </ul>	<ul style="list-style-type: none"> <li>• Trusted products and ingredients</li> <li>• Animal testing and welfare</li> <li>• Consumers and sustainability</li> <li>• Talent</li> <li>• Communicable diseases</li> </ul>

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

ESG-related risks are not necessarily new. In particular, corporations, organizations, governments and investors have been considering governance risks for many years, focusing on aspects such as financial accounting and reporting practices, the role of board leadership and composition, anti-bribery and corruption, business ethics, and executive compensation.

However, over the last several decades – and particularly the last 10 years – the prevalence of ESG-related risks has accelerated rapidly. In addition to a clear rise in the number of environmental and social issues that entities now need to consider, the internal oversight, governance and culture for managing these risks also require greater focus.

### The evolving global risk landscape

Each year, the World Economic Forum's *Global Risks Report*<sup>6</sup> surveys business, government, civil society and thought leaders to understand the highest rated risks in terms of impact and likelihood. Over the last decade, these risks have shifted significantly. In 2008, only one societal risk, pandemics, was reported in the top five risks in terms of impact. In 2018, four of the top five risks were environmental or societal, including extreme weather events, water crises, natural disasters, and failure of climate change mitigation and adaptation.

The World Economic Forum also highlights the increasing interconnectedness among ESG risks themselves, as well as with risks in other categories – particularly the complex relationship between environmental risks or water crises and social issues such as involuntary migration.

In the business world, this evolving landscape means ESG-related risks that were once considered "black swans"<sup>7</sup> are now far more common – and can manifest more quickly and significantly. A report by the Society for Corporate Governance<sup>7</sup> in the United States found that these issues often, although not always:

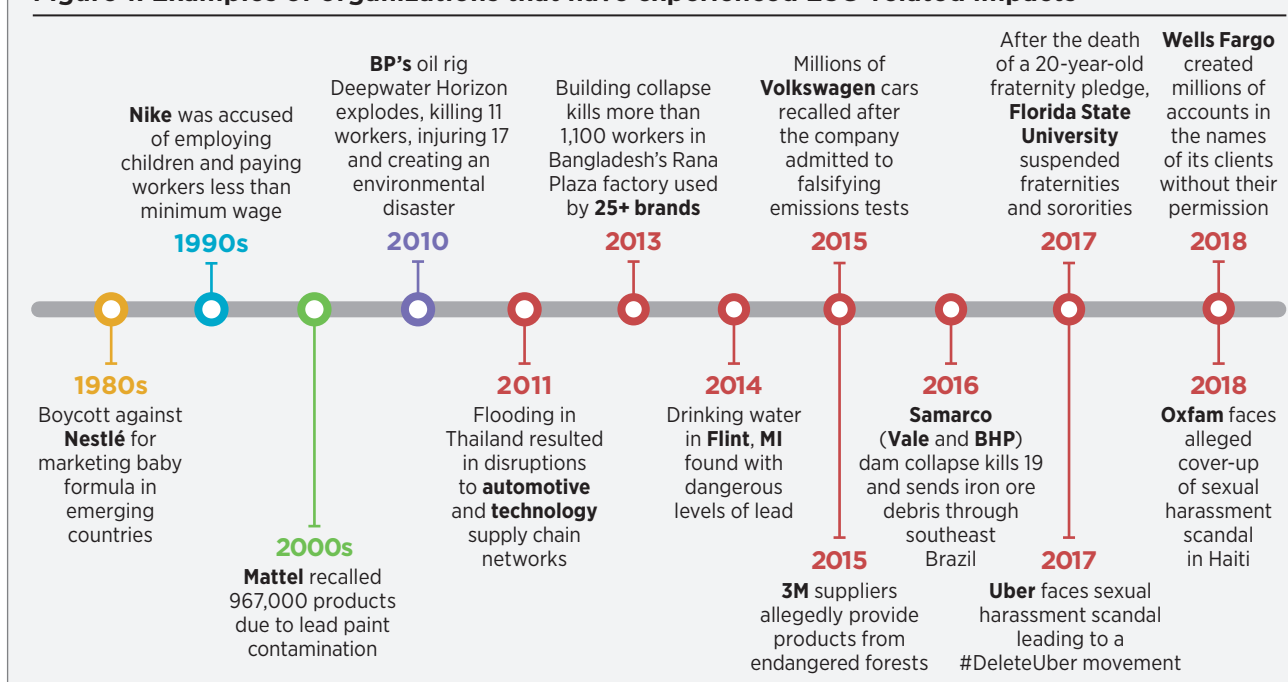
- Derive from a risk or impact inherent in the core operations or products
- Have the potential to meaningfully damage a company's intangible value, reputation or ability to operate
- Are accompanied by persistent media interest, organized stakeholders and associated public policy debates that could magnify the impact of a company's existing position or practice and increase the reputational risk (or opportunity) created by a change in company policy or practice

<sup>6</sup> The black swan theory was developed by Nassim Nicholas Taleb, who describes it as "first, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable." For more information, refer to the 2007 New York Times article "The Black Swan: The Impact of the Highly Improbable."

An illustration of this is JBS SA's (JBS) experience between 2015 and 2017. JBS is the world's largest meat company by revenue, capacity and production across poultry, lamb and pork. Beginning in late 2015 and continuing into June 2017, successive allegations of meat contaminations, corruption, deforestation, slave labor and fraud were levied against JBS as part of several extensive and ongoing probes centered on the meatpacking industry, and JBS in particular. Ultimately, JBS faced material financial impacts, including a loss of equity value of 31%. While the most direct impact resulted from weak governance, the challenges were exacerbated by a series of complex and interconnected ESG-related challenges, reflected in declining investor and consumer interest in international markets that prioritize ESG concerns.<sup>8</sup>

JBS's experience is not unique. Figure 1 outlines the growing pace with which other organizations have failed to manage ESG issues, leading to impacts on reputation, customer loyalty and financial performance. In many cases, the media, social media and other non-governmental organization campaigns play a role in bringing these issues to the attention of civil society and the organization.

**Figure 1: Examples of organizations that have experienced ESG-related impacts**



When incidents related to pollution, customer and employee safety, ethics and management oversight have such dramatic impacts on market prices, it becomes clear that ESG issues are business issues and that their near-term market impacts reflect anticipated long-term effects on cash flows and associated risks.

#### Investor interest in ESG-related risks

There is also growing interest from investors seeking to understand how organizations are identifying and responding to ESG-related risks.<sup>9</sup> In recent years, environmental and social proposals in the US have accounted for around half of all shareholder proposals submitted – representing the largest category of proposals (the other categories include board, anti-takeover/strategic, compensation or routine/other).<sup>d</sup>

In 2018, shareholder proposals on environmental and social topics that reached a vote included high-profile topics such as political spending and lobbying, greenhouse gas emissions, sustainability reporting, diversity and inclusiveness, human rights, gun control, and prescription drugs. Governance-focused shareholder proposals related to board matters such as director elections and executive and director compensation. The growing level of investor support for environmental issues has been notable; for example, in recent years, climate-related proposals received majority support of votes cast at large-cap companies such as ExxonMobil, Occidental Petroleum, PPL Corporation and Anadarko.<sup>10</sup>

<sup>d</sup> Although average support for environmental and social proposals has been on the rise, a significant number (around one-third) are typically withdrawn from proxy ballots and addressed through company-investor engagement, robust dialogue and company action. Based on governance data of more than 3,000 US public companies. Includes data up to August 31, 2018.

These proxy voting results are not surprising given the growing attention by large institutional investors to responsible investing and how companies are addressing social and environmental challenges to achieve long-term, sustained growth.<sup>e</sup> Once limited to a small set of investors, the focus on ESG investing has expanded to mutual funds, exchange-traded funds and private equity. The largest passive investors globally, including BlackRock, which has USD\$6.3 trillion in assets under management, State Street Global Advisors (USD\$2.8 trillion) and the Government Pension Fund of Japan (USD\$1.4 trillion), have embraced purpose and ESG considerations in their investing, engagement, risk management practices and marketing practices.<sup>11</sup>

“A company’s ability to manage environmental, social and governance matters demonstrates the leadership and good governance that is so essential to sustainable growth, which is why we are increasingly integrating these issues into our investment process. Companies must ask themselves: What role do we play in the community? How are we managing our impact on the environment? Are we working to create a diverse workforce? Are we adapting to technological change? Are we providing the retraining and opportunities that our employees and our business will need to adjust to an increasingly automated world? Are we using behavioral finance and other tools to prepare workers for retirement, so that they invest in a way that will help them achieve their goals?”<sup>12</sup>

Larry Fink, CEO BlackRock, 2018

## ESG disclosures and regulation

Sustainability reporting has become a norm for many public and private companies. Non-profits and public entities have also started to disclose ESG information to their stakeholders.<sup>f</sup> Most entities face some level of investor, customer and/or supplier demand for more transparency about ESG issues, particularly those related to questions around supply chain integrity, board diversity or climate change adaptation. In 2018, 85% of all S&P 500 companies produced some type of ESG disclosure.<sup>13</sup>

There has also been growth in ESG-related regulation and disclosure requirements – totaling 1,052 requirements (80% of which are mandatory) in 63 countries.<sup>9</sup> From 2017, the European Union Directive on Non-Financial Reporting requires that companies that operate in EU member states and meet certain criteria prepare a statement containing information relating to environmental protection, social responsibility and treatment of employees, respect for human rights, anti-corruption and bribery, and diversity on boards. Regulatory bodies and stock exchanges are also responding to growing investor demands for uniform ESG information linked to financial performance.

In 2017, Singapore introduced a listing rule for listed issuers to prepare an annual sustainability report, identifying material ESG factors, policies, practices, performance, targets and a board statement.<sup>14</sup> NASDAQ’s Nordic and Baltic exchanges issued voluntary guidance in March 2017.<sup>15</sup>

The *Recommendations of the Task Force for Climate-related Financial Disclosures* (TCFD)<sup>16</sup> are a significant step to support preparedness in the transition to a low-carbon economy and against anticipated increases in the frequency or intensity of extreme climate events. Drawing on numerous guidance documents, initiatives, reporting and risk management mechanisms, the TCFD has issued recommendations on climate-related risks that can be applied to corporations and other entities.

<sup>e</sup> An EY survey revealed that more than 80% of institutional investors surveyed agreed that for too long, companies have failed to consider environmental and social risks and opportunities as core to their business. They believe that 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. For more information, refer to the 2017 EY report “Is your nonfinancial performance revealing the true value of your business to investors?”

<sup>f</sup> Some examples include the DMCC (Free Zone and Government of Dubai Authority on commodities trade and enterprise), Eskom, NASA, NASDAQ, Oxfam and WWF.

<sup>9</sup> These countries include Argentina, Australia, Austria, Bangladesh, Belgium, Bolivia, Brazil, Canada, Chile, China, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Ecuador, El Salvador, Finland, France, Germany, Greece, Guatemala, Honduras, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Kazakhstan, Luxembourg, Malaysia, Mexico, Myanmar, Netherlands, New Zealand, Nigeria, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Romania, Russia, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Kingdom, United States, Uruguay and Vietnam. For more information, refer to the Reporting Exchange at [reportingexchange.com/](http://reportingexchange.com/)



### Comparing ESG disclosures to risk disclosures

Despite an increase in ESG disclosures, evidence shows that the issues reported in sustainability reports or ESG disclosures do not always align to the risks reported in an organization's risk disclosures. WBCSD member companies point to a range of reasons for this, including:

- The challenge of quantifying ESG-related risks in monetary terms. Not doing so makes prioritization and appropriate allocation of resources much more difficult, particularly when the risk is long term with uncertain impacts emerging over an unknown time period.
- Lack of knowledge of ESG-related risks across the entity and limited cross-functional collaboration between risk management and sustainability practitioners.
- ESG-related risks are managed and disclosed by a team of sustainability specialists and viewed as separate or less significant than conventional strategic, operational or financial risks – leading to a range of biases against ESG-related risks.

Refer to *Sustainability and ERM: The first step towards integration*<sup>17</sup> for more information or Appendix I for a summary of this research.

## How can ERM help risk management and sustainability practitioners navigate ESG-related risks?

There is a case to be made for entities taking a more active role in understanding and addressing ESG-related risks – whether that means reducing or removing risk, adapting and preparing for risk or being more transparent about how the organization is addressing risk.

The COSO ERM Framework defines ERM as “the culture, capabilities and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving and realizing value.”<sup>18</sup>

Many entities have ERM structures and processes in place to identify, assess, manage, monitor and communicate risks. Even in the absence of a formalized ERM function, roles and responsibilities for risk management activities across the business are often defined and executed.<sup>h</sup> These processes provide a path for boards and management to optimize outcomes with the goal of enhancing capabilities to create, preserve and ultimately realize value.<sup>19</sup> While there are many choices in how management will apply ERM practices and no one better approach is universally better than another, research has shown that mature risk management can lead to higher financial performance.<sup>i</sup>

Leveraging these structures and processes can also support organizations to identify, assess and respond to ESG-related risks. Given ESG-related risks can be complex or unfamiliar to organizations, COSO and WBCSD have developed guidance to support entities to better understand and manage the full spectrum of ESG-related risks.

<sup>h</sup> A 2017 report by the AICPA that surveyed 432 executives across large organizations, public companies, financial services and not-for-profit organizations found that 28% of organizations have a “complete formal enterprise-wide risk management process in place” while 37% have a “partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed). (Beasley, M., Branson, B., & Hancock, B. (2017, March). “The state of enterprise risk oversight: an overview of risk management practices 8th edition.”)

<sup>i</sup> For example, a 2013 study by EY found that companies with mature risk management practices outperformed their competitors financially. Companies that ranked in the top 20% in terms of risk management maturity reported earnings three times higher than companies in the bottom 20%. (EY (2013). “Turning risk into results: how leading companies use risk management to fuel better performance.” p. 3) A 2014 study found that “firms with advanced levels of ERM implementation present higher performance, both as financial performance and market evaluation.” (Florio, C. and Leoni, G. (2017). “Enterprise risk management and firm performance: The Italian case” *British Accounting Review* 49. p. 56-74)

## About the guidance – audience

The guidance is designed to be used by any entity facing ESG-related risks – including startups, non-profits, for-profits, large corporations or government entities. The intended audience includes any decision-makers as well as risk management and sustainability practitioners who are looking for guidance on managing ESG-related risks. The audience may include those positioned in an ERM or sustainability function or with oversight responsibilities of those functions, but may also include any risk owner or operations manager whose roles are impacted by ESG-related risks – whether a procurement manager, an analyst in investor relations or a marketing director. The intended audience and their application of this guidance may be described as follows:

Everyone has the responsibility to manage risk. While many ESG risks will be owned by the ESG or sustainability team – as stated by Larry Fink, “We want ESG risk management to be a tool that every manager is looking at.”

- **Decision-makers:** The guidance generates awareness that ESG is a mainstream topic encompassing a wide range of issues that require effective oversight and decision-making.
- **Risk management practitioners:** Risk management practitioners primarily include those with a direct role in the ERM process; however, the guidance is applicable to anyone with responsibilities to manage risk (including operational management, risk owners and line management). The guidance aims to help these practitioners understand the types of ESG-related risks that may impact the entity along with tools, resources and frameworks that can support further understanding.
- **Sustainability practitioners:** Sustainability practitioners primarily include those with a direct role in a sustainability function; however, the guidance is applicable to anyone impacted by ESG-related considerations. The guidance aims to help these practitioners integrate their knowledge and awareness of ESG-related trends, issues, impacts and dependencies with ERM tools and processes to better support identifying, defining, assessing, responding to and disclosing ESG-related risks.

In some cases, practitioners may hold more than one of these roles.

### Application of the guidance to small and medium-sized enterprises (SMEs)<sup>i</sup>

ESG-related risks are as relevant for small and medium-sized entities as they are for large corporations or government bodies. However, resources in SMEs are often limited, making it challenging for these entities to establish robust governance or to adequately identify, assess and respond to all ESG-related risks. SMEs should take a common sense approach that uses available resources efficiently. This may include focusing on strategy and objective-setting and performance (Chapters 2 and 3) while being aware of the importance of continual monitoring and improvement (Chapter 4).

## About the guidance – purpose and scope

### Purpose

The purpose of the guidance is to help organizations apply ERM principles and practices to ESG-related risks. To this extent, the guidance applies COSO’s ERM Framework *Enterprise Risk Management—Integrating with Strategy and Performance*.<sup>20</sup>

<sup>i</sup> This is defined by the European Union as companies with less than 250 employees.



**Figure 2: COSO's Enterprise Risk Management Framework**

While the guidance is aligned to COSO's five components and 20 principles shown in Figure 2, it also offers a practical approach to entities using other risk management frameworks, such as ISO 31000 or entity-specific risk management frameworks. Wherever possible, the document leverages existing frameworks, guidance, practices and tools from both the risk management and sustainability fields.<sup>k</sup> It is not intended to be used as ERM guidance in isolation and should be used in conjunction with an established ERM framework.

The purpose of the guidance is to help an entity achieve:

- **Enhanced resilience:** An entity's medium- and long-term viability and resilience will depend on the ability to anticipate and respond to a complex and interconnected array of risks that threaten the strategy and objectives.
- **A common language for articulating ESG-related risks:** ERM identifies and assesses risks for potential impact to the strategy and business objectives. Articulating ESG-related risks in these terms brings ESG issues into mainstream processes and evaluations.
- **Improved resource deployment:** Obtaining robust information on ESG-related risks enables management to assess overall resource needs and helps optimize resource allocation.
- **Enhanced pursuit of ESG-related opportunities:** By considering both positive and negative aspects of ESG-related risks, management can identify ESG trends that lead to new opportunities.
- **Realized 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 entity's top risks.
- **Improved disclosure:** Improving management's understanding of ESG-related risks can provide the transparency and disclosure investors expect and achieve compliance with jurisdictional reporting requirements.

<sup>k</sup> Examples include the COSO Internal Control Integrated Framework, Global Reporting Initiative (GRI) Standards, the Greenhouse Gas Protocol, International Integrated Reporting Council's (IIRC) Integrated Reporting <IR> Framework, Natural Capital Protocol, Social & Human Capital Protocol, Sustainability Accounting Standards Board (SASB) Standards, Recommendations of the Task Force on Climate-related Financial Disclosures (TCFD).

## Scope of ESG-related risks

This document provides guidance for applying ERM processes to ESG-related risks. Relevant ESG-related risks will depend on the organization, which may apply a narrow definition, focusing on a selection of pertinent environmental or social risks, or a broad application that considers a myriad of issues, such as the MSCI issues set out in Table 2.

**Table 2: MSCI ESG issues and themes<sup>21</sup>**

3 pillars	10 themes	37 ESG key issues	
Environment	Climate change	Carbon emissions Product carbon footprint	Financing environmental impact Climate change vulnerability
	Natural resources	Water stress Biodiversity and land use	Raw material sourcing
	Pollution and waste	Toxic emissions and waste Packaging materiality and waste	Electronic waste
	Environmental opportunities	Opportunities in clean tech Opportunities in green building	Opportunities in renewable energy
Social	Human capital	Labor management Health and safety	Human capital development Supply chain labor standards
	Product liability	Product safety and quality Chemical safety Financial product safety	Privacy and data security Responsible investment Health and demographic risk
	Stakeholder opposition	Controversial sourcing	
	Social opportunities	Access to communications Access to finance	Access to health care Opportunities in nutrition and health
Governance	Corporate governance	Board Pay	Ownership Accounting
	Corporate behavior	Business ethics Anti-competitive practices Tax transparency	Corruption and instability Financial system instability

Many of the governance (i.e., the “G”) issues listed in Table 2, such as ownership, accounting and anti-competitive practices, have been long-standing issues for organizations and are generally well managed in established ERM processes. The guidance therefore places greater focus on environmental and social issues, which for some organizations have historically been managed *outside* the influence of robust governance and ERM. The governance risks discussed throughout the guidance tend to focus on either the governance of environmental or social issues, or other issues that have recently gained interest in the business community such as business ethics or diversity on boards.

## About the guidance – structure

The guidance has five chapters that mirror the five components of the COSO ERM Framework, starting with Governance and culture and Strategy and objective-setting, then moving through the ERM process focusing on Performance (identifying, assessing and prioritizing and for responding to ESG-related risks) and finally the Review and revision and Information, communication and reporting for ESG-related risks.

- 1. Governance and culture for ESG-related risks:** 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 raising the board and executive management’s awareness of ESG-related risks – supporting a culture of collaboration among those responsible for risk management of ESG issues.
- 2. Strategy and objective-setting for ESG-related risks:** All entities have impacts and dependencies on nature and society. Therefore, a strong understanding of the business context, strategy and objectives 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.

### 3. Performance for ESG-related risks:

- a) **Identifies risk:** Organizations use multiple approaches for identifying ESG-related risks: megatrend analysis, SWOT analysis, impacts and dependency mapping, stakeholder engagement and ESG materiality assessments. These tools can help identify and express ESG issues in terms of how a risk threatens achievement of an entity's strategy and business objectives. Applying these approaches through collaboration between risk management and sustainability practitioners elevates ESG-related risks to the risk inventory and positions them for appropriate assessment and response.
- b) **Assesses and prioritizes risks:** Companies have limited resources, so they cannot respond equally to 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 a language management can use to prioritize risks. Leveraging ESG subject-matter expertise is critical to ensure emerging or longer-term ESG-related risks are not ignored or discounted, but instead assessed and prioritized appropriately.
- c) **Implements risk responses:** How an entity responds to identified risks will ultimately determine how effectively the entity preserves or creates value over the long term. Adopting a range of innovative and collaborative approaches that consider the source of a risk as well as the cost and benefits of each approach supports the success of these responses.






**4. Review and revision for ESG-related risks:** Review and revision of ERM activities are critical to evaluating their effectiveness and modifying approaches as needed. Organizations can develop specific indicators to alert management of changes that need to be reflected in risk identification, assessment and response. This information is reported to a range of internal and external stakeholders.

**5. Information, communication and reporting for ESG-related risks:** Applying ERM to ESG-related risks includes consulting with risk owners to identify the most appropriate information to be communicated and reported internally and externally to support risk-informed decision-making.



## Is your entity ready for the ESG-related risks of today and tomorrow?

The following actions are outlined throughout the guidance to help an entity to identify and manage the ESG-related risks of today while maintaining resilience to adapt and respond to the megatrends of tomorrow.

Chapter	Actions
<b>1</b>	<b>Governance and culture for ESG-related risks</b>
	<input type="checkbox"/> Map or define the organization's mandatory or voluntary ESG-related requirements <input type="checkbox"/> Consider opportunities for embedding ESG in the entity's culture and core values <input type="checkbox"/> Be informed of the ways to increase board awareness of ESG-related risks <input type="checkbox"/> Map the operating structures, risk owners for ESG-related risks, reporting lines and end-to-end ERM and strategic planning process to identify areas for improved oversight and collaboration <input type="checkbox"/> Create opportunities for collaboration throughout the organization <input type="checkbox"/> Embed ESG-related skills, capabilities and knowledge in hiring and talent management to promote integration
<b>2</b>	<b>Strategy and objective-setting for ESG-related risks</b>
	<input type="checkbox"/> Examine the value creation process and business model to understand impacts and dependencies on all capitals in the short, medium and long term. To assist with this understanding, conduct: <ul style="list-style-type: none"> <li>- Megatrend analysis to understand the impact of emerging issues in the external environment</li> <li>- Strengths, weaknesses, opportunities and threats (SWOT) analysis</li> <li>- Impact and dependency mapping for all types of capital</li> <li>- An ESG materiality assessment to describe significant ESG issues</li> <li>- Engagement with internal and external stakeholders to understand emerging ESG trends</li> <li>- Analysis leveraging ESG-specific resources</li> </ul> <input type="checkbox"/> Throughout the risk management process, align with the entity's strategy, objectives and risk appetite <input type="checkbox"/> Consider the ESG-related risks that will impact the entity's strategy or objectives
<b>3</b>	<b>Performance for ESG-related risks</b>
<b>3a</b>	<b>Identifies risk</b>
	<input type="checkbox"/> Examine the entity's risk inventory to determine which ESG-related risks have or have not been identified <input type="checkbox"/> Involve ESG risk owners and sustainability practitioners in the risk identification process to leverage subject-matter expertise <input type="checkbox"/> Convene meetings with both risk management and sustainability practitioners to understand ESG-related risks <input type="checkbox"/> Identify the ESG-related risks that may impact the organization's strategic and operational plans <input type="checkbox"/> Define the impact of ESG-related risks on the organization precisely <input type="checkbox"/> Use root cause analysis to understand drivers of the risk
<b>3b</b>	<b>Assesses and prioritizes risk</b>
	<input type="checkbox"/> Understand the required output of the risk assessment (e.g., the impact in terms of the strategy and business objectives) <input type="checkbox"/> Understand the entity's criteria for prioritizing risks <input type="checkbox"/> Understand the metrics used by the entity for expressing risk (i.e., quantitative or qualitative) <input type="checkbox"/> Select appropriate assessment approaches to measure risk severity <input type="checkbox"/> Select and document data, parameters and assumptions <input type="checkbox"/> Leverage subject-matter expertise to prioritize ESG-related risks <input type="checkbox"/> Identify and challenge organizational bias against ESG issues
<b>3c</b>	<b>Implements risk responses</b>
	<input type="checkbox"/> Select an appropriate risk response based on entity-specific factors (e.g., costs and benefits and risk appetite) <input type="checkbox"/> Develop the business case for the response and obtain buy-in <input type="checkbox"/> Implement the risk response to manage the entity's risk <input type="checkbox"/> Evaluate risk responses at the entity level to understand the overall impacts to the entity risk profile
<b>4</b>	<b>Review and revision for ESG-related risks</b>
	<input type="checkbox"/> Identify and assess internal and external changes that may substantively affect the strategy or business objectives <input type="checkbox"/> Review ERM activities to identify revisions to ERM processes and capabilities <input type="checkbox"/> Pursue improvements in how ESG-related risks are managed by ERM
<b>5</b>	<b>Information, communication and reporting for ESG-related risks</b>
	<input type="checkbox"/> Identify relevant information and communication channels for internal and external communication and reporting <input type="checkbox"/> Communicate and report relevant ESG-related risk information internally for decision-making <input type="checkbox"/> Communicate and report relevant ESG-related risk information externally to meet regulatory obligations and support stakeholder decision-making <input type="checkbox"/> Continuously identify opportunities for improving the quality of ESG-related data reported internally and externally

## Notes

## Notes



## References

- <sup>1</sup> MSCI (2018, April). "ESG Ratings Methodology: Executive Summary." Retrieved from <https://www.msci.com/documents/10199/123a2b2b-1395-4aa2-a121-ea14de6d708a>
- <sup>2</sup> Robeco. "ESG definition." Retrieved from <https://www.robeco.com/me/key-strengths/sustainability-investing/glossary/esg-definition.html>
- <sup>3</sup> COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 9
- <sup>4</sup> Unilever. "Our strategy for sustainable growth." Retrieved from Unilever: <https://www.unilever.com/sustainable-living/our-strategy/>
- <sup>5</sup> Unilever. "Defining our material issues." Retrieved from Unilever: <https://www.unilever.com/sustainable-living/our-approach-to-reporting/defining-our-material-issues/index.html>
- <sup>6</sup> World Economic Forum (2018, January 17). "The Global Risks Report 2018, 13th Edition." Retrieved from World Economic Forum: [reports.weforum.org/global-risks-2018/](https://reports.weforum.org/global-risks-2018/)
- <sup>7</sup> Society for Corporate Governance and BrownFlynn (2018, June). "ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals." p. 6.
- <sup>8</sup> Akipeo Inc. (2018, March). "The Financial Materiality of Environmental Risks in Food Production: A preliminary review of the downside exposure and upside opportunities for financial institutions engaging in soft commodity supply chains." pp. 7-9
- <sup>9</sup> EY (2018). "How can data lead to better corporate governance?" Retrieved from <https://www.ey.com/us/en/issues/governance-and-reporting/ey-corporate-governance-by-the-numbers>
- <sup>10</sup> KPMG (2017). "ESG, strategy and the long view: A framework for board oversight." p. 5
- <sup>11</sup> Society for Corporate Governance and BrownFlynn (2018, June). "ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals." p. 10
- <sup>12</sup> Fink, L. (2018). Larry Fink's Annual Letter to CEOs: A Sense of Purpose. Retrieved from BlackRock: <https://www.blackrock.com/corporate/investor-relations/larry-fink-ceo-letter>
- <sup>13</sup> The Governance & Accountability Institute (2018, March 20). "Flash Report: 85% of S&P 500 Index® Companies Publish Sustainability Reports in 2017." Retrieved from <https://www.ga-institute.com/press-releases/article/flash-report-85-of-sp-500-indexR-companies-publish-sustainability-reports-in-2017.html>
- <sup>14</sup> "SGX-ST Listing Rules: Practice Note 7.6." Retrieved from [http://rulebook.sgx.com/net\\_file\\_store/new\\_rulebooks/s/g/SGX\\_Mainboard\\_Practice\\_Note\\_7.6\\_July\\_20\\_2016.pdf](http://rulebook.sgx.com/net_file_store/new_rulebooks/s/g/SGX_Mainboard_Practice_Note_7.6_July_20_2016.pdf)
- <sup>15</sup> NASDAQ(2018). "ESG Reporting Guide: A voluntary support program for the Nordic and Baltic markets." Retrieved from <https://business.nasdaq.com/esg-guide>
- <sup>16</sup> TCFD (2017, June). "Recommendations of the Task Force on Climate-related Financial Disclosures." Retrieved from <https://www.fsb-tcfd.org/publications/final-recommendations-report/>
- <sup>17</sup> WBCSD (2017, January 18). "Sustainability and enterprise risk management: the first step towards integration." Retrieved from WBCSD: <http://www.wbcd.org/Projects/Non-financial-Measurement-and-Valuation/ResourcesSustainability-and-enterprise-risk-management-The-firststep-towards-integration>
- <sup>18</sup> COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 10
- <sup>19</sup> COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 3
- <sup>20</sup> COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance."
- <sup>21</sup> MSCI (2018, April). "ESG Ratings Methodology: Executive Summary." Retrieved from <https://www.msci.com/documents/10199/123a2b2b-1395-4aa2-a121-ea14de6d708a>

This publication is released in the name of the WBCSD and COSO. It does not, however, necessarily mean that every member company and organization agrees with all expressed views. This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, the WBCSD, COSO, their members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.



# Enterprise Risk Management

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

EXECUTIVE SUMMARY

October 2018

***COSO***

[coso.org](http://coso.org)



[wbcsd.org](http://wbcsd.org)