Enterprise Risk Management

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



October 2018

COSO | wbcsd

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.

Table of Contents

Introduction 1

1. Governance and culture for ESG-related risks 13

2. Strategy and objective-setting for ESG-related risks 23

3. Performance for ESG-related risks 39

   3a. Identifies risk 40

   3b. Assesses and prioritizes risks 47

   3c. Implements risk responses 67

4. Review and revision for ESG-related risks 77

5. Information, communication and reporting for ESG-related risks 85

Glossary 93

Acknowledgements 96

Appendices 98

References 107

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.

This 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.[a] 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 this guidance, the term ESG-related risks encompasses the issues that are prominent on investors' and other stakeholders' agendas, such as those described by MSCI[1] and Robeco[2] in Table 1:

Table 1: Definitions of ESG

	MSCI definition	Robeco definition
Environmental	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.
Social	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.
Governance	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)[b] 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."[3] 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).

[a] Although these terms are used interchangeably, this 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.

[b] 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."[4] The table below highlights Unilever's identified ESG topics that may affect achievement of this purpose or vision.[5]

Improving health and well-being	Reducing environmental impact	Enhancing livelihoods	Responsible business practices	Wider sustainability topics
• Nutrition and diets • Sanitation and hygiene	• Agricultural sourcing • Climate action • Deforestation • Packaging and waste • Water • Non-agricultural sourcing	• Human rights • Women's rights and opportunities • Economic inclusion • Employee well-being • Fair compensation	• Ethics, values and culture • Data security and privacy • Governance and accountability • Responsible marketing and advertising • Tax and economic contribution • Responsible use of innovation and technology	• Trusted products and ingredients • Animal testing and welfare • Consumers and sustainability • Talent • Communicable diseases

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*[6] 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"[c] are now far more common – and can manifest more quickly and significantly. A report by the Society for Corporate Governance[7] in the United States found that these issues often, although not always:

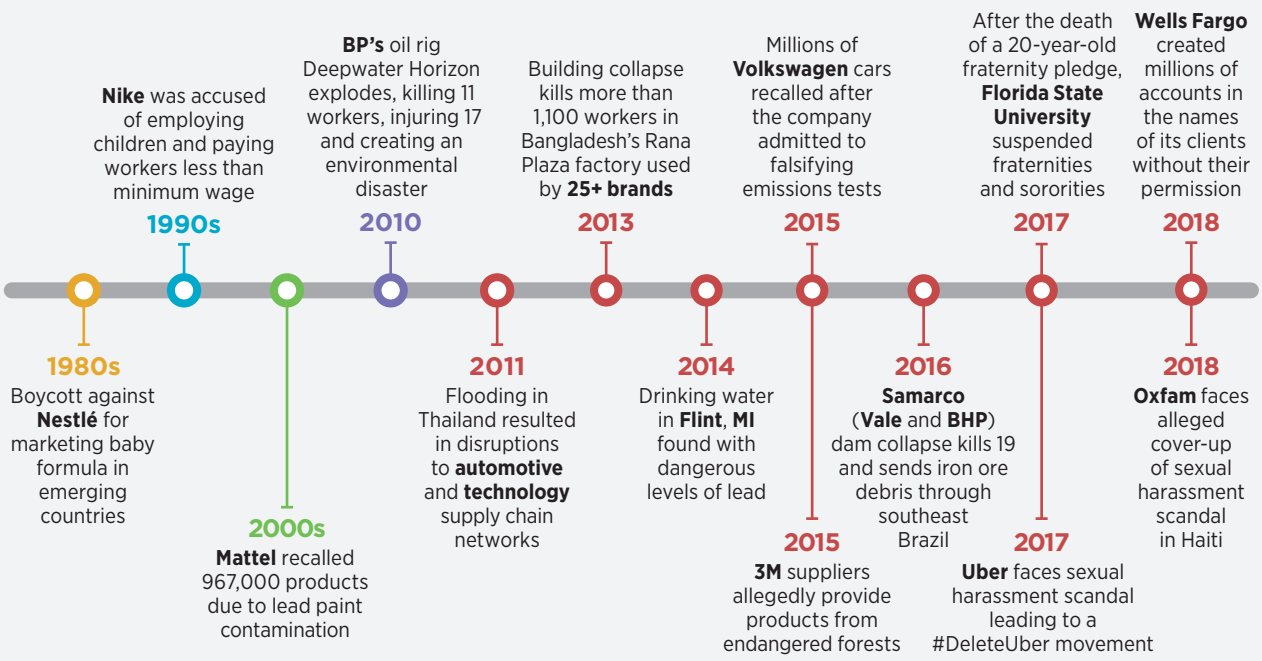
- Derive from a risk or impact inherent in the core operations or products
- Have the potential to meaningfully damage a company's intangible value, reputation or ability to operate
- Are accompanied by persistent media interest, organized stakeholders and associated public policy debates that could 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

[c] 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.[8]

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.[9] 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).[d]

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.[10]

[d] 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 then 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.[e] 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.[11]

> "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?"[12]
>
> **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.[f] 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.[13]

There has also been growth in ESG-related regulation and disclosure requirements – totaling 1,052 requirements (80% of which are mandatory) in 63 countries.[g] 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.[14] NASDAQ's Nordic and Baltic exchanges issued voluntary guidance in March 2017.[15]

The *Recommendations of the Task Force for Climate-related Financial Disclosures* (TCFD)[16] 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.

[e] 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?"

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

[g] 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/

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*[17] 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."[18]

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.[h] 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.[19] 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.[i]

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.

[h] 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.")

[i] 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 this guidance – audience

This 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 this guidance to small and medium-sized enterprises (SMEs)[i]

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 this 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*.[20]

[i] This is defined by the European Union as companies with less than 250 employees.

Figure 2: COSO's Enterprise Risk Management Framework



GOVERNANCE & CULTURE

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops and Retains Capable Individuals

STRATEGY & OBJECTIVE-SETTING

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

PERFORMANCE

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

REVIEW & REVISION

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

INFORMATION, COMMUNICATION & REPORTING

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture and Performance

© 2017 COSO. Used by permission. All rights reserved.

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, this document leverages existing frameworks, guidance, practices and tools from both the risk management and sustainability fields.[k] 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 this 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.

[k] 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[21]

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. This 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 this 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.



Throughout the guidance, icons are used to indicate specific actions or guidance (summarized in the table below), case studies or examples or references to an illustrative example (Pro Packaging & Paper) included in Appendix VIII.

The following icons are used throughout this guidance to indicate:

Guidance **Case study or example** **Pro Paper & Packaging**

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
1	**Governance and culture for ESG-related risks**
	☐ Map or define the organization's mandatory or voluntary ESG-related requirements ☐ Consider opportunities for embedding ESG in the entity's culture and core values ☐ Be informed of the ways to increase board awareness of ESG-related risks ☐ 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 ☐ Create opportunities for collaboration throughout the organization ☐ Embed ESG-related skills, capabilities and knowledge in hiring and talent management to promote integration
2	**Strategy and objective-setting for ESG-related risks**
	☐ 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: - Megatrend analysis to understand the impact of emerging issues in the external environment - Strengths, weaknesses, opportunities and threats (SWOT) analysis - Impact and dependency mapping for all types of capital - An ESG materiality assessment to describe significant ESG issues - Engagement with internal and external stakeholders to understand emerging ESG trends - Analysis leveraging ESG-specific resources ☐ Throughout the risk management process, align with the entity's strategy, objectives and risk appetite ☐ Consider the ESG-related risks that will impact the entity's strategy or objectives
3	**Performance for ESG-related risks**
3a	**Identifies risk**
	☐ Examine the entity's risk inventory to determine which ESG-related risks have or have not been identified ☐ Involve ESG risk owners and sustainability practitioners in the risk identification process to leverage subject-matter expertise ☐ Convene meetings with both risk management and sustainability practitioners to understand ESG-related risks ☐ Identify the ESG-related risks that may impact the organization's strategic and operational plans ☐ Define the impact of ESG-related risks on the organization precisely ☐ Use root cause analysis to understand drivers of the risk
3b	**Assesses and prioritizes risk**
	☐ Understand the required output of the risk assessment (e.g., the impact in terms of the strategy and business objectives) ☐ Understand the entity's criteria for prioritizing risks ☐ Understand the metrics used by the entity for expressing risk (i.e., quantitative or qualitative) ☐ Select appropriate assessment approaches to measure risk severity ☐ Select and document data, parameters and assumptions ☐ Leverage subject-matter expertise to prioritize ESG-related risks ☐ Identify and challenge organizational bias against ESG issues
3c	**Implements risk responses**
	☐ Select an appropriate risk response based on entity-specific factors (e.g., costs and benefits and risk appetite) ☐ Develop the business case for the response and obtain buy-in ☐ Implement the risk response to manage the entity's risk ☐ Evaluate risk responses at the entity level to understand the overall impacts to the entity risk profile
4	**Review and revision for ESG-related risks**
	☐ Identify and assess internal and external changes that may substantively affect the strategy or business objectives ☐ Review ERM activities to identify revisions to ERM processes and capabilities ☐ Pursue improvements in how ESG-related risks are managed by ERM
5	**Information, communication and reporting for ESG-related risks**
	☐ Identify relevant information and communication channels for internal and external communication and reporting ☐ Communicate and report relevant ESG-related risk information internally for decision-making ☐ Communicate and report relevant ESG-related risk information externally to meet regulatory obligations and support stakeholder decision-making ☐ Continuously identify opportunities for improving the quality of ESG-related data reported internally and externally

1. Governance and culture for ESG-related risks

Introduction

Governance is the systems and processes that ensure the overall effectiveness of an entity – whether a business, government or multilateral institution.[1] Effective governance provides the oversight, structure and culture needed to establish the goals of the organization, the means to pursue them and the ability to understand any associated risks.

The COSO ERM Framework emphasizes that governance, including strong oversight, is a prerequisite to effectively identifying, assessing and addressing the full spectrum of risks to the organization. Incorporating ESG-related risks into the governance structure, systems and processes is critical for overcoming the challenges many organizations face in managing these risks – such as organizational silos, quantification challenges and organizational biases.



This chapter relates to the COSO ERM Framework component on Governance and culture and the five associated principles:[2]

1. **Exercises board risk oversight:** The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes operating structures:** The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines desired culture:** The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates commitment to core values:** The organization demonstrates a commitment to the entity's core values.
5. **Attracts, develops and retains capable individuals:** The organization is committed to building human capital in alignment with the strategy and business objectives.

This chapter outlines the following actions to help risk management and sustainability practitioners integrate ESG-related risks into ERM governance and culture:

- ☐ Map or define the organization's mandatory or voluntary ESG-related requirements

- ☐ Consider opportunities for embedding ESG in the entity's culture and core values
- ☐ Be informed of the ways to increase board awareness of ESG-related risks
- ☐ 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
- ☐ Create opportunities for collaboration throughout the organization
- ☐ Embed ESG-related skills, capabilities and knowledge in hiring and talent management to promote integration

Oversight and governance for ESG

Each organization has its own approach to oversight and governance. The *King IV Report on Corporate Governance for South Africa*[3] (King IV report), published in 2016, provides one perspective on what defines good governance in the context of ESG-related business and societal changes, such as inequality, climate change, radical transparency and rapid technological and scientific advancements. The King IV report[a] offers a principles-based approach to ethical and effective leadership by the governing body in pursuit of defined outcomes, that include an ethical culture, good performance, effective control and legitimacy. Some of the King IV report recommendations that can help support ESG-related risk governance include:[4]

- Establishing a social and ethics committee as a prescribed board committee.
- Emphasizing the critical role of stakeholders in the governance process. The board should consider the legitimate and reasonable needs, interests and expectations of stakeholders, while recognizing the role of stakeholders to hold the board and the company accountable for their actions and disclosures.
- Having a strong focus on opportunity management as well as risk management – so task the risk committee with identifying opportunities linked to certain risks.
- Requiring the board to pay specific attention to opportunities in the strategic planning process.

Responsibilities to manage ESG-related risk

ESG-related risks are often characterized as evolving, interconnected, longer-term or less familiar to an organization and, therefore, difficult to manage effectively. However, the potential impact of these risks on an organization's performance can be significant, and so the responsibility for the organization to manage these risks is no different than for any other business risk. Even when ESG issues are managed by a separate function, such as a corporate social responsibility or sustainability department, integrating ESG-related risks into the core ERM structures and processes of the organization is critical for supporting an entity and its directors to meet their responsibilities.

This section outlines some of the regulatory and voluntary ESG-related obligations that may drive an entity's responsibilities in relation to ESG-related risks.

Questions for risk management and sustainability practitioners to consider:

- Has the entity had financial, operational or reputational issues in the past because of an ESG-related event?
- What are the ESG-related regulations, requirements or obligations in the entity's markets? Are there risks that coincide with a failure to adhere to these regulations, requirements or obligations?
- How are relevant regulations, requirements or obligations communicated to leadership and integrated into operations?
- Does the entity have a clear message on how its mission, vision, core values or long-term strategy considers ESG-related risks?
- Which policies, statements or voluntary commitments have the entity made in relation to ESG issues?

Regulatory responsibilities

In many countries, financial, health and safety and environmental regulators may bring civil or criminal penalties to a company executive or employee found mismanaging ESG issues. For example, in 2015, two former Quality Egg LLC (a US-based consumer products company) executives were found to be criminally liable for their roles in a 2010 salmonella outbreak – due to their knowledge that the egg facilities were at risk of contamination. Fines were issued to both the company (USD$6.8 million) and the executives (USD$100,000 each).[5]

[a] The King IV Report has been designed to apply to listed and unlisted companies, for-profit and non-profit as well as private and public entities.

Even when regulatory fines or penalties are not enforced, entities may still experience financial impacts for failing to manage an ESG-related risk. Examples include the decline in market value of Chipotle after food-borne illness scares,[6] or the USD$500 million litigation settlement paid by Michigan State University in the wake of sexual abuse allegations regarding the doctor of female gymnasts.[7]

Governing bodies are tasked with ensuring the long-term best interests of the entities they govern. Part of this is routine management of enterprise risks. As with any potentially significant risks, ESG matters should be included in enterprise risk assessments and disclosures.[b] See Appendix II for an overview of risk disclosure requirements in a selection of jurisdictions.

Specific ESG-related requirements are also emerging in many jurisdictions. Some of these regulations impose duties, while others establish requirements for companies to disclose information on how they are managing ESG issues. Many of these regulations have enforcement provisions that extend to senior executives (see Table 1.1).

One-tier versus two-tier board structures

A one-tier board typically oversees executive management and its decisions on behalf of shareholders (common in the US, UK and Australia). Under a two-tier system, executive directors of the management board determine and implement the company's objectives while the non-executive directors of the supervisory board monitor decisions on behalf of other parties (more common in Europe).[8]

Guidance

- ☐ Map or define the organization's mandatory or voluntary ESG-related requirements

Table 1.1: Examples of ESG-related regulations

Regulation	Scope	Enforcement
Directive 2014/95EU (European Union Directive on Non-financial Reporting)[9]	EU law requiring approximately 6,000 large companies (including listed companies, banks, insurance companies and public-interest entities) to disclose certain information (e.g., environmental protection and respect for human rights) on the way they operate and manage social and environmental challenges.	Full reporting compliance is required by reporting year 2017. The country in which the company is based is responsible for enforcement. Violation of the requirements is considered a violation of the measure itself.
Dodd-Frank 1502 (Conflict Minerals Rule)[10]	US law requiring SEC filers to disclose whether any of their manufactured or contracted products contain conflict minerals (i.e., tantalum, tin, gold or tungsten) that originate in the Democratic Republic of Congo or any of the adjoining parties.	Issuers are subject to Section 18 liability[c] (Exchange Act of 1934) if they do not comply in good faith. Outside of the legal implications of not complying, issuers may also face pressure from human rights activists, non-governmental organizations (NGOs), or consumer or other market forces to prove they are conflict free.
Lacey Act of 1900[11]	US conservation law prohibiting the trade of wildlife, fish and plants taken, possessed, transported or sold illegally.	A misdemeanor violation is punishable by up to one year in prison. There are also fines of USD$200,000 for companies and USD$100,000 for an individual. Felony culpability is punishable by up to five years in prison and a USD$500,000 fine per violation for a company and USD$250,000 for an individual.
Law 2010-788 (Grenelle II Law)[12]	French law requiring listed and unlisted companies with more than 500 employees and €100 million in revenue to issue an integrated report with third-party assurance reporting on social, environmental and economic indicators.	Companies are required to produce information at stakeholder request. Further laws in 2015 and 2017 strengthen reporting requirements and hold boards accountable to fines/penalties if they do not report ESG information to interested parties.
Modern Slavery Act 2015[13]	UK law designed to tackle slavery, servitude and forced or compulsory labor and human trafficking, including provisions for the protection of victims.	Although there are no direct penalties, the UK Government has the ability to bring proceedings in the High Court for an injunction requiring an organization to comply.
National Greenhouse and Energy Reporting Act 2007 (NGER Act)[14]	Australian federal law requiring certain companies to report and disseminate information about greenhouse gas emissions, energy production and energy consumption in line with this framework.	Failure to comply with obligations under the NGER Act may result in penalties of up to USD$220,000 for the corporation and for executive officers. Criminal penalties may be imposed in serious offenses.

[b] For example, the US Securities and Exchange Commission (SEC) regulations require publicly listed companies to disclose risk factors associated with their securities. Similarly, the EU Directive 2004/109/EC requires that companies include a description of the principal risks and uncertainties that they face in the annual financial report. The Australian Stock Exchange recommends that all listed entities establish a risk management framework and periodically review the effectiveness of that framework. See to Appendix II for more information.

[c] Section 18 liability is a private right of action for investors to sue for false or misleading material statements in a company's SEC filings. With this enforcement, it is acknowledged that it would be difficult for an investor to bring a case under Section 18 because the burden of proof is high.

Voluntary responsibilities

In addition to an entity's regulatory requirements, management and the board should be aware of any voluntary codes or obligations undertaken or signed by the entity. This may also include any sustainability, human rights, natural resource, supply chain and commodity, privacy or environmental policies, or statements that a company approves. Some of these commitments are made at the CEO level (such as the UN Global Compact or PRI) and, while voluntary, constitute a commitment to which an entity may be held accountable. Companies that do not uphold the principles or requirements may be exposed to reputational damage and scrutiny from shareholders, customers, NGOs or communities. See Appendix III for some of the commonly adopted voluntary frameworks and commitments.

The Reporting Exchange

In partnership with CDSB and Ecodesk, WBCSD launched the Reporting Exchange (reportingexchange.com) in 2017. It is *the* global resource for corporate sustainability reporting, with requirements from over 60 countries.

There is also a multitude of voluntary sector-, issue- or geography-specific codes or standards that an entity may choose to follow. For example, apparel companies that engage suppliers from Bangladesh may choose to participate in the Bangladesh Accord, which targets building safety and working conditions of factories in the region.[15] Similarly, entities that are members of the Roundtable on Sustainable Palm Oil (RSPO)[16] commit themselves to advancing the production, procurement, finance and use of sustainable palm oil products. For the seafood sector, the Marine Stewardship Council (MSC)[17] and the Aquaculture Stewardship Council (ASC)[18] provide standards and certification for environmental sustainability and social responsibility for aquaculture producers, seafood processors, retail and food-service companies, scientists, conservation groups and consumers.

Embedding ESG awareness in the entity's culture

The COSO ERM Framework defines culture as the "attitudes, behaviors and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision and core values of the organization."[19] Taken together, the mission, vision, core values and strategy describe why an entity exists, who it is, what it intends to do and how it intends to do it.[20] These elements provide insight, offer motivation and point the way forward as the entity grows and achieves its goals. As such, embedding ESG elements into the mission, vision and core values may help to cultivate a culture that exhibits "ESG conscious" behaviors and decisions.

Stora Enso, a global leader in providing renewable solutions for packaging, biomaterials, wooden constructions and paper, has demonstrated the importance of corporate governance for integrating sustainability into ERM.[21] Stora Enso's stated purpose of "Do Good for the People and the Planet" embodies the importance of sustainability. Sustainability is fundamental to the investor proposition and strategy. Further, it is integral to decision-making across all of Stora Enso's operations and activities such as the production and sales of renewable products, buying trees from local forest owners, selling electricity generated at its mills and managing its logistics on a global scale.[22,d]

Specific events, such as leadership changes, mergers and acquisitions, lessons learned from unforeseen incidents, negative publicity from NGO campaigns, investigative journalism or consumer pressure on ESG issues, may be a catalyst for change in culture. These events may challenge or threaten the existing culture and provide an opportunity for the organization to modify or strengthen its culture.

Guidance

- ☐ Consider opportunities for embedding ESG in the entity's culture and core values

[d] A full case study is available at wbcsd.org. (WBCSD (2017). "Stora Enso: A governance model and culture that enables enterprise risk management and sustainability integration.")

Some considerations for enhancing ESG culture and integration include:[23]

- Do the organization's mission, vision and core values address ESG-related risks?
- Does the tone from the organization's leaders convey expectations on ESG?
- Does management carry out the entity's mission, vision, core values and strategy?
- Is the entity hiring the right talent and is the selection process compatible with building an inclusive and talented workforce that reflects its business needs?
- Does the entity tie compensation and promotion decisions to the metrics that advance performance on critical ESG issues?
- Is the entity empowering people and giving authority to teams that can make decisions by considering ESG information reflecting local knowledge?
- Is the entity's culture promoting employee behaviors that are consistent with priorities?

For more information on embedding sustainability into corporate culture, refer to *Embedding Sustainability in Organizational Culture: A How to Guide for Executives*.[24]

ESG at the board level

In accordance with the COSO ERM Framework, the board "provides oversight of the company's strategy and carries out governance responsibilities to support management in achieving its strategy and business objectives."[25] These responsibilities apply to any governing body that provides organizational oversight.[e]

Questions for risk management and sustainability practitioners to consider:

- Is the board aware of the ESG-related risks that may impact achievement of the entity's strategy and objectives?
- Is there an escalation path within the organization that ensures that material ESG-related risks are brought to the attention of the board?
- Does the board have access to the information needed to evaluate risks emerging from ESG trends?
- Does the board have the relevant capabilities and capacities to appreciate the implications of ESG issues?
- Is there a subcommittee focused on ESG-related risks?
- Are significant ESG-related risks and resources for the entity's control and management confirmed regularly by the board?
- Does the board charter capture governance of ESG-related risks?
- Is the board receiving regular reports about ESG-related risks?
- What are board members' expectations relative to ERM and ESG?

Overseeing the full spectrum of risks requires boards to have an adequate understanding, appropriate information and experience/expertise to guide the organization through the ESG-related risks that may threaten the business strategy or objectives.

To achieve this, the board may require regular briefings on relevant ESG matters and the entity's approach to managing them.[26] Organizations with more mature ESG programs may have established specific responsibilities at the board or committee level to monitor and report back on significant ESG issues or risks. These approaches for enhancing ESG-related risk awareness at the board level are described in Table 1.2.

Guidance

☐ Be informed of the ways to increase board awareness of ESG-related risks

[e] The COSO ERM Framework uses the term "board of directors" or "board" to encompass the governing body, including board, supervisory board, board of trustees, general partners or owner.

Table 1.2: Approaches for enhancing ESG-related risk awareness on the board

Approaches	Description	Example
Include references to ESG-related risks or issues in the board charter	In some cases, a formal mandate is used to describe the board's (or committee's) responsibilities for overseeing ESG-related risks. Specific reference to ESG issues in the charter or terms of reference provides clear direction for ESG integration at the board level.	Stora Enso has a subcommittee on sustainability and ethics which includes the following duties in its charter: • Review of matters, including those of a legislative and regulatory nature, which may have a significant impact on Stora Enso's activities and reputation with respect to sustainability and ethics • Review of social, political, economic and environmental trends that may have a significant impact on Stora Enso's business activities and performance[27]
Establish a board committee that focuses on ESG-related risks and issues	A separate committee with an ESG focus may be established with a clear mandate to oversee ESG-related risks. The remit of this committee may include a selection of ESG-related risks, such as environmental and social risks, with governance risks managed by the risk or audit committee. Other board committees, such as the audit committee, may focus on specific aspects of ESG-related risk, such as the reporting and disclosure of greenhouse gas emissions or human rights.	Mondi plc, an international paper and packaging company, divides responsibility for overseeing risks between a sustainable development subcommittee and the audit committee.[28] The sustainable development committee manages health, safety and environment risks, and the audit committee manages the rest of the company's risks.
Appoint directors with ESG-related knowledge or expertise to the board or relevant committee	Boards should understand the company's most important ESG issues and have access to expert points of view to inform the board or relevant committee (e.g., ESG committee or audit committee). Some boards may choose to appoint directors with specific ESG experience. Regardless of whether there are sustainability experts on the board, companies should consider whether directors should have some minimum competency in areas relevant to the entity's ESG issues.	In 2017, ExxonMobil added an atmospheric scientist and former president and director of the Woods Hole Oceanographic Institution[f] to its 13-member board of directors.[29] Other companies including ConocoPhillips and GM[30] also recently added directors with ESG to their boards.

Risk management and sustainability practitioners can play a critical role in enhancing ESG-related risk awareness at the board level by preparing information for the board (e.g., KPIs and metrics that reflect the organization's ESG performance), determining what communication channels should be used and establishing how frequently the information should be provided. In addition, practitioners may leverage internal capabilities in the organization to provide informed perspectives to individual board members and/or committees on ESG-related risks. Where appropriate, practitioners may also obtain expert third-party opinion or perspectives.

> "Not every director or member of senior management can be an 'ESG expert' but directors and appropriate company personnel should educate themselves on the key ESG issues facing the company and be able to converse comfortably on those issues that matter or present significant risks."[31]
>
> **Wachtell, Lipton, Rosen and Katz**

For additional guidance on enhancing board awareness for ESG, refer to the UNEP's *Integrated Governance: A New Model of Governance for Sustainability*,[32] *NACD's Governance Challenges 2017: Board Oversight of ESG*,[33] *Oversight of Corporate Sustainability Activities (Director's Handbook Series; 2014-2015)*,[34] Ceres 2018 report *Systems Rule: How Board Governance Can Drive Sustainability Performance*[35] or Eccles and Youman's 2015 working paper *Materiality in Corporate Governance: The Statement of Significant Audiences and Materiality*.[36]

[f] Woods Hole Oceanographic Institution is dedicated to advancing knowledge of the ocean and its connection with the Earth system through a sustained commitment to excellence in science, engineering, and education, and to the application of this knowledge to problems facing society.

ESG at the management level

The board is ultimately responsible and accountable for the organization's long-term success, with the CEO entrusted with decision-making and management activities. The CEO delegates to company executives who themselves delegate down the chain of command to management, which performs the operational activities of risk management. An example of some of the different roles in the organization throughout the ERM process can be found in Appendix V.

Questions for risk management and sustainability practitioners to consider:

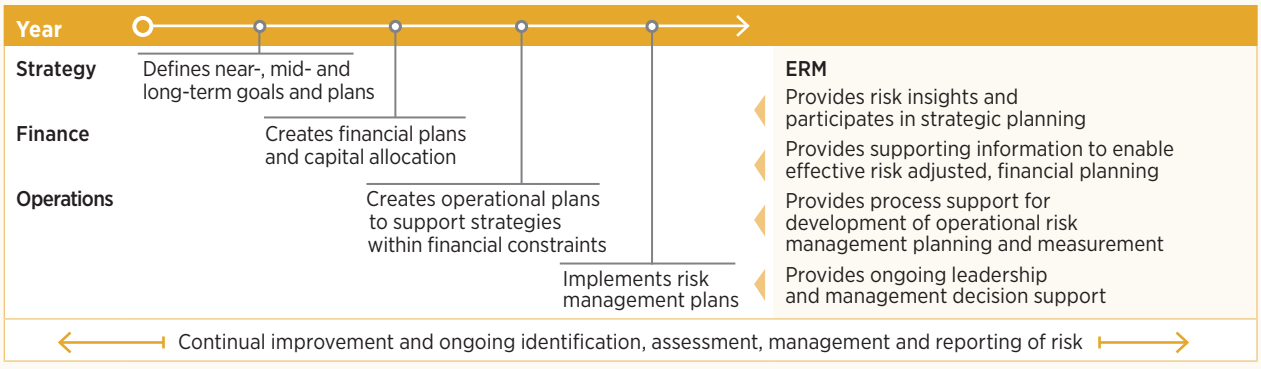
- Is oversight of the ERM process clearly defined and implemented?
- Do risk and sustainability have operationally and strategically integrated processes?
- Are continual process improvements jointly developed and monitored?
- Does the ERM process connect ESG to risk management?
- Is there agreement on which stakeholder interests are critical to the long-term success of the entity?
- Is ERM embedded in key business processes, reporting and metrics?
- What are competitors and peers doing to identify, manage and disclose their ESG-related risks?
- Have ERM practitioners been trained in ESG and vice versa?

The ERM structures, process and continual improvement

Organizations should not approach ERM solely as a compliance process, a once-a-year activity or checklist of activities to be performed on an annual cycle. ERM is intended to be ongoing and iterative, embedded in everyday business processes to allow the entity to stay aware and ahead of emerging threats and opportunities.

Nonetheless, it is common for organizations to have a structured timeline for ERM activities. This is partly dictated by reporting obligations and other strategic and regulatory milestones, such as the budgeting cycle, strategic planning process and annual general meetings. Sustainability practitioners should obtain an understanding of the end-to-end risk management process and strategic planning cycle to allow relevant ESG subject-matter experts to be included in annual surveys or workshops and ESG-related risk to be included in strategic planning and operational discussions. An example strategic planning and operational cycle and how ERM may support this is illustrated in Figure 1.1.

Figure 1.1: Strategic planning and operational cycle

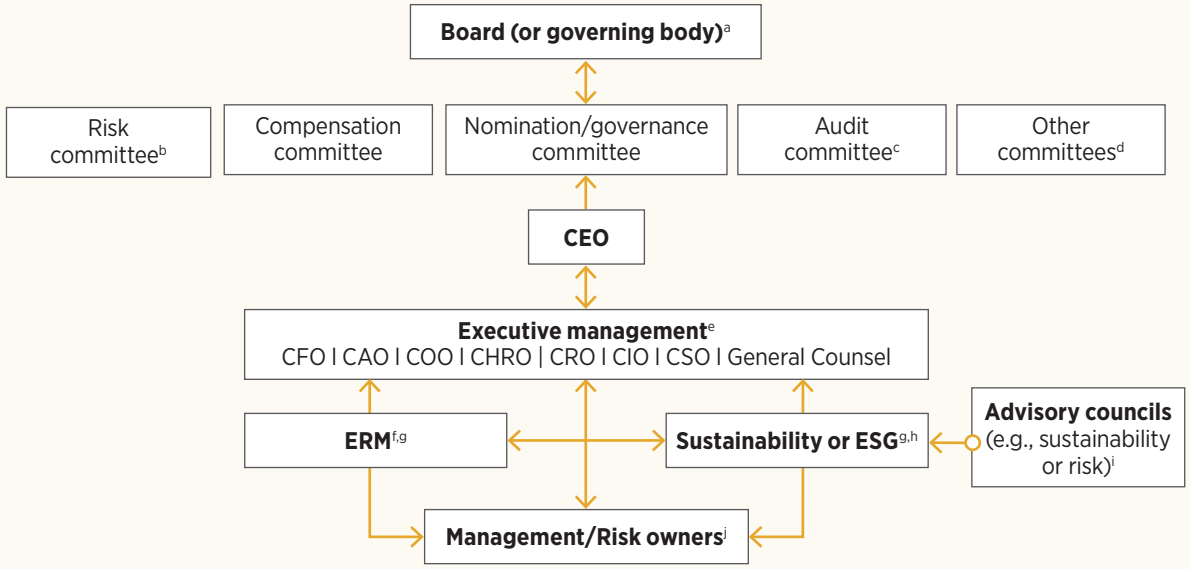


Risk management and sustainability practitioners should map their organization's operating structures, reporting lines and processes to identify areas that could strengthen ESG-ERM oversight and collaboration. In some cases, ESG-related risks may materialize unexpectedly, and the appropriate risk owners and subject-matter experts will need to be located quickly to develop an appropriate response. Figure 1.2 sets out an example governance structure and some of the key roles for risk management and sustainability.

Guidance

- ☐ 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

Figure 1.2: Example governance structure



a. The board is responsible for overseeing and, where appropriate, challenging management's approach to ESG-related risk ownership as well as ensuring there is a program in place to identify, assess, manage and monitor ESG-related risks effectively.

b. The risk committee establishes the direct oversight of enterprise risk management. The focus of the risk committee is entity-wide in non-financial areas that go beyond the authority of the audit committee and its available resources (e.g., operational, obligations, credit, market, technology).

c. The audit committee assists the board of directors in fulfilling its corporate governance and overseeing responsibilities in relation to an entity's financial reporting, internal control, risk management and internal and external audit functions.

d. Some companies have additional board committees, such as a sustainability committee, separate from the risk committee and the audit committee, comprising cross-functional representatives to identify, monitor and review ESG-related risks.

e. Connections to strategic planning and operations personnel are also critical to linking sustainability to new strategies and risk responses. These connections support timely assessment of new and emerging ESG-related risks so that the organization is better prepared to identify risks and related opportunities.

f. The ERM function or director is responsible for coordinating and consolidating ERM activities and will typically report into the CRO or other C-suite as well as lead the process for managing enterprise-wide risks in an integrated, systematic manner.

g. The sustainability director should maintain a close relationship with the ERM director.

h. The sustainability director may report to the CFO, CSO or COO and provides support in coordinating ESG-related activities. This includes monitoring megatrends as well as identifying, assessing and monitoring risks.

i. Cross-functional or multi-stakeholder advisory councils (either internal or external) can provide perspective on particular aspects of ESG issues or other risks.

j. Although management collectively 'owns' the entity risks, a 'risk owner' is frequently designated as the point person with accountability for ensuring specific risks are appropriately managed.

In the same way that ERM is not the sole responsibility of the Chief Risk Officer, management of ESG-related risk is not the responsibility of the sustainability practitioner alone. All of management should be able to articulate significant ESG-related risks that impact strategy and decision-making. Table 1.3 provides examples of risk owners for ESG-related risks, who may or may not be ESG specialists.

Table 1.3: Examples of risk owners for ESG-related risks

Enterprise-level risk	ESG element	Relevant risk owner	Supporting the risk owner
Risk of increasing raw material prices	Change in prices caused by rising energy costs associated with climate change regulation	Vice president of supply chain	Chief sustainability officer Sustainability analyst (energy)
Risk of injury or fatality in operations	Health- and safety-related considerations	Environmental health and safety manager	Site managers
Risk of reputational damage because of poor communication on ESG issues in the supply chain	Pressure for greater supply chain transparency around human rights	Chief procurement officer	Chief sustainability officer

Towards collaboration and integration

Increasing complexity from emerging trends and forces requires organizations to be more adaptable and resilient to risk. To support this, collaboration and integration on risk management across the organization can help risk management and sustainability practitioners find a common language for discussing ESG issues, create a shared responsibility for

Guidance

- ☐ Create opportunities for collaboration throughout the organization

risk ownership and develop more innovative solutions to address ESG-related risks. In a fully integrated approach, risk management and sustainability practitioners, along with other subject-matter experts, may work in formal and symbiotic partnerships, such as a cross-functional risk committee. Under this approach, all risks, whether financial, environmental, governance related, technological, social or other, are considered as part of a single process.

An emerging trend among some large corporations is to combine the risk and compliance function with the function that manages ESG issues (particularly human rights). The change comes as part of a growing recognition that protecting the organization's reputation and mitigating its risks requires a more coordinated and integrated response. Combining these functions can give a better view of the risks faced as an organization and how those risks could impact the ability to deliver on strategic priorities. Part of this emerging shift is driven by the increased focus of activists using social media to shame entities that displease them and among governments to hold companies to account for the impact their decisions have.[37]

Leveraging skills, capabilities and knowledge

Applying ERM to ESG requires a multi-disciplinary approach from experts and practitioners across the entity. In some cases, it may also require external expertise. Sustainability practitioners possess knowledge about stakeholder expectations, potential environmental and social-related risks and opportunities and how these may be best avoided or leveraged. Risk management practitioners possess knowledge and skills in risk identification, assessment and prioritization and in implementing responses and tracking effectiveness.

Guidance

- ☐ Embed ESG-related skills in hiring and talent management to promote integration

Table 1.4 highlights some of the skills, capabilities and knowledge that risk management and sustainability practitioners may possess. Transferring or sharing these skills can support ESG integration. Organizations should consider embedding these ESG risk-related skills, capabilities and knowledge in hiring and talent management.

Table 1.4: Example of skills, capabilities and knowledge that can be transferred or shared

Risk management practitioner	Sustainability practitioner
• Knowledge of the end-to-end ERM process and the timing of ERM and strategic activities • Escalation path to senior management and the board (or committees) for critical risks • Proficient in ERM frameworks, such as COSO, and in understanding the financial, operational and strategic impacts of risks • Understanding of the broader risk landscape • Capability to deploy tools or approaches used to assess financial risks (e.g., scenario planning, Monte Carlo simulation) that may be leveraged for ESG-related risks • Skills in assessing the impact in terms of profit, loss and capital allocations	• Understanding of ESG-related megatrends and how these might compound other risks or impacts • Knowledge of the widely accepted frameworks that can support an understanding of ESG issues to business and society • Technical understanding of ESG-related risks, such as detailed knowledge of the company's carbon inventory and the levers to reduce or mitigate the related risk • Leadership capability to present ESG issues and related business risks to management and the board • Knowledge of broader stakeholder landscape and their priorities on ESG issues (shareholders, customers, employees, unions, NGOs) • Understanding of current ESG initiatives in place to mitigate risk or capture value and opportunity

← Transfer or share skills, capabilities and knowledge →

Risk management, sustainability and other functions working to identify and manage risks should build a common purpose and understand how their composite skills, capabilities and knowledge can contribute to that purpose. Entities may develop education programs to share risk or ESG-related best practices across the company, such as:

- Identified risks and responses across business units
- Effective mitigation strategies
- Lessons learned
- Certification or training in ERM
- Tools and resources used for assessing risks

2. Strategy and objective-setting for ESG-related risks

Introduction

Maintaining a strong understanding of the entity's strategy, objectives and business context is critical to ERM. When identifying, assessing or managing ESG-related risks, risk management and sustainability practitioners should work to gain a holistic view of the internal and external environment, as well as how possible events and trends may impact the entity's strategy, business objectives and performance.

Global trends, such as globalization, rapid advances in technology, changes to the natural environment, demographic shifts and geopolitical influences,[1] have caused the business context for many entities to become more complex and interconnected. Entities employ specialists, such as sustainability practitioners, to monitor global megatrends and to understand how these trends translate to ESG issues for their organization. Risk management practitioners and risk owners can leverage this understanding to support a more holistic view of the entity's risk profile.



This chapter relates to the COSO ERM Framework component on Strategy and objective-setting and the four associated principles:[2]

6 **Analyzes business context:** The organization considers potential effects of business context on risk profile.

7 **Defines risk appetite:** The organization defines risk appetite in the context of creating, preserving and realizing value.

8 **Evaluates alternative strategies:** The organization evaluates alternative strategies and potential impact on risk profile.

9 **Formulates business objectives:** The organization considers risk while establishing the business objectives at various levels that align and support strategy.

This chapter outlines the following actions to help risk management and sustainability practitioners evaluate the business context while considering a broader perspective on how an entity creates, preserves and realizes value:

- ☐ 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:
  - Megatrend analysis to understand the impact of emerging issues in the external environment
  - Strengths, weaknesses, opportunities and threats (SWOT) analysis
  - Impact and dependency mapping for all types of capital
  - An ESG materiality assessment[a] to describe significant ESG issues
  - Engagement with internal and external stakeholders to understand emerging ESG trends
  - Analysis leveraging ESG-specific resources
- ☐ Throughout the risk management process, align with the entity's strategy, objectives and risk appetite
- ☐ Consider the ESG-related risks that will impact the entity's strategy or objectives

Value creation and the business model

According to the COSO ERM Framework, an entity's value is created, preserved, eroded or realized based on the relationship between the benefits derived from resources deployed and the cost of those resources.[3] The value of an entity is largely determined by the decisions that management makes – from the overall strategy to day-to-day decision-making. Effective ERM helps boards and management optimize outcomes to enhance capabilities for creating, preserving and ultimately realizing value.

Historically, this value has been measured primarily on the financial and economic factors that impact an entity's tangible assets. However, this has shifted rapidly. According to a study by Ocean Tomo,[4] between 1975 and 2015, the value of intangible assets as a proportion of total enterprise value among S&P 500 companies increased from 17% to 84%. The concept of value has also broadened to encompass shared resources between an entity and wider society. Capital is no longer a singular term; it has evolved to speak of the multiple stocks and flows of capitals, recognizing the range of resources upon which entities rely.[5]

As such, organizations may want to adopt a definition of value creation that goes beyond financial value and also considers value to a broader group of stakeholder and/or society. Acknowledging that there is no universally agreed definition of value creation, the former Technical Task Force of the International Integrated Reporting Council (IIRC) established a Technical Collaboration Group,[6] which defined ten themes that inform the meaning generally and consider a more comprehensive definition of value. These themes are described below.[b]

Ten themes that inform the meaning of value creation

1. Value creation takes place within a context
2. Financial value is relevant, but not sufficient, for assessing value creation
3. Value is created from tangible and intangible assets
4. Value is created from private and public/common resources
5. Value is created for an organization and for others
6. Value is created from the connectivity between a wide range of factors
7. Value creation manifests itself in outcomes
8. Innovation is central to value creation
9. Values play a role in how and what type of value is created
10. Measures of value creation are evolving

[a] An ESG materiality assessment is an exercise in stakeholder engagement designed to gather insight on the relative importance of specific environmental, social and governance (ESG) issues.

[b] Note that these themes are based on input from the lead participants of the Technical Collaboration Group (TCG) from a range of disciplines and countries. They reflect the collective views of TCG participants, not necessarily those of their organizations or the IIRC.

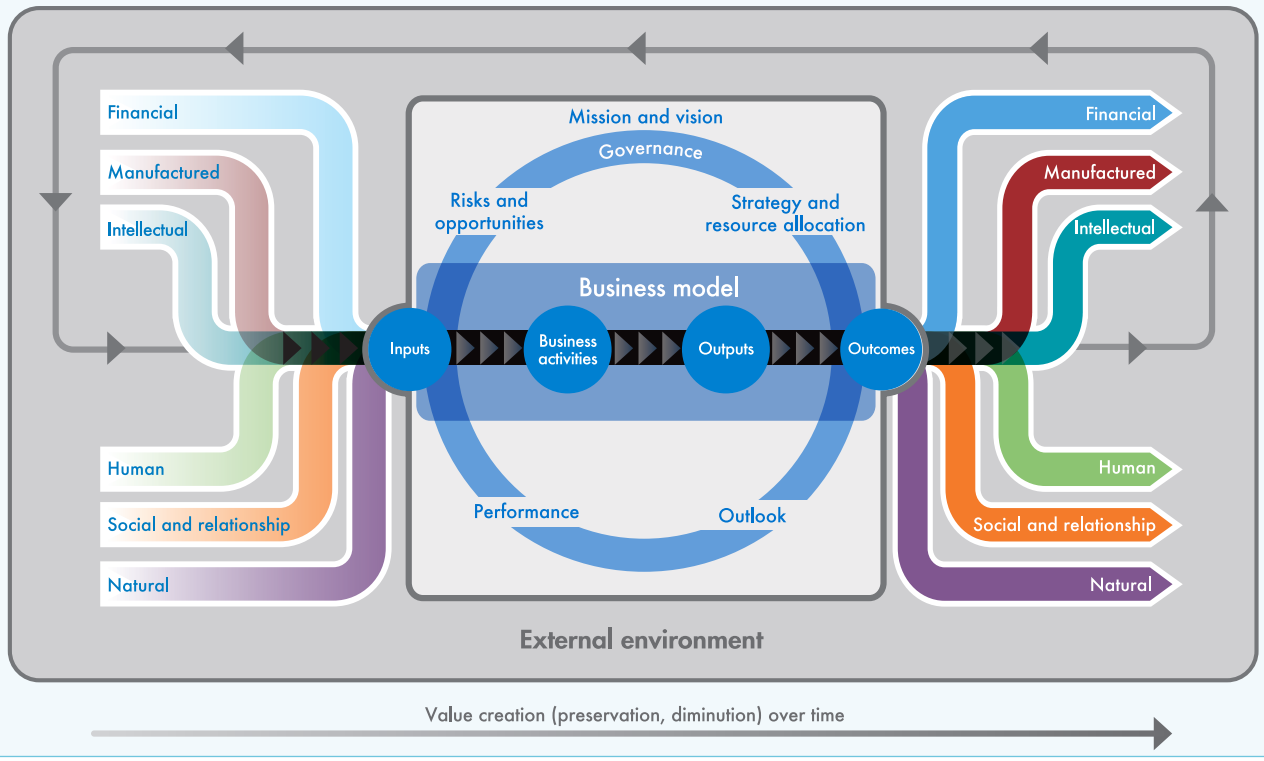
To support these considerations in practice, some organizations recommend a multi-capital approach to enhance an entity's understanding of its business model.[c] Underlying the multi-capital approach is the concept of integrated thinking,[d] which is defined by the IIRC[7] as "the active consideration by an organization of the relationships between its various operating and functional units and the capitals that the organization uses or affects." The IIRC developed the *Integrated Reporting Framework (<IR> Framework)* to provide an approach for embedding integrated thinking. Two salient features of this framework are:

Guidance

- ☐ Examine the value creation process and business model to understand impacts and dependencies on all capitals in the short, medium and long term

1) **The value creation process:** Value is created through an entity's business model, which takes inputs from the capitals and transforms them through business activities and interactions to produce outputs and outcomes that, over the short, medium and long term, create or destroy value for the organization, its stakeholders, society and the environment (see Figure 2.1).[e]

Figure 2.1: The IIRC's value creation process



2) **The capitals:** Integrated thinking recognizes the broader range of resources and relationships used and affected by the entity. Though each entity can define important physical and intangible resources that it uses or affects by using a multi-capital approach, the *<IR> Framework* defines six capitals: financial, manufactured, human, social and relationship, natural and intellectual, which are shown in Table 2.1.

[c] For example, the United Nations Inclusive Wealth Index, first launched at the Rio +20 conference, provides a way of measuring their wealth, growth, and societal progress in more inclusive and sustainable ways. The Index was created to complement GDP by introducing the impact and value of Inclusive Wealth: natural capital, human capital, and produced capital. Other examples include "King IV: Report on Corporate Governance for South Africa 2016" produced by the Institute of Directors Southern Africa, the Natural Capital Protocol from the Natural Capital Coalition and Social & Human Capital Protocol from the Social & Human Capital Coalition.

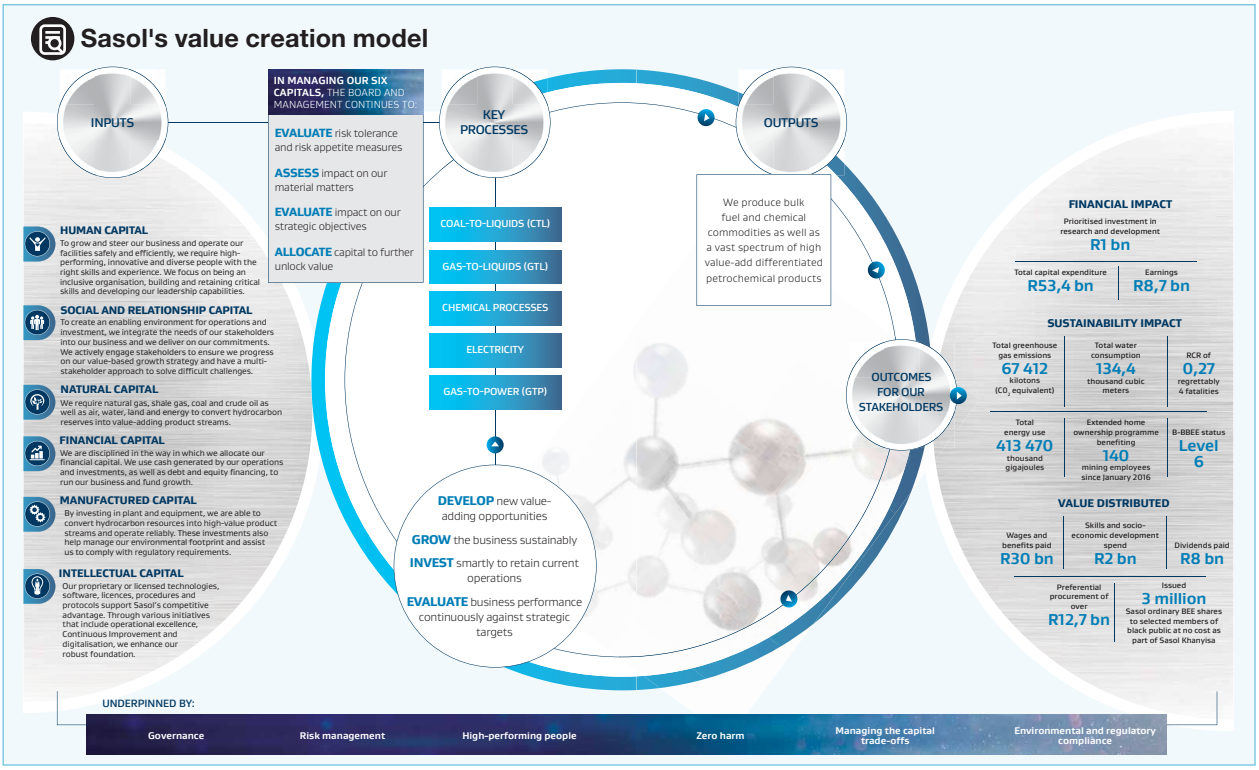
[d] For more information, refer to the *<IR> Framework* or "CGMA in Integrated Thinking: The next step in integrated reporting" and others.

[e] The *<IR> Framework* is used for illustrative purposes throughout this chapter, though other resources, such as the CGMA Business Model Framework (Retrieved from cgma.org), take a broader definition of value and help organizations articulate their business model as well as facilitate stakeholder communication.

Table 2.1: The six capitals[f]

Type	Description
Financial capital	The traditional yardstick of performance; includes funds obtained through financing or generated by means of productivity
Manufactured capital	Encompasses physical infrastructure and related technology, such as equipment and tools
Human capital	The knowledge, skills, competencies and other attributes embodied in individuals that are relevant to economic activity[g]
Social (and relationship) capital	Networks together with shared norms, values and understandings that facilitate cooperation within or among groups[h]
Natural capital	The stock of renewable and non-renewable natural resources (e.g., plants, animals, air, water, soils, minerals) that combine to yield a flow of benefits to people[i]
Intellectual capital	The skills and know-how of an organization's personnel, in addition to their commitment and motivation – which affect their ability to fulfill their roles

The diagram below depicts how Sasol Limited,[8] an integrated energy and chemical company based in the Republic of South Africa, uses the six capitals to create value.



The business context

Changes to the business context can influence an entity's vision, strategy and business objectives and its ability to create and preserve value. The COSO ERM Framework defines business context as the "trends, events, relationships and other factors that influence, clarify or change the company."[9] Principle 6 of the Framework describes the importance of understanding the potential affects of the business context on risk profile, including external factors – such as political, economic, social, technological, legal and environmental forces – and internal resources such as capital, people, processes and technology.[10] Integrating ESG issues into an organization's understanding of the business context sharpens its ability to identify and respond to risks.

[f] The definitions used in this table are adapted from the *<IR> Framework* except where otherwise noted.

[g] This is the OECD definition of human capital, which is used in the draft "Social & Human Capital Protocol" due for publication in 2019. This definition of human capital is similar to that used by the *<IR> Framework*, which is defined as "people's competencies, capabilities and experience, and their motivations to innovate."

[h] This is the OECD definition of social capital which is used in the draft "Social & Human Capital Protocol" due for publication in 2019. This definition is similar to that used by the *<IR> Framework*, which is defined as "the institutions and the relationships within and between communities, groups of stakeholders and other networks, and the ability to share information to enhance individual and collective well-being."

[i] This definition was obtained from the Natural Capital Coalition's "Natural Capital Protocol." This definition is similar to that used by the *<IR> Framework*, which is defined as "all renewable and nonrenewable environmental resources and processes that provide goods or services that support the past, current or future prosperity of an organization."

Applying a broader definition of value can serve as a starting point for understanding the complete business context in which an entity operates. A multi-capital approach brings together material considerations about an entity's strategy, governance and performance and presents them in a way that reflects the commercial, social and environmental context. Table 2.2 sets out a series of questions to support a more complete understanding of the business context, adapted from the *<IR> Framework*.

Table 2.2: ESG-related risk considerations to understand the complete business context[i]

	Content element	Questions to consider
Value creation process	**Organizational overview and external environment**	• What are the external environment aspects of the legal, commercial, social, environmental and political context that affect the entity's ability to create value in the short, medium and long term? • What do the entity's mission and vision require from an ESG perspective? • How does the ESG context link to value creation for the business more broadly? • What are the megatrends likely to impact the entity? In particular, which societal issues (e.g., demographic changes, health, poverty) or environmental challenges (e.g., climate change, resource shortages, planetary limits[k]) impact the entity? • What are the legitimate needs and interests of key stakeholders from an ESG perspective? • What are the relative ESG-related strengths, weaknesses, opportunities and threats (SWOT)? • Which shifts in the regulatory or legislative environment impact the organization?
Business model	**Inputs**	• What are the ESG issues for the capitals that the business relies on, such as ecosystem services, raw materials, natural resources, labor and water sources? • How do the stocks and flows of capitals, on which the business depends, impact the robustness and resilience of the business model?
	Business activities	• What is the value chain of the entity? • How does it differentiate itself in the marketplace? • What is the revenue-generating model? • How does the entity innovate? • How well is the entity designed to adapt to change?
	Outputs	• What are the impacts or potential impacts of the products or waste across the value chain?
	Outcomes	• What are the outcomes and contributions (e.g., employee engagement, reputation, customer satisfaction, societal acceptance, environmental impacts and license to operate)?
	Strategy and resource allocation	• How does the entity define short, medium and long term? • What are the organization's short-, medium- and long-term strategy objectives? • What are the ESG impacts and dependencies to achieving those objectives? In particular, what are the medium- to long-term risks that will impact strategy (e.g., climate change)? • To what extent have environmental and social considerations been embedded into the strategy to give it a competitive advantage? • Which ESG-related risks should be reflected in the strategy? • Which resources and capital allocations are required to implement the strategy? • How are stakeholder interests incorporated into strategy development?

To support the answers for these questions, sustainability practitioners can draw on their own experience, for example, the knowledge derived from certifying the entity in accordance with the ISO 14001 environmental management system or from participation in sustainability-focused organizations or industry collaborations. Risk management and sustainability practitioners can also use a selection of tools and resources to understand the impacts and dependencies on the entity. Some commonly used approaches include megatrend analysis, SWOT analysis, impact and dependency mapping, ESG materiality assessment, stakeholder engagement and a range of other ESG-specific resources, each explored below.

[i] See Appendix IV for more guidance on planetary boundaries.

Time horizons for considering the business context

COSO's ERM Framework recommends that the time horizon for risk management align to that used for strategy setting and business objectives.[11] However, this can be a challenge for ESG-related risks, which can take longer to materialize, resulting in an underestimation or discounting of the potential impacts of the risk. For example, the potential impacts of climate change may not threaten a company operations in the short or medium term, leading the company to disregard this as a risk as it does not represent a threat to the company's three to five year business strategy.

However, it is important to consider that value may be created in the short, medium and long term, for different stakeholders and through different capitals.[12] For example, the actions taken by entities today increase financial capital in the next quarter or year but decrease the natural capital available in 20 years. To combat the challenge of short-termism, some companies manage risks considering 3-year, 10-year and 50-year strategic time frames. This encourages them to think about significant risks that may occur in the future and how to make short-term decisions that support value realization in the medium and long term.

Incorporating future trends with megatrend analysis

Megatrends are "large, transformative global forces that define the future by having far-reaching impacts on business, economies, industries, societies and individuals."[13] Organizations can use megatrend analyses to better understand the ESG factors that may impact the business context in the future. Think tanks, governments, non-profit organizations, industry associations and consultancies prepare and publish research and analyses on global megatrends. These reports help to identify and highlight new, complex and unpredictable forces and trends that may impact business, environment and society (see examples in Table 2.3).

Guidance

- ☐ Conduct megatrend analysis to understand the impact of emerging issues in the external environment

Table 2.3: Resources for identifying emerging risks

Data sources	Description
World Economic Forum Global Risk Report	Since 2006, the annual Global Risks Report works with experts and decision makers across the world to identify the most pressing economic, societal, technological, geopolitical and environmental risks.[14]
Global Opportunity Report	Since 2015, when the UN's Sustainable Development Goals were adopted, the annual opportunity report has mapped tomorrow's sustainable markets. Each subsequent report builds upon the first, starting with the top five goals in the 2015 report and expanding to describe new market opportunities.[15]
Industry associations	Several industry associations produce reports on the megatrends that specifically impact an industry or sector. Examples include the Conning US and Global Insurance Industry Outlook[16] and the Biotechnology Innovation Organization Industry Analyses.[17]
Megatrends reports from consulting firms	Reports produced by consultancies such as Accenture,[18] Deloitte,[19] EY,[20] KPMG,[21] McKinsey[22] and PwC[23] on an annual basis describe the top megatrends and an outlook on the future. They also offer specialized reports that are industry specific, such as for mining and metals.[24] ESG-specific megatrends reports may also be helpful to identify the most critical ESG trends organizations may face now and in the near future.[k]
Political reports	National economy planning agencies typically issue reports describing government plans for the future. For example, the National Economic and Social Development Board of Thailand publishes a five-year government strategy plan.[25]
ESG-focused organizations and conferences	Global ESG-focused consortiums of businesses, NGOs and alliances provide insights into trends, leading practices and groups such as WBCSD, Sustainable Brands, Ceres, GreenBiz, CSR Asia, European Sustainable Development Network and the UN, including the UN Global Compact, the UN Development Programme, the UN Environment Programme (UNEP) and the UNEP Finance Initiative.[l]
Insurance company reports	Several insurance companies annually publish reports detailing the top business risks. For example, the 2018 Allianz Risk Barometer identifies the top ten global business risks based on insight from over 1,900 risk management experts from 80 countries.[26]

As demonstrated in Table 2.4, megatrend analysis can help organizations gain an understanding of significant global risks, some of which are often ESG-related (e.g., climate change and increasing volatility of weather or health and safety incidents).

[k] For example, refer to CPA Australia, KPMG Australia and GRI Focal Point Australia (2014). "From Tactical to Strategic: How Australian businesses create value from sustainability." GRI Focal Point Australia, Sydney.

[l] For example, WBCSD's "Societal megatrends and business – operating, innovating and growing in a turbulent world" identifies the key societal areas that they believe can materially affect companies' ability to operate, innovate and grow.

Table 2.4: Top ten global business risks for 2018

Megatrend	Description
Business interruption	Supply chain disruption, factory fires, destroyed shipping containers, cyber incidents
Cyber incidents	New threats such as "cyber hurricanes" and tougher data regulation; a single cyber attack can potentially impact hundreds of companies
Natural catastrophes	Numerous natural catastrophes in 2017 could indicate increases in the future due to the impact of a changing climate
Market developments	Waves of M&A activity, digital revolution, political uncertainty
Changes in legislation	Changes in global trade agreements, uneven monetary and regulatory conditions between regions
Fire/explosion	Physical damage and business disruption result in losses from fire and explosions
New technologies	Technological advances, digitalization, interconnectivity and information exchange
Loss of reputation/brand value	Health and safety incidents, product recalls and data security breaches – exacerbated by social media and interconnected supply chain
Political risks and violence	Terrorism, threats to transportation infrastructure and locations with large groups of people, increased political activism
Climate change/increasing volatility of weather	Increasing frequency and severity of weather events

Adapted from 2018 Allianz Risk Barometer

Using megatrend analysis as a starting point for ESG analysis in the business content

CLP Holdings Limited's (CLP) Senior Director of Group Financial Planning and Control and Director of Group Sustainability piloted an approach to update its annual ERM process to better capture longer-term risks, including ESG-related risks.

The first step was to identify the global risks and trends affecting CLP. Various groups collaborated to draw on the Risk Management Group's experience analyzing economic megatrends and the Sustainability Group's experience analyzing longer-term environmental and social megatrends.

The combined group developed criteria to select appropriate information sources, such as consultancies and global organizations. Using these sources, they narrowed the list of megatrends to the top five impacting the industry and company.

Next, they analyzed these megatrends, as well as any possible "microtrends" underlying them, for general implications for the industry and CLP.

SWOT analysis

A SWOT analysis uses a two-by-two matrix to define the strengths, weaknesses, opportunities and threats an entity is facing. A SWOT considers both internal and external factors, so is a commonly used by organizations as a strategic planning tool.

The World Resources Institute (WRI)[27] has developed a sustainability-specific SWOT tool focused on understanding the SWOT from an ESG perspective (i.e., impacts, dependencies and related megatrends). The example shown in Table 2.5 relates to a hypothetical consumer products company.

Guidance

- ☐ Conduct strengths, weaknesses, opportunities and threats (SWOT) analysis

Table 2.5: SWOT analysis example

	Helpful	Harmful
Internal origin	**Strengths** What are unexpected ways the company can apply its strengths to ESG challenges? Example: The company begins measuring water use and promoting efforts to reduce water consumption.	**Weaknesses** Do any peers experience similar weaknesses or face similar risks from ESG challenges? Example: The company is focused on its main competitive advantage for a single, water-intensive product.
External origin	**Opportunities** Where is there a growing gap in which the company and others can create new solutions to ESG challenges? Example: New technologies reduce the amount of water required in manufacturing.	**Threats** Where are ESG challenges creating broad threats to future business value? Example: Some locations are experiencing water scarcity and drought.

Questions adapted from WRI's SWOT user guide

Impact and dependency mapping

In the *<IR> Framework*, impacts and dependencies are described in terms of the stock and flow of capitals in the value creation model. Impacts and dependencies should be considered using a multi-capital approach, as relevant to the organization.

Guidance

- ☐ Conduct impact and dependency mapping for all types of capital

The *Natural Capital Protocol*[28] and *Social & Human Capital Protocol*[29] provide guidance for companies to capture the complexity of impacts and dependencies on natural, social and human capitals through impact and dependency pathways. An impact pathway describes how, as a result of business activity, a particular impact driver results in changes in natural capital (or other capital) and how these changes impact different stakeholders. A dependency pathway shows how a particular business activity depends on specific features of natural and/or human and social capital (or other capital).[30] Table 2.6 defines and provides examples of ESG-related impacts and dependencies.

Table 2.6: Examples of impacts and dependencies

Flows	Application to social or natural capital
Impacts	The negative or positive effect of business activity on financial, social and relationship, human and natural capital. Some examples include an organization's contribution to air pollution, job creation or safe working conditions.
Dependencies	Resources (e.g., human, social, natural) that businesses need in order to create and sustain value. For example, a company relies on available freshwater supplies, dams for flood control or employees and suppliers that follow the entity's code of conduct.

Examples	Impact or dependency	Value creation or loss
Apparel companies use third-party manufacturers in low-cost countries (e.g., Bangladesh, China, and Vietnam).	Employees working for apparel manufacturers in Bangladesh are **impacted** by the standard of the buildings leased or owned by those companies.	The Rana Plaza factory in Bangladesh collapsed because health and safety standards were not enforced. The UN-backed scheme to support families raised less than half of target compensation for families.[31] Apparel companies have worked to improve working conditions in factories because of reputational damage.[32]
Coca-Cola opened a bottling plant in a water-scarce region of India in 1993.	Beverage manufacturing **depends** on water availability in the country of operations.	The local watershed could not support both community water requirements and Coca-Cola's manufacturing process. Local authorities closed Coca-Cola's plant.[33]
Freeport McMoRan was accused by its union of improperly firing furloughed workers in 2017.[34]	Copper mining **depends** on a stable workforce; 3,000 full-time and 1,000 contract employees who were absent and had "voluntarily resigned" were **impacted**.	The treatment of employees resulted in a loss of trust with local community and globally. The company then incurred time and expense to draft a company statement and open an Employee Return to Work center.[35]
Wells Fargo & Company opened financial accounts without its customers' consent.	Customers were **impacted** when the company created millions of accounts in their name without consent, likely impacting credit scores among other concerns.[36] Wells Fargo is impacted by the limits on growth, fines, penalties, settlements and effects on its reputation.	The bank paid USD$185 million in fines plus another USD$5 million in customer remediation to the Consumer Financial Protection Bureau.[37] The bank paid USD$110 million in settlement to customers.[38]

Leveraging the entity's ESG materiality assessment

Each entity faces a unique set of ESG issues, depending on the industry, size of the entity, selected strategy and business objectives, stakeholders and more. Entities often use a materiality assessment (or ESG materiality assessment), to gather insight on the relative importance of specific environmental, social and governance (ESG) issues. Sustainability practitioners should share these results with risk management practitioners to support a broader understanding of the internal and external business context.

Guidance

- ☐ Conduct an ESG materiality assessment to describe significant ESG issues

In 2018, the WBCSD reported that 89% of its member companies[m] disclose that they perform a materiality assessment process to identify the ESG issues relevant to business and stakeholder interests.[39] The process typically involves a combination of peer benchmarking, megatrends analysis and engagement with internal and external stakeholders. Table 2.7 outlines a selection of frameworks, guidance and standards to support ESG materiality assessments.

[m] WBCSD's member companies comprise over 200 leading businesses working together to accelerate the transition to a more sustainable world. They represent a combined revenue of more than USD$8.5 trillion and with 19 million employees.

Table 2.7: Resources for performing ESG materiality assessment

Framework, guidance and standards	Description
AccountAbility Five-Part Materiality Test	Designed to help organizations identify: • What issues are most material, or relevant, to their business and its stakeholders. • What information should be disclosed or reported in sustainability and corporate social responsibility reports.[40]
Ceres Roadmap for Sustainability 2010	Resource to help companies re-engineer themselves for success in a world beset with unprecedented environmental and social challenges that threaten the economy and local communities; designed to guide companies toward corporate sustainability leadership and ultimately support an accelerated transition toward a more sustainable global economy.[41]
Environmental and social impact assessments	Completed separately or together, these assessments are designed to identify and quantify the environmental or social impact from business activities or projects; impacts are measured against a baseline by identifying and assessing the drivers for impacts – both independent and related.[42]
Global Reporting Initiative Standards (GRI)	General and industry-specific guidelines for reporting a full range of economic and ESG impacts of operations.[43]
Human rights due diligence	Human rights due diligence described by the UN Guiding Principles Reporting Framework is "an ongoing risk management process…to identify, prevent, mitigate and account for how [to address] adverse human rights impacts." It includes four key steps: assessing actual and potential human rights impacts, integrating and acting on the findings, tracking responses and communicating about how impacts are addressed.[44]
Integrated Reporting <IR> Framework	Framework for the preparation of an integrated report that explains to providers of financial capital how an organization creates value over time. It provides a process for identifying risks based on the legal, commercial, social, environmental and political contexts that affect the entity's ability to create value in the short, medium and long term.[45]
Sustainability Accounting Standards Board (SASB) Standards	Investor-focused standards on suggested material issues by industry and category: environment, social capital, human capital, business model and innovation and leadership and governance. SASB's five-factor test enables an organization to systematically consider each topic and draw insights regarding topics that are reasonably likely to have material impacts.[46]

The concept of materiality

Much like the term ESG, there is no universally accepted definition of materiality, though the term is used pervasively. In the context of financial or legal filings in the US, information is material if there is "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."[n] This definition has been adopted by SASB[o] to identify sustainability topics that are reasonably likely to be material for a specific industry. SASB recommends that a company's management consider these "material" topics to determine whether the relevant SASB standard should be used to comply with the disclosure requirements of the federal securities laws.[47]

Conversely, some ESG practitioners and organizations guide entities to take into account the perspectives beyond those concerned with financial capital in defining materiality. For example, GRI defines "material aspects as those that reflect the organization's significant economic, environmental and social impacts; or that substantively influence the assessments and decisions of stakeholders."[48] GRI, therefore, recommends highlighting the importance of considering issues that are not yet financially material.[p] Similarly, the IIRC defines a matter as material "if it could substantively affect the organization's ability to create value in the short, medium or long term."

This distinction is important to help risk management, sustainability and other practitioners to communicate in a common language when leveraging an organization's ESG materiality assessment to understand an organization's ESG issues.

[n] The Financial Accounting Standards Board (FASB), the US Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB) and American Institute of Certified Public Accountants (AICPA) define materiality as "the magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement" (Financial Accounting Standards Board (2008). "Original Pronouncements as Amended: Statement of Financial Accounting Concepts No. 2."

[o] SASB applies the US Supreme Court definition, suggesting that information is material if there is "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" (TSC Indus. v. Northway, Inc., 426 U.S. 438, 449 (1976)).

[p] For further information, the differences in the concept of materiality offered by various organizations has been covered to a larger extent in the March 2016 publication "Statement of Common Principles of Materiality of the Corporate Reporting Dialogue."

Stakeholder engagement

Different stakeholders may have different perceptions of value and different expectations of an entity's roles and obligations. Within sustainability, the concept of stakeholder engagement refers to the process used by an organization to engage relevant stakeholders for the purpose of achieving agreed outcomes. The process can be used to help all parties better understand the business context, including issues or risks that may otherwise be overlooked by risk management practitioners, sustainability practitioners and the business. It provides outside perspectives of events and enables entities to question and challenge assumptions.

Guidance

- ☐ Conduct engagement with internal and external stakeholders to understand emerging ESG trends

Stakeholder engagement can also:

- Offer perspectives on the issues or impacts of greatest concern
- Inform the relative importance of issues and impacts
- Provide data, information and expertise on a particular issues or trend
- Inform, validate and add credibility to the prioritization process and results

Many large organizations collect stakeholder input as a matter of regular operations. Risk management practitioners can review stakeholder feedback periodically and leverage this information to:

- Explore how stakeholder feedback highlights issues that could pose threats to achieving an organization's strategy and objectives
- Confirm existing risks and identify new or emerging risks
- Identify what additional stakeholder engagement would benefit ERM activities, including engaging stakeholder groups omitted from existing efforts or engaging stakeholders in discussions

> "Stakeholders are defined as those individuals, groups of individuals or organizations who affect and/or could be affected by an organization's activities, products or services."[49]

Entities usually define their own stakeholder groups; however, these typically include customers, communities, suppliers, shareholders, employees, government, unions, investors, media and non-profit organizations. Companies can use the AA1000 Stakeholder Engagement Standard (2015) to assess, design, implement and communicate an approach to stakeholder engagement. The following example demonstrates one way entities can use existing feedback processes to identify ESG-related risks.

Other ESG-specific resources

Risk management and sustainability practitioners can also leverage a variety of ESG-specific resources to enhance their understanding of ESG-related impacts and dependencies. For example, leveraging the Greenhouse Gas Protocol can help an entity calculate its carbon footprint and, in doing so, better understand the entity's exposure to climate-related risk. Table 2.8 includes a list of open-source tools or resources that organizations can use to better understand specific ESG issues in the business context.

Guidance

- ☐ Conduct analysis leveraging ESG-specific resources

Table 2.8: ESG-specific resources or tools for understanding the business context

Resources	Application
CEO Water Mandate	Aims to mobilize businesses to advance water stewardship and sanitation practices by creating a forum for corporate water discussions and access to water stewardship resources that cover areas such as operation, context, strategy, engagement and communication[50]
CDP	Runs a global disclosure platform that enables companies to measure, manage and self-report on their environmental impacts; offers specific disclosure platforms for climate, water and forest impacts with companies completing and submitting the CDP questionnaires on an annual basis[51]
Context-Based Sustainability	Uses metrics to help companies assess their impacts on vital capitals in relation to what they would need to be in order to be sustainable, taking into account factors such as the needs of stakeholders, the sufficiency of these capitals and competing uses of these capitals[52]
Embedding Project's "The Road to Context: Contextualizing your Strategy and Goals: A Guide"	Provides an understanding of how to factor social and ecological limits into corporate strategy and goal-setting processes as well as helping make sense of the different frameworks and tools designed to aid this process[q,53]
The Equator Principles	Provides a risk management framework, adopted by financial institutions, for determining, assessing and managing environmental and social risk in development projects; it is primarily intended to provide a minimum standard for due diligence and monitoring to support responsible risk decision-making[54]
Greenhouse Gas Protocol	Provides a framework and assessment tool for companies measuring their carbon footprint in terms of scopes 1, 2 and 3 greenhouse gas emissions[r,55]
The Future-Fit Business Benchmark	Offers a set of indicators for supporting companies in determining the gap between their current performance and where their performance needs to be in relation to key threshold(s)[56]
Human rights impact assessment (HRIA)	Provides guidelines, in-practice examples, HRIA levels and steps for understanding human rights-based risks and opportunities[57]
Life Cycle Analysis	Offers an approach to support a systems-based identification of the socio-ecological impacts of products and processes; the assessments typically account for all the inputs and outputs throughout the life cycle of a product (design, raw material extraction, production, use and disposal or reuse)[58]
MultiCapital Scorecard	Seeks to support the development of a contextual approach to sustainability reporting that measures an organization's impacts on vital capitals relative to organization-specific norms or standards for what they should be in order to be sustainable[59]
Net Positive	Aims to support companies in achieving net gains with respect to a threshold stemming from their business activities[60]
Natural Capital Protocol Toolkit and Social Capital & Human Protocol Toolkit	Offers a variety of tools ranging from frameworks to measurement approaches to help companies understand and then assess impacts and dependencies of natural[61] and social capital[62]
Planetary Boundaries	Identifies nine tightly coupled processes that regulate the stability and resilience of the Earth's economical system boundaries and, for each of these systems, attempts to quantify the boundaries at which human survival is threatened[63] (for more information, see Appendix IV)
The Alliance for Water Stewardship	Provides a globally recognized standard and framework that enable water users to correctly select appropriate catchment boundaries and understand their use of water and their impact on water within a catchment context; the standard encourages users to expand their collaboration and be more transparent in their disclosure[64]
The Doughnut of Planetary Boundaries and Social Foundations	Together with the Planetary Boundaries framework, helps to introduce the role companies play in maintaining and enhancing social resilience or, conversely, how their actions contribute to social instability in the regions where they operate[65] (for more information, see Appendix IV)
The Living Planet Index	Aims to measure the state of the world's biological diversity and uses the trends in the populations of vertebrates living in terrestrial, freshwater, and marine habitats; its database holds time-series data for over 18,000 populations that are aggregated to produce indices of the state of biodiversity[66]
WRI Aqueduct	Helps map water risks and opportunities emerging worldwide[67]

Alignment to strategy and business objectives

The COSO ERM Framework emphasizes the importance of integrating ERM with strategy and objective-setting to provide an organization with insight into the risk profile associated with its strategy and business objectives.[68] Doing so guides the organization and helps sharpen the strategy and the activities necessary to carry it out.

Guidance

- ☐ Throughout the risk management process, align with the entity's strategy, objectives and risk appetite

[q] Some of the resources referenced in this report are provided in this table or Appendix III. This guide also provides further resources not included here.

[r] In accordance with the Greenhouse Gas Protocol, scope 1 refers to direct GHG emissions occurring from sources that are owned or controlled by the company, scope 2 accounts for GHG emissions from the generation of purchased electricity consumed by the company and scope 3 allows for the treatment of all other indirect emissions.

The COSO ERM Framework defines strategy as the organization's plan to achieve its mission and vision and to apply its core values.[69]

To effectively manage ESG-related risks, it is critical to understand the strategic and operating plans of the business. Risk management and sustainability practitioners should not attempt to identify, assess or respond to ESG-related risks in isolation from the entity's strategic direction, business objectives or risk appetite. For example, the risk of bribery and corruption impacting the operations of a business unit will be very relevant to an entity with a growth strategy into emerging markets (such as South America and Africa) as compared with a European-based organization.

Pro Paper & Packaging

See Appendix VIII for illustrative example of aligning risks to the strategy and business objectives.

Risk appetite

The COSO ERM Framework defines risk appetite as the types and amount of risk, on a broad level, that an entity is willing to accept or reject in pursuit of value.[70] Tolerance is defined as the boundaries of acceptable variation in performance related to achieving business objectives.[71] Once set, risk appetite and tolerance become the boundaries for acceptable decision-making. Boards and management typically set the risk appetite for the entity when considering strategy and business context, as the two are often intertwined. Table 2.9 illustrates one approach to setting risk appetite.

Entities with effective ERM practices contemplate risk appetite in decision-marking. If an organization has an aggressive growth strategy, it may be willing to accept more risk in general. In contrast, an entity in a mature industry may be risk averse generally but willing to accept more risk in certain strategic areas.

Table 2.9: Example risk appetite application

Approach to setting risk appetite
• Risk appetite is: - Defined at a high level (top down) - Based on the entity's core values and strategic ambition - Rooted in the business context • Risk appetite considers the types of risks (strategic, operational, financial, compliance) the entity needs to take, or avoid, in order to achieve its strategic ambition. • The organization typically is willing to take on a net total amount of risk, which can be allocated to each category of risk to align with the organization's core values and strategy. • Risk capacity is the maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives. It considers liquidity, stakeholder relationships, capabilities and other factors. • Risk capacity provides a set of boundaries for defining meaningful risk appetite and tolerance.

Consideration of the organization's risk appetite is instrumental when prioritizing risks and selecting risk responses. It supports thoughtful deployment of resources and inhibits development of objectives that would exceed the risk appetite. Risk management practitioners compare the severity of a potential risk against their risk appetite. If the severity is within their appetite, then entities typically accept or pursue the risk. If the severity is greater than the appetite, then they avoid, reduce or share the risk (see sub-chapter 3c).

Risk management and sustainability practitioners should consider risk appetite throughout the ERM process. Some example questions include:

- What ESG-related risks are necessary and acceptable for achieving strategic ambitions?
- What ESG-related risks should the entity avoid?
- What levels of ESG-related risks are acceptable?
- How do current investments, operations and commitments compare to the entity's risk appetite?
- Do incentives and performance targets align with the entity's risk appetite?

Risk appetite in action

The Gold Coast Waterways Authority (GCWA)[72] developed a risk appetite statement that covers the critical risk categories (e.g., strategic, operations, environmental, community and resilience) within its risk register. Some examples of the GCWA's risk appetite statements relating to ESG-related risk include:

Environmental

- A very low risk appetite for activities or events with significant environmental impacts
- A very high risk appetite for activities that have net environmental benefits

Community

- A low risk appetite for activities that present safety risk to people using waterways
- A very low risk appetite for activities that amplify the risks associated with peak visitor times
- A very low risk appetite for unauthorized activities
- A very low risk appetite for behaviors that compromise the safety of other waterways users, the environment, infrastructure and property

Evaluating alternative strategies and formulating business objectives

As part of strategy and objective-setting, organizations typically evaluate different strategic alternatives. In doing so, they assess the risks and opportunities of each option, which may include:

- Evaluating the possibility that the strategy does not align with the mission, vision and core values of the entity. For example, consider a pharmaceutical company that is evaluating the strategy of significantly increasing the price of drugs for which competitors have left the market. This may be at odds with its mission of providing affordable health care to patients.
- Evaluating the implications from the chosen strategy. For example, in 1999, Skanska (a Swedish construction and materials company) acquired an Argentinian company and began operating in South America. The company soon learned the implications of applying what would be considered a routine business ethics policy in Europe or North America to such a diverse range of operations, in a region often characterized by unlawful employment practices.[73]
- Evaluating whether a potential business objective can be achieved given the risk appetite or resources available to the entity. For example, before setting a target to procure 100% certified or organic raw materials, a company needs to assess the availability of organic product and potential risks to that availability.

Guidance

☐ Consider the ESG-related risks that will impact the entity's strategy or objectives

Making changes to strategy

Typically, organizations hold periodic strategy-setting sessions to outline both short-term and long-term strategies. According to the COSO ERM Framework, a change in strategy may be warranted if:

- The organization determines that the current strategy fails to create, preserve or realize value
- A change in business context causes the entity to get too near the boundary of risk it is willing to accept
- Resources and capabilities are required that are not available to the organization
- Developments in business context results in the organization no longer having a reasonable expectation that it can achieve the strategy[74]

In some cases, substantial changes to the internal or external business context may lead an organization to reconsider its business strategy or objectives. For example, in 2017, French food-company Danone responded to shifting consumer preferences for healthier choices by developing a "One Planet, One Health" vision with a strategy that focuses on brands that encourage healthier, more sustainable eating and drinking habits.[75] In 1994, the founder of Interface recognized the need to take a more proactive stance on environmental compliance, thereafter shifting the company from a petroleum-intensive carpet business to focus on a strategy that included taking back and recycling used carpet, designing new products from recycled materials, developing nontoxic adhesives and textiles, harnessing nature's designs for products and experimenting with leasing "flooring services" as an alternative to selling carpet.[76]

The approaches outlined in this chapter can be helpful for risk management and sustainability practitioners to understand the potential ESG-related risks and impacts when evaluating alternative strategies or formulating objectives. Practitioners may also consider impacts beyond those of their own operations to look at their business within context the social and environmental systems that surround them. Guidance developed by the Embedding Project[77] encourages entities to consider *context* when setting sustainability strategies and objectives using four iterative steps:

- Understand key socio economic issues and their associated thresholds (the level at which resiliency becomes threatened)
- Understand where the company has the greatest impact on these thresholds
- Determine the magnitude of change required to operate within these thresholds
- Commit to the allocation of the change that is required

Applying context to sustainability plan and goals at Mars Incorporated (Mars)

Mars considers the impact its business has on the environment and society in its decision-making, and recognizes that this approach also lowers operational and reputation risk. Mars worked with key stakeholders and the Planetary Boundaries Framework to prioritize five socio-ecological issues across its full value chain. From each of these five broad impact areas, Mars has articulated long-term targets for GHG emissions, water, water quality, wages and human rights, and how it plans to track progress using scientifically credible metrics.[78]

Additional guidance on setting ESG-related context-based goals is provided in sub-chapter 3c.

3. Performance for ESG-related risks

Performance focuses on practices that support the organization to make decisions in the pursuit of its strategy and objectives. This chapter relates to the COSO ERM Framework component on Performance and the five associated principles:[1]

10 **Identifies risk:** The organization identifies risk that impacts the performance of strategy and business objectives.

11 **Assesses severity of risk:** The organization assesses the severity of risk.

12 **Prioritizes risks:** The organization prioritizes risks as a basis for selecting responses to risks.

13 **Implements risk responses:** The organization identifies and selects risk responses.

14 **Develops portfolio view:** The organization develops and evaluates a portfolio view of risk.

These principles cover the areas over which sustainability practitioners often need the most guidance – effectively quantifying ESG-related risks in a common language and developing innovative responses in the face of challenges presented by an evolving risk landscape.[a]

This chapter is divided into three sub-chapters:

3a. Identifies risk: Using the understanding of strategy and context from Chapter 2, management identifies the risks or events that impact performance of strategy and business objectives (COSO Principle 10).

3b. Assesses and prioritizes risks: For each risk or event, management identifies the possible outcomes based on the understanding of the business context and strategy to feed into the assessment and prioritization of the risks (COSO Principles 11 and 12).

3c. Implements risk responses: From this assessment, management determines which of those events and outcomes are a priority to manage and how to respond (COSO Principles 13 and 14).

This chapter also discusses the role of organizational biases in identifying, prioritizing and responding to ESG-related risks (see sub-chapter 3b).



[a] In a survey of risk professionals, more than 65% indicated their company did not use any scientific methods to quantify and evaluate sustainability issues. An additional 23% did not know whether or not quantification methods were used. Similarly, in a survey of sustainability professionals, approximately 70% indicated their organizations did not have a process for quantifying sustainability risks. Professionals indicated they required help to develop and improve such processes. (According to surveys of approximately 70 sustainability and risk professionals at the WBCSD Liaison Delegate Meeting in April 2017 and the Institute of Internal Auditors General Audit Management (GAM) Conference in March 2017.)

3a. Identifies risk

Introduction

Risks are present in all business activities. They often come into focus due to changes in business strategy, objectives, context or risk appetite. Chapter 2 describes how entities can better understand ESG-related shifts, impacts and dependencies that may affect a business's ability to achieve its strategy or objectives. Management can leverage the outcomes from these activities to gain a more complete understanding of their entity's ESG-related risks.



This sub-chapter relates to the following COSO ERM Framework principle:[1]

10 **Identifies risk:** The organization identifies risk that impacts the performance of strategy and business objectives.

It is important to remember that not all ESG issues present an enterprise-level risk. Managers need to translate external trends and drivers into identified risks and assess the impact and severity on the organization. Although many entities have processes in place to do this, ESG-related risks can be more challenging to identify because they are often:

- New or emerging and may unexpectedly threaten an organization's ability to achieve its strategy and business objectives
- Not well known to the business and include "black swans" or other unforeseen events that can challenge the entity's short-term or long-term performance or even survival
- Longer term, going beyond the timeline with which strategy is set or risks have been considered historically
- Difficult to quantify and communicate in the context of business language and objectives
- Beyond the scope of one entity and therefore require response at industry or government levels

This sub-chapter outlines the following actions to help risk management and sustainability practitioners identify and define new and existing ESG-related risks:

- ☐ Examine the entity's risk inventory to determine which ESG-related risks have or have not been identified
- ☐ Involve ESG risk owners and sustainability practitioners in the risk identification process to leverage subject-matter expertise
- ☐ Convene meetings with both risk management and sustainability practitioners to understand ESG-related risks
- ☐ Identify the ESG-related risks that may impact the organization's strategic and operational plans
- ☐ Define the impact of ESG-related risks on the organization precisely
- ☐ Use root cause analysis to understand drivers of the risk

Using a risk inventory

According to the COSO ERM Framework, the objective of risk identification is to determine the risks that could interrupt operations, affect the reasonable expectation of achieving the entity's strategy and business objectives or materially impact the entity's license to operate (including reputational issues).[2] Identifying opportunities should be a key part of the risk identification process. COSO defines opportunities as the actions or potential actions that create or alter goals or approaches for creating, preserving and realizing value.[3]

Many entities maintain a risk inventory or register to list the risks that they face. This inventory provides common categories and standard definitions through which risks can be described and discussed. A risk inventory may also include a description of the impact of each risk, mitigation actions and a risk owner.[4]

When ESG-related risks meet the entity's risk criteria, these risks should be included in the risk inventory, so they can be managed and monitored. See Table 3a.1 for an example risk inventory.

Table 3a.1: Example risk inventory

Strategic	Operational	Financial	Compliance
• Vision and core values • Corporate governance • Organizational structure • Strategic planning • Mergers and acquisitions valuation and pricing • Investor relations • Competition • Changing customer preferences or lifestyles • Growing middle class • Urbanization/growing population • Emerging markets	• Research and development • New products • Marketing • Budgeting and forecasting • Raw material availability • Suppliers • Production management • Product stewardship • Inventory management • Employee engagement • Labor relations • Human rights • IT investment • Cybersecurity • Business continuity • Pandemic • Physical impacts of climate change	• Interest rate volatility • Foreign currency volatility • Cash management • Credit risk • Accounting policies • Accounting estimates • Internal control • Tax strategy and planning	• Fraud • Bribery • Conflicts of interest • Country/state/local regulation • Tax regulation • Trade regulation • IP management and protection • Greenhouse gas emissions • Water treatment • Health and safety

Typical categories of risk include strategic, operational, financial and compliance. Some organizations may include a separate category for "sustainability" or "reputational" risks. However, these risks can usually be grouped in other risk categories (for example, climate-related risks are often operational or financial in nature). Further, reputational implications are often an *impact* from another type of risk, rather than a risk in and of itself (for example, reputational damage resulting from an environmental incident or pollution). In addition, many ESG-related risks are not entirely new but rather represent an additional source to an existing risk or compound the risk's impact or likelihood of materializing. For example, climate change impacts often increase the risk of raw materials cost fluctuations, which is an existing risk for many entities (see Table 3a.2).

Guidance

- ☐ Examine the entity's risk inventory to determine which ESG-related risks have or have not been identified

Table 3a.2: Example ESG-related risks or opportunities

Type	ESG-related risk or opportunity	Environmental	Social	Governance
Strategic	• Shifting **customer preferences** toward products that are manufactured with ethical supply chains		■	
	• Growing **investor interest** in ESG issues, resulting in proxy voting against the company on a range of topics (e.g., diversity, deforestation and human rights)	■	■	■
Operational	• Increased cost of **raw materials** due to sustainable forestry practice requirements	■		
	• **Reduction of waste** and **raw material** costs through improved manufacturing processes	■		
	• Changing weather patterns and increased natural disasters disturbing operations and **business continuity**	■		
Financial	• Reputation impacts and societal concerns due to a **tax avoidance strategy** and **lack of tax transparency**		■	■
	• **Investment in local content** to generate sustained and inclusive growth through economic diversification and employment opportunities		■	
	• Increased **taxation** from carbon tax regulation	■		
Compliance	• Enhanced **reporting requirements** for greenhouse gas emissions and energy usage	■		
	• Inaccurate or fraudulent **disclosure of emissions** resulting in fines and penalties and loss of consumer trust	■		■

In many cases, an ESG-related risk impacts several or all of these categories. For example, human rights-related risks are predominantly operational; however, some jurisdictions have compliance requirements relating to human rights in the supply chain.

State Street identifies emerging risks

State Street Global Advisors (SSGA) is one of the world's largest asset managers.[a] Recently its sales function identified a new risk and opportunity: gender diversity. Management identified related megatrends and early studies showing that companies with higher rates of female participation at the senior management level benefit from return on equity, reduced volatility and fewer governance-related issues. SSGA implemented a three-pronged approach to address this risk and opportunity. Employees in operations, leadership and corporate governance started the Fearless Girl campaign, modified the Asset Stewardship Program and launched a gender diversity index. Identifying this risk and implementing a response have helped increase awareness of gender diversity's impact on company performance, attract clients who want to promote gender diversity and promote the long-term value for clients' investments.[b]

Approaches to identifying risks

Many entities have an ERM process in place to identify risks that impact the business strategy and include them in the risk inventory. This process may include surveys, workshops and interviews with risk owners and executives to confirm existing risks or understand new or emerging risks.[5] For entities with enhanced ERM processes, this may also include quantitative and in-depth analytical approaches.

In addition, entities have ongoing activities and processes performed by the sustainability function, corporate strategy function or risk owners that can support the identification of ESG-related risks.

Guidance

☐ Involve ESG risk owners and sustainability practitioners in the risk identification process to leverage subject-matter expertise

[a] SSGA has USD$2.73 trillion under management, making it the third largest asset manager in the world. SSGA is a pioneer in index investing and has capabilities spanning both traditional and non-traditional asset classes across both active and index investing. See ssga.com for more info.

[b] A full case study is available at wbcsd.org. (WBCSD (2017). "State Street Global Advisors: Gender diversity as an opportunity to reduce investment risks."

Examples include:

- Internal and external audit from which findings may be ESG related (e.g., environmental health and safety, greenhouse gas emissions, certification audits performed by third parties)
- Due diligence activities from mergers, acquisitions and divestments
- Due diligence activities from new product or new market assessments
- ESG analyses performed for investment decisions (particularly for the financial services and manufacturing sectors)
- Project management activities (particularly for construction; information, technology and communication; professional services)
- Supply chain due diligence
- Media monitoring, web scraping
- Data tracking and analysis of events or issues faced in the past
- Monitoring regulatory changes
- Megatrend analysis
- SWOT analysis
- Impact and dependency mapping
- ESG materiality assessment
- Stakeholder engagement

Guidance

☐ Convene meetings with both risk management and sustainability practitioners to understand ESG-related risks

Some of these processes are described in detail in Chapter 2. In the risk identification stage, the critical question is which of these issues are threats or opportunities to the entity. This is illustrated in Figure 3a.1.

Figure 3a.1: Connecting the business context and strategy to risk identification



The Task Force on Climate-related Financial Disclosures (TCFD), formed by the Financial Stability Board in December 2015, recommends companies "describe their risk management processes for identifying and assessing climate-related risks," including "whether they consider existing and emerging regulatory requirements related to climate change."[6]

Risk management and sustainability practitioners can overlay the outputs of these activities or processes on the business strategy and objectives to identify ESG-related risks or opportunities. Some examples of this are provided in Table 3a.3.

Pro Paper & Packaging

See Appendix VIII for illustrative example of identifying the ESG-related risks that may impact a strategy or business objectives.

Table 3a.3: Example of overlay of strategic vision for risk identification

	Overlay of business strategy and objectives	Examples of ESG-related risks or opportunities
Megatrend analysis	How might the emergence of a global risk or megatrend impact the entity's strategy and operations?	• Consider the impact of global risks identified by the Allianz Risk Barometer 2018:[7] - The impact of extreme weather events and water crises on the company - The impact of natural disasters on the ability of the supply chain to operate efficiently to meet customer expectations
SWOT analysis	What are the ESG-related strengths, weaknesses, opportunities and threats?	• Consider how the entity can leverage technology and innovation to improve the sustainability of its product offering • Consider the impact of a safety incident
Impact and dependency mapping	What are the impacts and dependencies relating to the business model (inputs, business activities, outputs, outcomes)?	• Consider the entity's impacts and dependencies on local communities • Consider the entity's dependency on scarce resources for many of the packaging products • Consider the entity's impact on the safety of its employees and customers
Stakeholder engagement	Engaging internal and external stakeholders can help identify risks that are related to a broader group of stakeholders or have been overlooked by internal management. It is important to consider: • Who is sharing the information? • Why is it important to the stakeholder? • How does it impact the strategy?	• Consider the NGOs that have launched campaigns against the entity due to ESG-related concerns • Consider engagement with unions regarding labor relations • Consider how to leverage the relationship with stakeholders to build goodwill and stay ahead of emerging trends and preferences
Materiality and ESG assessments	The significant issues identified through the company's ESG materiality assessment or other ESG risk assessment tools should be considered for their impact on the business.	• Consider significant issues identified in the ESG materiality assessment (e.g., climate change, circular economy, human rights) and which of these may translate into ESG-related risks • Consider the salient human rights issues identified through the Human Rights Impact Assessment • Consider the greenhouse gas emissions profile and the resulting exposure of the organization to future carbon liabilities

It is every employee's responsibility to manage risk. Although often led by ERM, everyone in the organization – whether a project manager, sustainability manager, investment analyst or procurement manager – is responsible for identifying risks.

Framing risks

When identifying risks, it is important to go beyond simply "listing" the risks; rather, risks should be articulated *precisely* in terms of the impact to the strategy and business objectives as well as understanding the nature and root cause of the risk.

Understanding impact to business strategy

COSO defines risks as possible events that can affect the achievement of strategy and business objectives.[8] Therefore, any risk identified needs to be considered, described and framed in the context of how it will impact the strategy. Identified risks are translated into impacts at all levels of an organization (e.g., entity, business unit, division or other functional level).

Guidance

☐ Identify the ESG-related risks that may impact the organization's strategic and operational plans

Some aspects to consider when identifying and defining ESG-related risks include:

- What is the nature of the risk?
- What is the source of the risk?
- What is the root cause of the risk?
- Why is the issue relevant to the business?
- What is the business case for addressing the risk?
- Which business decisions may be impacted by the risk?
- What will be improved or enhanced by addressing the risk?

Not all ESG issues identified by an entity's ESG materiality assessment or megatrend analysis should be included in the risk inventory. For some issues, it may be appropriate for sustainability practitioners to perform ongoing monitoring and evaluation as to whether these risks should be elevated to an enterprise level and included in the risk inventory in the future. Regardless of whether the risk is included in the enterprise risk inventory, once a risk has been identified, risk management and sustainability practitioners can deploy ERM processes outlined in this guidance to assess, prioritize and respond to the risk.

Risks should be identified at any level of business in which there is a strategy, including entity, business unit, product and market/regional levels.

Describing risks with precision

When identifying risks, practitioners should aim to precisely describe each risk. The risk description should focus on the risk itself, rather than calling out a general ESG issue (e.g., climate change), the root cause of the risk, the potential impacts of the risk or the effect of the risk response being poorly implemented. In accordance with COSO, precise risk identification enables the organization to:

Guidance

- ☐ Define the impact of ESG-related risks on the organization precisely

- More effectively manage the risk inventory and understand its relationship to the business strategy, objectives and performance
- More accurately assess the severity of a risk in the context of business objectives
- Identify root causes and impacts and therefore select the most appropriate risk responses
- Understand interdependencies between risks and across business objectives
- Reduce the "framing bias" that can occur when a risk is framed to focus on either the potential upside or downside
- Aggregate risks to produce the portfolio view

COSO advises the following sentence structures for precisely articulating the risk:

- "The possibility of *[describe potential occurrence or circumstance]* and the associated impacts on *[describe specific business objectives set by the organization]*"
- "The risk to *[describe the category set by the organization]* relating to *[describe the possible occurrence or circumstance]* and *[describe the related impact]*"[9]

For guidance for assessing and articulating the impact of the risk on the entity, see sub-chapter 3b. Table 3a.4 provides examples of precise risk definitions for ESG issues, including the root cause and impact on strategy, objectives and performance.

Table 3a.4: Examples of precise ESG-related risk definitions

Precise risk definition	ESG issue or megatrend	Root cause	Impact on strategy, objectives and performance
The possibility that drought will impact crop yields and revenue	Water scarcity	The organization has invested primarily in water-intensive crops and therefore will be impacted by water scarcity during April and May.	Water scarcity may impact the ability to produce enough crops at the right price to meet the organization's revenue goals.
The possibility that a declining customer base will impact sales	Demographic shifts	The entity's customer base in Europe is declining because of negative population growth, an aging population and restrictive immigration laws.	The declining number of domestic customers in Europe could decrease revenue and profitability.
The possibility that participating in corrupt activities will impact the entity's operations	Anti-corruption	The entity operates in markets where corruption is commonplace and does not have processes in place to assess due diligence risks.	Bribery violates the US Foreign Corrupt Practices Act, UK anti-bribery legislation and the entity's core values and would preclude operations in those countries.

Analyzing root cause

Each risk in the inventory is driven by an underlying cause. Root cause analysis is a useful approach to understanding these drivers of business risk. It helps isolate the required changes so that entities can address a problem at its source rather than its symptoms.

Guidance

- ☐ Use root cause analysis to understand drivers of the risk

Collaborating to determine root cause increases the breadth of knowledge, understanding and experience, which can make the analysis more robust. Organizations should consider involving senior management and daily operations personnel to support this analysis.

Tools for understanding root causes include the five whys, cause-and-effect diagrams, hypothesis testing and comparative analysis. The example below illustrates how an organization may perform root cause analysis in practice.

The five whys

Asking "why" is key to effective root cause analysis. The "five whys" tool, starting with the issue or observation, guides managers to continue to ask "why" until they arrive at the root cause. For example:

Issue: The safety performance at one of the facilities is significantly worse than organizational averages, presenting an increased risk to the entity and inhibiting the ability to achieve the goal of zero incidents.

Why? There is a higher level of Occupational Safety and Health Administration (OHSA) violations at the facility than at other facilities.

Why? Workers at the facility are not using appropriate personal protective equipment (PPE) at all times.

Why? Workers at the facility are not being provided with appropriate PPE equipment and training.

Why? There is no specific environmental health and safety (EH&S) action plan for improvement at this facility.

Why? This facility was recently acquired by another entity, and its due diligence processes did not adequately assess the (EH&S) gaps existing in that entity.

3b. Assesses and prioritizes risks

Introduction

Effective risk management requires constant balancing of risk exposures, benefits and expenditures. For that reason, management assesses the severity of risks to support prioritization and maximize the strategic, financial and operational benefits to an entity.

ESG-related risks can be challenging to assess and prioritize. By nature, the financial or business implications of an ESG-related risk may not be immediately clear or measurable. These challenges are often exacerbated by an organization's (1) limited knowledge of ESG-related risks, (2) tendency to focus on near-term risks without paying adequate attention to risks that may arise in the longer term or (3) difficulty quantifying ESG-related risks. Even when the severity of an ESG-related risk can be quantified, the outcome may be uncertain. Finally, the risk may not be prioritized appropriately simply due to a conscious or unconscious bias towards risks that are known or better understood.



This sub-chapter relates to the following COSO ERM Framework principles:[1]

10 **Assesses severity of risk:** The organization assesses the severity of risks.

11 **Prioritizes risks:** The organization prioritizes risks as a basis for selecting responses to risks.

The following actions allow risk management and sustainability practitioners to assess the extent to which ESG-related risks impact the entity's strategy, business model and objectives:

- ☐ Understand the required output of the risk assessment (e.g., the impact in terms of the strategy and business objectives)
- ☐ Understand the entity's criteria for prioritizing risks
- ☐ Understand the metrics used by the entity for expressing risk (i.e., quantitative or qualitative)
- ☐ Select appropriate assessment approaches to measure risk severity
- ☐ Select and document data, parameters and assumptions
- ☐ Leverage subject-matter expertise to prioritize ESG-related risks
- ☐ Identify and challenge organizational bias against ESG issues

Assess and prioritize risks

An effective risk assessment examines the extent to which identified risks impact the entity's strategy and business objectives. As summarized in Table 3b.1, organizations achieve this by:

- Identifying the impacts or effects that the risk may have on the entity
- Selecting the most appropriate approach, data and assumptions for the assessment (analytical choices)

Taken together, these support an effective dialogue for prioritization that considers the severity of a risk relative to corresponding business objectives and the entity's risk appetite.

These considerations are not necessarily sequential and may require an iterative process. The appropriate metrics for severity are not the same for all types of risk, and they are subject to data or information availability. Further, the assessment approach selected depends on the risk prioritization criteria of the organization. Each of these considerations is discussed in more detail below (see Table 3b.1 for corresponding section references).

Table 3b.1: Overview of considerations for assessing risk severity

Assess risk severity
Perform assessments to express risks relative to the organization's ability to achieve its strategy and objectives.

1. Impacts and effects How does a risk impact the organization's ability to achieve its strategy and business objectives?	**2. Analytical choices** What is the appropriate method to assess risk severity?
1.1 Understand risk prioritization approach What criteria does the organization use to prioritize risks? Does the organization use judgmental evaluations or quantitative scoring methods?	**2.1 Assessment approach** Which assessment approach is appropriate for measuring the severity of ESG-related risks (e.g., expert input, forecasting and valuation, scenario analysis or ESG-specific tools)? What additional tools are available to support the assessment?
1.2 Understand metrics for severity Which metrics are used to express impact on the business strategy and objectives (e.g., earnings, costs, revenues, assets and capital allocation/investments)? Which metrics are used to measure the likelihood, rate of onset, frequency? Are metrics qualitative or quantitative?	**2.2 Data, parameters and assumptions** What are the data requirements? What data is available? Which parameters and assumptions should be applied (e.g., time, period, scope)?
3. Prioritize risks Prioritize risks based on severity, importance of the corresponding business objective and the organization's risk appetite.	

Adapted from the Task Force on Climate-Related Financial Disclosures (2017, June). *Technical supplement: The use of scenario analysis in disclosure of climate-related risks and opportunities.*

1. Impact and effects

A risk is relevant if it could impact the achievement of an entity's strategy or business objectives.[a] Once a risk is identified, understanding the potential business impacts and effects allows management to prioritize risks and allocate resources to respond and monitor the risk over time. To achieve this, risks should be translated into a common language that captures *risk severity*.

The following case study demonstrates how the impact of an ESG-related risk can be connected to the financial impact on an organization's strategy and business objectives. These results can be used in prioritization and resource allocation.

Guidance

- ☐ Understand the required output of the risk assessment (e.g., the impact in terms of the strategy and business objectives)

Pro Paper & Packaging

See Appendix VIII for illustrative example describing the impacts and effects of a risk.

[a] Note that there are exceptions to this, such as human rights impacts, which are discussed in detail later in this sub-chapter.

The financial impact of deforestation-free supply chains on Brazilian beef production

Brazil is the world's largest exporter of beef, making up almost 20% of the world market. However, the impact on Brazil's natural resources – and global GHG emissions – is significant. With only 1% of beef production in Brazil certified as sustainable, NYU Stern's Center for Sustainable Business led a research project to assess the financial benefits (e.g., productivity and profitability) of shifting to sustainable beef production. This analysis assessed the benefits for all players in the industry's value chain – namely, ranchers, slaughterhouses and retailers.[2]

The project looked at the benefits of sustainable and deforestation-free practices across five areas: cost reduction, revenue increase, risk avoidance, financial and valuation, and other. Using research, data analysis and interviews, benefits were calculated based on market demand, probabilities and penalty costs consistent with each indicator.[3]

The results are powerful for decision-makers, with evidence that sustainable agricultural practices lead to improved profitability across the value chain. The uptake of sustainable agricultural practices provided the most financial benefit, while the uptake of deforestation-free commitments reduced risk. In particular, ranchers reaped the most benefits as a percentage of total income – between USD$18 million and USD$34 million (12% and 23% of revenues) net present value over 10 years.[4]

1.1 Risk prioritization criteria

A range of quantitative and qualitative measures can be used to estimate the severity of risks while comparing and prioritizing them. Risk severity is commonly expressed in terms of impact and likelihood. However, some organizations are expanding their risk severity criteria (using, for example, velocity and recovery) to improve risk management of ESG-related risks.

Guidance

- ☐ Understand the entity's criteria for prioritizing risks

The COSO ERM Framework defines impact as "the result or effect of a risk" and explains that there may be a range of possible impacts associated with a risk. Further, those impacts may be positive or negative relative to the strategy or business objectives.[5] Table 3b.2 provides some examples of criteria used to assess the impact of risk.

Table 3b.2: Examples of impact prioritization criteria

Risk rating	Definition
Catastrophic	• Financial loss: [ ]% of earnings before interest, taxes, depreciation and amortization (EBITDA) or more than [ ]% impact on share price • International negative media coverage for more than six months that results in at least [ ]% revenue loss • More than [ ]% employee turnover • Prosecution, fines and litigation greater than [ ]% of expenses • Threatened or actual loss of [ ]% or more strategic customers
High	• Financial loss: [ ]% of EBITDA or share price • Reputation damage from media coverage that persists for one to six months and results in [ ]% nonrecurring revenue loss • Results from employee survey showing staff morale more than [ ]% less than peer organizations • Threatened or actual loss of [ ]% strategic customers
Medium	• Financial loss: [ ]% of EBITDA or share price • Reputation damage from media coverage that persists for less than one month and results in [ ]% nonrecurring revenue loss • Results from employee survey showing morale [ ]% less than peer organizations • Threatened or actual loss of [ ]% strategic customers
Low	• Financial loss: less than [ ]% of EBITDA or share price • Local reputation damage from NGO or media resulting in less than [ ]% revenue loss • Individual feedback from employees on low staff morale • Customer complaints from less than [ ]% of strategic customers

Please note percentages are not specified as they are for illustrative purposes only.

The COSO ERM Framework defines likelihood as "the possibility that a given event will occur."[6] In determining the likelihood, management may consider the following questions:

- What is the probability of the risk occurring? This may be qualitative (e.g., low, medium, high), quantitative (e.g., 20% likelihood in the next 5 years or 50% in the next 50 years) or frequency (e.g., once every 12 months).
- How quickly will the risk progress to the impact identified (e.g., considers velocity)?

Table 3b.3 provides some examples of criteria used to assess the likelihood of a risk occurring.

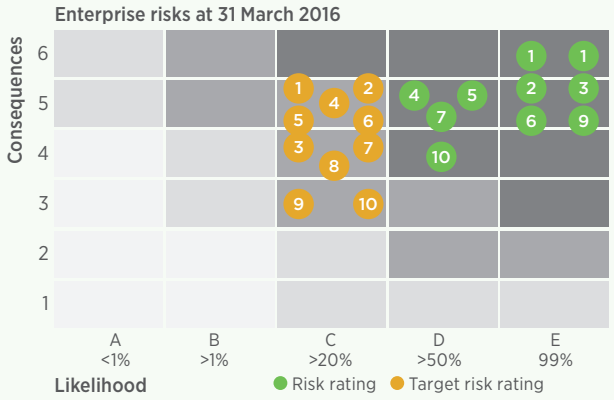
As shown in the example below, risks are commonly presented in a risk matrix or heat map depicting impact and likelihood of individual risks.

Table 3b.3: Example of likelihood prioritization criteria

Risk rating	Definition
Very high	• Once a year or more frequent • More than [ ]% chance of occurring
High	• Occurs once every 1-3 years • [ ]% chance of occurring
Medium	• Occurs once every 3-5 years • [ ]% chance of occurring
Low	• Occurs once every 5-10 years • Less than [ ]% chance of occurring

Eskom: using a heat map to prioritize risks

Eskom, a utility company based in the Republic of South Africa, uses a heat map to depict the prioritization of its most critical risks according to the likelihood and consequences (impact). The company's high-priority risks fall in the top right corner, depicting the inherent risk rating. The company assesses the risk against its target risk rating – or the target residual risk that management aims to retain once risk responses are deployed.[7]



The COSO ERM Framework states that, as part of the risk assessment, management considers inherent risk, target residual risk and actual residual risk.[8] These considerations support management in prioritizing risks and, even more so, in understanding the effectiveness of risk responses. For example, management may identify redundant risk responses that do not result in a measurable change to the severity of the risk.

Although impact and likelihood are common criteria for risk prioritization, in some cases, relying on these attributes alone can lead to a less accurate assessment or prioritization. In *Resilience: A journal of strategy and risk,* PwC[9] outlines some of the characteristics of ESG-related risks that render them different from traditional risks and causes these challenges in assessment:

- ESG-related risks can be more unpredictable and manifest over a longer and often uncertain time frame.
- Assessment of risk is often based on historical data. For ESG-related risks, particularly those that are new or emerging, it can be difficult to find historical precedence to estimate the risk impact.
- ESG-related risks are macro, multi-faceted and interconnected and can affect the business on many dimensions. This can make assessing an ESG-related risk more complex.
- Risks may be outside an entity's control. Responding to a risk may rely on the actions of other parties or may require coordinated efforts.

ESG-related risks also tend to be affected by organizational biases that exist when assessing and prioritizing risks. Specifically, organizational bias can lead to a failure to identify the full range of outcomes that may stem from a risk, or overconfidence in the accuracy of risk assessments and mitigations in place. There is also a tendency for individuals to anchor risk assessment estimations based on readily available evidence despite the known limitations of extrapolations of recent historical data to an uncertain and variable future. This bias is often compounded by confirmation bias, which drives individuals to favor information that supports a certain position and suppress information that contradicts that position.[10] Confirmation bias can be particularly common among those who hold strong positions about the science of climate change (either affirming or questioning the causes and expected impacts). See Table 3b.13 for more information.

To overcome these challenges, it can be helpful to consider additional criteria (beyond impact and likelihood) that provide a more complete understanding of the nature and extent of an entity's exposure. Table 3b.4 details a list of example criteria provided by COSO[11] that can be used for assessing and prioritizing risks and the relevance for ESG-related risks.

Table 3b.4: Application of prioritization criteria to ESG-related risks
(adapted from the COSO ERM Framework)

Criteria	Description	Relevance for ESG-related risks
Adaptability	The capacity of an entity to adapt and respond to risks	A risk may be significant and unpredictable; however, an organization can build in adaptability mechanisms to respond to or absorb the risk. For example, in the 1980s, Shell diversified its portfolio and used scenario planning to prepare and adapt to potential oil price fluctuations that were generally considered unforeseeable.[12]
Complexity	The scope and nature of a risk to the entity's success	Many ESG-related risks are interrelated, global, industry-wide and constantly changing. For example, health care companies are aware of the complex relationship between climate change and health. Climate change impacts may lead to potential disruptions to operations, while also leading to health impacts on individuals (increasing the demand for health care services). CPA Australia, KPMG and GRI reported that companies that incorporated megatrend analysis into the risk processes tended to focus on one characteristic and did not deal with the "complex and systemic megaforce whose impacts are over the short, medium and long term." For example, companies with exposure to water scarcity are more likely to focus on immediate water efficiency than investigating the risks associated with future water scarcity. Similarly, companies looking at resource scarcity and deforestation are considering efficient consumption of energy, water and paper as well as recycling initiatives but are less likely to explore deeper issues of changing land use practices and systemic impacts on ecosystem design.[13]
Velocity or speed of onset	The speed at which risk impacts an entity	ESG-related risks are often emerging and unforeseen until swift events result in extreme consequences. Climate change impacts often manifest in the form of more extreme or frequent occurrences of known events, such as droughts and floods, and are best understood by studying longer temporal horizons than are usually associated with typical risk management.
Persistence	How long a risk impacts an entity	Risk severity should consider the extent to which the impact will be an acute, onetime impact (e.g., cyclones, hurricanes or earthquakes) versus a chronic issue that will cause ongoing impacts (e.g., sustained higher temperatures or droughts).
Recovery	The capacity of an entity to return to tolerance	Consider how quickly the business would recover if a risk occurred today. For some ESG issues, impacts are irreversible. For example, in the food, beverage and agriculture sector, the impacts of climate change have the potential to alter growing conditions and seasons, increase pests and disease and decrease crop yield.[14] Recovery from these impacts requires enhancing capacity to manage and respond to the risk.

Additional considerations can be captured in alternative assessment criteria for understanding the risk severity or by incorporating these considerations into the impact and likelihood assessment during prioritization. This may be done at the enterprise level or for a specific risk.

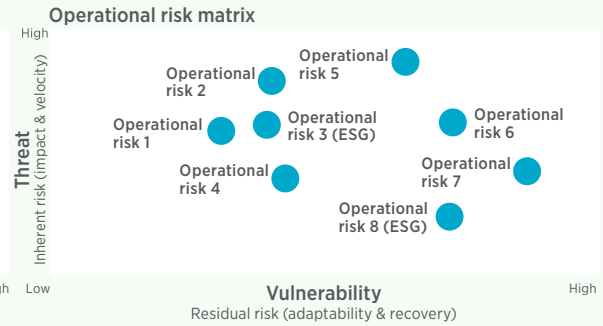
For example, in Figures 3b.1 and 3b.2, a threat (inherent risk) is defined in terms of the impact and velocity of individual risks to the entity, while vulnerability (residual risk) is defined in terms of adaptability and recovery. This approach expands on the traditional criteria of impact and likelihood to present the information in a way that supports decision-making.

Illustration of threat and vulnerability matrices[b]

Figure 3b.1



Figure 3b.2



- Figure 3b.1 summarizes threat and vulnerability of disparate risks (i.e., financial, compliance, strategic and operational) at a high level.
- Figure 3b.2 details threat and vulnerability of individual operated risks. This analysis can be applied to any risk at any level of the organization without relying on quantitative assessments of likelihood. It can also be used to show the linkages between correlated risks. For example, climate change may have a compounding impact on both operational risk 3 (damage to facilities due to severe weather) and operational risk 5 (disruption to operations or supply chain).

[b] Contributed by Funston Advisory Services, LLC

For a further example of this, in 2008 a multinational transport company revised its risk assessment process to capture the company's vulnerability to a particular risk event. The shift provided the company with enhanced preparedness for risk, as well as a competitive advantage and sales proposition.

Assessing risk based on vulnerability: The case of a multinational transport company

Following the impacts of the 2008 financial crisis, a multinational transport company realized that its "once a year" approach to assessing risks based on impact and likelihood was no longer fit for purpose. Not only did it fail to mitigate against the losses during the 2008 crisis, but it did not provide the company with the ability to adapt rapidly to a changing environment.

This led the company to modify its approach to assessing risk, considering impact and vulnerability as a way to understand risk and the company's overall resilience.

In 2008, the risk of pandemics was no longer considered a "black swan" but was a potentially significant social risk. The World Economic Forum's *Global Risks Report*[15] rated it as the fourth global risk in terms of impact. The risk management team recognized this vulnerability and the potential for an event to cripple the company. In response, the team developed business continuity plans that included alternative routes and operational plans to build resilience in the face of a global risk event.

As this risk materialized with the H1N1 virus in 2009 and customers started asking questions about the company response, the risk management team was prepared. Risk managers were invited to sales meetings where customers selected the company over its competitors because of its ability to demonstrate preparedness and alternative operational plans in the event of pandemics or other global shocks.

1.2 Metrics for severity

Depending on its prioritization approach and criteria, an organization selects a series of severity measures to assess, prioritize and communicate disparate risks. This may include metrics to understand:

- The potential impact of the risk
- The likelihood of the risk occurring
- Aspects relating to other criteria used in the assessment and prioritization process

Guidance

- ☐ Understand the metrics used by the entity for expressing risk (i.e., quantitative or qualitative)

Organizations consider both the quantitative and qualitative impact and likelihood of a risk.[16] Some organizations prefer risks to be quantified (and even monetized) to allow different risks to be compared and prioritized. In other cases, a qualitative assessment may be sufficient – particularly when quantification cannot be achieved. Risk management and sustainability practitioners should understand how the organization expresses risks to determine the output and level of precision required for assessing each risk, which can help in selecting the measurement method consistent with the language of the business. Some questions to consider in determining this include:

- What are the entity's mission, vision, core values, strategy and business objectives?
- What are the risk prioritization approaches and the criteria used by the organization (see Section 1.1)?
- What denominator(s) does the organization prefer to use for measuring and comparing risks (e.g., capital costs, operating costs, revenues, business interruption)?
- What assessment approaches are available to signal early detection and pattern recognition for prioritization and response?
- For which areas are qualitative measurements relevant for assessment and prioritization versus areas where a quantitative assessment is more appropriate?
- What is the appropriate level of rigor to apply to an assessment? Is it sufficiently reliable for decision-making?
- When are quantitative models, scenarios and other output values necessary and/or possible?

Table 3b.5 provides an example hierarchy used for measuring risk severity (non-exhaustive). Although this may not always be documented, most organizations have a preference for how risks are communicated throughout the business – driven by the organizational culture and the risk prioritization criteria (discussed in Section 1.1 of this sub-chapter). In this example, monetized, quantitative measures are the preferred expression of severity, followed by other quantitative or qualitative measures.

Table 3b.5: Example hierarchy for risk severity measures

Measure	Example risk severity metrics
Quantitative (monetary)	**Revenue:** Projected or identified impact on revenue or expenditures **Expenditures:** Projected or identified impact on expenditures or costs **EBITDA:** Projected or identified impact on EBITDA **Assets and liabilities:** Write-off, asset impairment and early retirement of existing assets **Capital and financing:** Impact to cost of capital or access to capital, operating losses **Share price:** Impact (%) in share price[c] **Customer/reputation:** Reduction in customer confidence (%) (may also be measured in revenue) **Safety:** Lost time due to injuries
Quantitative (non-monetary)	**Social media coverage:** Number of viewers of the entity's video **Business continuity:** Maximum allowable outage **Greenhouse gas emissions:** Total emissions by type of greenhouse gas (GHG); carbon intensity (GHG/USD $ million) **Energy/fuel:** Total energy consumption in megawatt hours **Water:** Total freshwater withdrawn in cubic meters from water-stressed regions **Land use:** Percentage change in land cover type (e.g., grassland, forest, cultivated, pasture, urban) **Location:** Number of locations within a designated flood zone
Qualitative	**Capital and financing:** Increase or decrease in ability to raise capital **Reputation:** Type of complaints received from stakeholders[d] **Staff morale/turnover:** Engagement survey results/level of engagement

Where possible, ESG-related risks should be assessed and framed in the preferred denominators of the organization. For many entities, it means that risk management and sustainability practitioners or risk owners will need to, if possible, assess the severity of an ESG-related risk in terms of revenue, costs or EBITDA.

However, the need for monetary assessments can present some challenges. Many entities' interactions with ESG issues do not yet have an easily measurable impact on market value or the price of products, materials or cash flows. For some ESG-related risks, this can be addressed by including a non-financial measure directly in the prioritization criteria. For example, some organizations prioritize risks that lead to any significant safety incidents as ''high'' regardless of whether a financial impact can be quantified.

For other ESG-related risks, organizations may need to develop or leverage tools and capabilities for quantification. The *Natural Capital Protocol*[17] and the *Social & Human Capital Protocol*[18] can support this quantification. These protocols are designed to help organizations identify, measure and value impacts and dependencies on natural and social capital (respectively) in terms of costs and benefits for business and society.

Although the costs and benefits to the entity should be the primary focus of this analysis, external costs and benefits to society can also contribute to the long-term value of an entity. Consider the example of JetBlue (below). After identifying a dependency on natural capital (i.e., pristine beaches at its destinations) in its business model, JetBlue adopted an approach to quantify the risk and return relating to this dependency. These impacts and dependencies are becoming increasingly relevant due to an increasing drive from customers, NGOs and other stakeholders for transparency or voluntary action by businesses to recognize these costs and benefits.

JetBlue: EcoEarnings — a shore thing

Leisure travel to the Caribbean is a key part of JetBlue's business model, with 1.8 million customers per year flying to the 23 countries in the region to enjoy beautiful, clean oceans and beaches. However, large-scale environmental degradation puts the business model at risk.

It is well known that airlines depend on natural resources, such as jet fuel, to operate and meet business objectives. Less explored, and certainly less quantified, is how airlines rely on natural and well-preserved destinations to drive tourism and encourage customers to buy tickets. If natural surroundings that draw tourists to the region are destroyed, the airlines and the local communities would lose a vital revenue stream.

JetBlue conducted an analysis to quantify both the risk and return from the Caribbean's natural attractions – effectively, an understanding of the risk associated with its natural capital dependency. The results indicated positive correlations among water quality, mangrove health, limited waste on shorelines and revenue per available seat mile (RASM).[19]

[c] Although fluctuation in share price can provide an indication of the impact of an event on how a company is perceived by the market; these fluctuations are often short term and may not have a long-term implication for the performance of the company.

[d] Using qualitative reputational metrics can also be problematic. Although companies are concerned about reputational impacts of risk, it is preferable that these are expressed in terms of a monetary or quantifiable impact on the strategy.

The particular case of business impacts on human rights

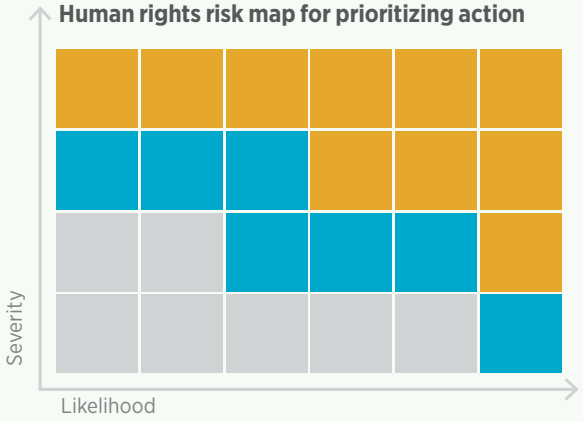
Responsible companies analyze their potential impact on the human rights of their stakeholders. The process of identifying, preventing, mitigating and accounting for potential human rights impacts is generally informed by the *UN Guiding Principles on Business and Human Rights*,[20] a document unanimously endorsed by the Human Rights Council in 2011 following rigorous consultation with business, governments and civil society. The *UN Guiding Principles* (UNGP) set out the content of the corporate responsibility to respect human rights - a responsibility that exists regardless of governments' ability or willingness to uphold their own duty to protect citizens from corporate human rights impacts. In other words, today's stakeholders expect companies to go beyond domestic law when necessary to uphold international standards of human rights.

The process for managing human rights impacts is referred to as "human rights due diligence" (HRDD). Under the UNGP, companies should develop and communicate a commitment to respect human rights, undertake human rights due diligence, embed the results of the due diligence across their operations and track results, communicate on their efforts and have in place operational-level grievance mechanisms to remedy impacts.

There are, however, key differences in the approach to risk assessment in the human rights context:

1. In HRDD, risk is assessed on the basis of likelihood and severity, but the perspective from which severity is assessed differs. In more familiar risk management processes, severity of risk is most often assessed in whole or in part from the perspective of risk to the organization, whether financial, reputational or otherwise. However, HRDD assesses risk from the perspective of the affected stakeholders only, that is, from the perspective of those who may be adversely impacted. This is a subtle yet crucial distinction: an organization may consider, for example, the risk of a certain indigenous group successfully protesting aspects of its operations as very low and the risk of reputational or other damage as unlikely; however, if that group is facing a human rights impact from the operations, HRDD would assess the risk as severe. Severity is also weighted slightly higher than likelihood, such that potentially severe events with low likelihood of occurrence may still be prioritized for management.
2. Stakeholder engagement is crucial in HRDD, and findings of a risk assessment should be tested with stakeholders. It is difficult for an organization to assess severity of risk from the perspective of potentially affected stakeholders unless it proactively engages with them to understand their vulnerabilities and potential to be impacted by the company's activities.

Key resources offer further guidance on risk assessment in a human rights context as set out in the next table.



Resources for human rights-related risk

Resource	Description
UN Guiding Principles on Business and Human Rights	Outlines principles on the corporate responsibility to respect human rights[21]
Shift and Mazars' UN Guiding Principles Reporting Framework	Provides implementation and assurance guidance on the UN Guiding Principles on Business and Human Rights[22]
Shift's "Assess" guidance	Provides guidance on how a company's operations and business relationships can pose risks to human rights[23]
Shift's Business and Human Rights Impacts: Identifying and Prioritizing Human Rights Risks	Reflects learning from a workshop with 12 Dutch companies together with expert stakeholders, hosted by the Social and Economic Rights Council of the Netherlands, about how companies can identify and prioritize human rights risks and test their findings through stakeholder engagement[24]
Global Compact and EY's Business and Human Rights: Corporate Japan Rises to the Challenge	Includes examples and provides guidance on human rights due diligence[25]
IFC Performance Standards	Focuses on the identification of relevant links between environmental and social considerations and human rights to support many important human rights, such as labor rights, rights of indigenous peoples and the right to health (through a clean environment)[26]

2. Analytical choices

In assessing the risk severity in terms of the business context and strategy, management makes a series of choices to determine an appropriate assessment approach and select the data, parameters and assumptions required for the risk assessment.

Guidance

- ☐ Select appropriate assessment approaches to measure risk severity

2.1 Assessment approaches

This section highlights four approaches that can be used to measure ESG-related risk severity qualitatively or quantitatively as outlined in Table 3b.6. This list is not exhaustive. There are a variety of other tools to support an evidence-based approach to risk severity assessment, such as competitor analysis, stakeholder assessments and peer benchmarking as well as specific data-driven approaches supported by technology and big data.

Table 3b.6: Measurement approaches

Approach	Description	Advantages and disadvantages
Expert input	Expert input refers to a forecasting method that relies on a panel of experts (e.g., Delphi approach) or interviews and discussions with subject-matter specialists.	• Relatively quick, limited analysis • Not always effective for ESG-related risks when relevant experts are not available to participate • May be appropriate for emerging risks, where data is sparse • Allows criteria other than "likelihood" and "impact" such as velocity or resilience to be included in the risk assessment discussion
Forecasting and valuation	Forecasting and valuation predicts the impact of a future event based on past and present data. Traditional ERM tools such as statistical regression and Monte Carlo simulation, as well as tools that leverage big data and artificial intelligence, can support quantification of ESG-related risks.	• Requires forecasting skills and internal or external data • Requires large amounts of data and probabilistic modeling tools
Scenario analysis	Scenario analysis develops plausible pathways to describe a future state.	• Requires forecasting and research of future outcomes • Allows simulation of events or disruptions
ESG-specific tools	Tools and approaches are available in the Natural Capital Protocol Toolkit[27] and Social & Human Capital Protocol Toolkit.[28]	• Leverages ESG issue and geography-specific assessment methods • Varying degrees of quality and maturity among the available tools

Selecting the appropriate assessment tool

The selected assessment tool should depend on a range of factors – such as the organization's prioritization approach, preference for severity metrics, time horizon of the risk and the type of risk being assessed.

For example, if a monetary assessment is appropriate, risk owners may leverage monetization approaches (e.g., climate-related risks based on scenario analysis, internal pricing mechanisms). Alternatively, risk owners may use existing and reputable non-monetary assessments (e.g., greenhouse gas emissions) or qualitative measures. Table 3b.7 shows the range of approaches organizations use to assess risk severity.

Table 3b.7: Examples of measurement approaches for risk assessment

Measure	Considerations	Measurement approaches
Quantitative (monetary)	• Useful when prioritization requires consistency with other risk severity assessments (e.g., financial value at risk and potential business impacts such as revenues, sales, margin, cost) • Supports decision-making for trade-offs • Assumptions and calculations can be complex • Example monetary impact: salaries paid (employment)	• Includes probabilistic and non-probabilistic models, decision trees, Monte Carlo simulations, value at risk (VaR), stress tests, severity, frequency and duration
Quantitative (non-monetary)	• Useful when time, resources or data are not available for monetization • Helpful for measuring progress over time • Disparate risks that cannot be compared (e.g., volumes of water versus loss of revenue) • Example non-monetary impact: number of jobs (employment)	
Qualitative	• Do not require significant amounts of data • Less precise, greater possibility of bias • Useful when there are many different perspectives or impacts • Helpful for risks that have a strong moral or ethical dimension • Example qualitative impact: expressed in categories of high, medium or low (employment)	• Environmental scanning, interviews, workshops, surveys, benchmarking, SWOT analysis, geopolitical assessments, root cause analysis and multimedia monitoring

The *type* of risk should also be considered when selecting the appropriate tool. Table 3b.8 demonstrates how the type of risk can guide the selection of the appropriate risk assessment tool.

Table 3b.8: Selecting the appropriate risk assessment approach[e]

Effect on performance	Risk description	Possible causes (risks)	Assessment approaches
Strategic	Failure to anticipate or adapt policy direction and business model in a rapidly changing environment	• Products/services • Geopolitical • Urbanization/growing population • Environmental • Social or stakeholder	• Environmental scanning • Peer benchmarking • Competitor analysis • Geopolitical assessments • Stakeholder assessments
Reputational	Unacceptable differences between how an organization wants and needs to be perceived and how it is actually perceived	• Reputation • A consequence of failure to manage other risks	• Media monitoring • Stakeholder engagement/surveys
Operational	Unacceptable differences between actual and expected operational performance (e.g., product quality, morale, training, ethics)	• Employee management • Human rights • Raw material availability	• Root cause analysis • Expert input • ESG-specific tools such as InVest (Integrated Valuation of Ecosystem Services and Trade-offs)
Business continuity	Inability to prevent, detect or correct business outages within established limits	• Natural disasters (e.g., hurricane, flood) • Supplier failure • Terrorism	• Maximum allowable outages • Probabilistic analysis • Forecasting and valuation (e.g., Monte Carlo simulation) • Scenario analysis

The appropriate tool may also depend on whether the risk is likely to have an immediate impact on the entity (e.g., worker fatalities) or those with a long-term indirect impact on the company, (e.g., CO_2 emissions).

Limitation of assessment approaches

All risk assessment tools have different strengths and weaknesses. Conventionally, impact and likelihood have been used to assess all risks, regardless of the type. Global reinsurer Swiss Re states, "Predictions about the likelihood of multi-causal losses actually depend on either sound understanding of cause-and-effect relationships or on a detailed loss history and the risks of the future have neither of the two."[29] Subjective probabilistic analyses are inevitably biased and may result in the over- or under estimation of opportunity or exposure. See also Table 3b.7.

[e] Contributed by Funston Advisory Services LLC

As such, all estimates are subject to some underlying uncertainty. Although this cannot be avoided, it is important to understand where the uncertainty occurs and document the limitations.[30] For example, an assessment of greenhouse gas emissions is subject to uncertainty due to the emissions factors selected, or extrapolation of data sets (if data for some facilities is not available). These key assumptions should be documented so they can be incorporated into the prioritization and decision-making process.

Expert input

Expert input harnesses the experience and knowledge of subject-matter professionals (either internal or external to the organization) in assessing or prioritizing a specific risk or set of risks. Expert input can also support identifying risks or providing additional understanding as to root causes, impacts or interdependencies. The results may be used as a stand-alone assessment or as inputs into further quantitative analysis for risk prioritization.

Expert input can be particularly useful for risks that have limited data or established models, which is often the case for ESG-related risks and other emerging risks. The absence of information or tools does not mean an organization can ignore the risks, particularly if they are rated high in the ESG materiality assessment. For these risks, organizations can engage subject-matter resources through a series of interviews or a workshop to obtain scenarios and estimates in terms of impact, likelihood or other criteria. These results are often used as data points into quantification tools such as scenario analysis or Monte Carlo simulation as described below.

The Delphi approach relies on a panel of experts (internal and/or external) who respond to several rounds of questionnaires or inquiry of risk ratings, assessing expected impact and likelihood of an individual risk or prioritizing a group of risks. Delphi may also be appropriate for identifying risks.

Example use of the Delphi approach for climate-related risk

The Delphi approach can be used with a group of climate subject-matter resources to develop distribution curves on climate impacts on a portfolio of facilities. The group could be presented with a series of questions, which may include the following:

- What is the range of sea level rise over the next 20 years in our operating regions (minimum, maximum and midpoints)?
- What is the range of anticipated distribution of major storms within our operating regions?
- What is the range of temperature changes anticipated in our operating regions?

This information can provide support to synthesize many sources of information into a distilled view. The outcomes of this workshop can support Monte Carlo modeling by providing the distribution curves that form the basis from the model.

From this, discussions with the operations team can help the company understand the resulting implications of the impacts on the facilities – for example, whether the impacts will lead to business disruptions, damage and flooding or changes in insurance pricing. The output provides the basis to appropriately prioritize the risk.

Many organizations also use the Delphi approach to prioritize overall risks, often using a survey, voting and/or average method (see section 3 for further discussion).

Forecasting and valuation

Forecasting and valuation can be effective measurement tools for ESG-related risks, by leveraging historical data from the entity or its peers to estimate the potential impact of a risk on revenue, costs or profit. Organizations can compare the impact of ESG-related risks in financial terms with other entity-level risks during prioritization.

The quality of forecasts is largely driven by the reliability of data and assumptions. For example, a Monte Carlo simulation (which provides the probability inputs for forecasts) requires large amounts of reliable data and assumptions developed by a group of experts (such as those described in the Delphi approach above) to produce a range of probabilities. Though less precise, data for an individual risk event can still contribute to a monetary risk assessment. For example, developing an assessment based on the cost of a single recall is less precise than an industry average of recalls over the past ten years.

Quantification of the impact of community conflict in the extractive sector

Human rights risks and impacts can be particularly difficult to quantify. A Harvard Kennedy School, Shift and the University of Queensland study in 2014 found that most companies do not adequately identify, understand or aggregate the cost of conflict with local communities, which can include contractual disputes, lost productivity and suspension of operations. Estimates suggest a USD$3-$5 billion project will suffer losses of USD$20 million per week of delayed production due to local communities' opposition.

This assessment provides a strong business case for developing human rights and stakeholder engagement programs to mitigate this risk.[31]

Data, parameters and assumptions can be based on historical entity experience (such as supplier spend or revenue) or proxy or extrapolated experience (such as the revenue and cost impact experienced by a competitor due to a product recall). These examples help to identify the value at stake for a selection of risks. See Appendix VI for some ESG examples that can be used to support these assessments.

Valuation can also be performed using methods that require more extensive data sets and subject-matter knowledge. A few examples of commonly used valuation approaches are shown in Table 3b.9 while other methods are included in the *Natural Capital Protocol*[32] and *Social & Human Capital Protocol*.[33]

Table 3b.9: Examples of ESG valuation approaches[34]

Resource	Examples
Abatement costs – the costs associated with limitation, prevention or repair of impacts (mostly used for environmental impacts)	TruCost estimates the "social cost of carbon" by monetizing the damages associated with an incremental increase in greenhouse gas emissions in a given year.[35]
Contingent valuation – survey-based approach to value non-market resources	A contingent valuation approach was used to estimate consumer willingness to pay for food safety health outcomes. It is estimated that there are about a million cases of foodborne disease in the UK each year, resulting in 20,000 hospital admissions and 500 deaths. Most of this illness is caused by microbial pathogens such as viruses and bacteria. The objective of this was to estimate this cost, for example, the willingness to pay to avoid pain, grief and suffering associated with illness and/or death caused by microbiological pathogens, chemical and radiological contaminants and allergens.[36]
Value-based pricing – estimation based on the next best available alternative	"Value-based pricing is the method of setting a price by which a company calculates and tries to earn the differentiated worth of its product for a particular customer segment when compared to its competitor." For example, a company can focus on a specific segment – such as buyers of paper towels made from recycled paper. The company would then compare the value against the next best available alternative, e.g., non-bleached paper towels. The company would determine the product differentiators (e.g., recycled and compostable) and estimate a dollar value on that differentiation (e.g., $0.75 per paper towel roll).[37]
Value (benefit) transfer – estimation method transferring information from another location or context to that in question	A benefit transfer approach was used to estimate the potential benefits from protecting and restoring the wetlands in Michigan. The researchers applied the values proposed in an Ohio study to coastal residents of Michigan. This enabled the researchers to determine monetary values for the Michigan wetlands.[38]

Assessing ESG-related risks is inherently uncertain, which may lead organizations to avoid monetary quantification. These forecasting tools enable management to develop its best risk assessment based on the information it has, while being transparent about limitations. Good practice does exist, and this should be leveraged. The examples below show how to use a range of internal and external data to develop monetary risk assessments.

Technology company: product safety and recall costs

A technology company assessed the potential severity of product safety risk resulting in a product recall. The company used data from Dell/Sony's 2006 lithium ion computer battery recall in which the company paid USD$400 million for 4.1 million recalled batteries.[39] The company considered this a reasonable comparison because it produces the same type of battery and has a similar manufacturing process.

Using the comparable average recall data for Dell/Sony, the company determined that in the event of a recall, the cost per recalled battery is approximately $98 per laptop battery (USD$400 million/4.1 million laptop batteries recalled).

The company has sold 5 million batteries, leading to a potential cost of USD$490 million (USD$98 x 5 million).

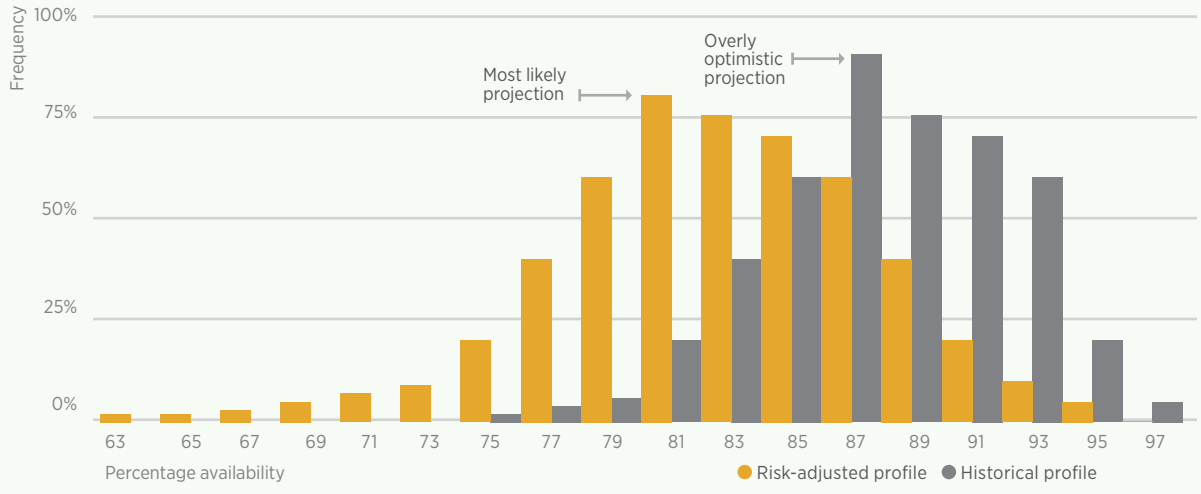
The managers understand that this estimated risk severity for product safety is not precise. However, the potential risk to the company and evidence of the event happening to peers were sufficient to elicit action from the company. It hired three additional personnel to implement controls over product safety, which reduced the company's risk and protected its customers.

Utility company: Monte Carlo simulation for severe weather risk

An electric utility company owns many generation plants. The company identified the risk of severe weather such as tornadoes impacting operating ability of generation plants for up to several weeks. This risk impacts revenue and customer confidence. The time horizon for risk assessments is five years, consistent with the company's strategic plan. It assessed the severity of the risk as follows:

- The risk managers obtained historical plant availability data for the past ten years. Using this data and the Monte Carlo simulation, they created a "historical profile."
- The risk management and sustainability practitioners worked together to obtain meteorological projections of expected storms in the next five years. They used this projection to determine the "risk-adjusted profile."

Generation plant availability



Based on this analysis, the managers observed that the plants were at a greater risk of deteriorating performance than history indicated. This warranted additional investment to prevent service degradation. Using this information, the company was able to prioritize the risk and develop and model its responses.

Scenario analysis

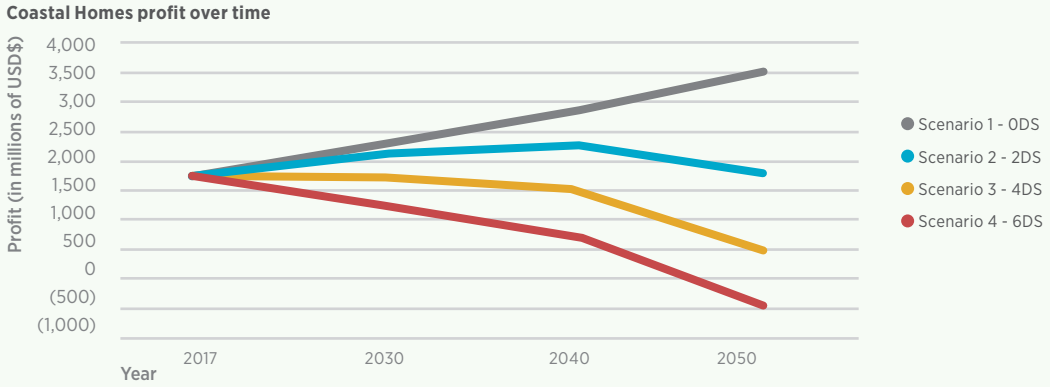
Scenario analysis is a well-established tool for assessing the potential implications of a range of long-term future states under conditions of uncertainty.[40] Originally developed at Shell Oil in the 1960s, scenario analysis is a systematic process for defining the plausible boundaries of future states.[41] This can be a particularly effective tool for ESG-related risks, as it reduces the extent to which managers need to "predict" possible outcomes – by providing a range of scenarios for the organization to consider and use for planning its response (e.g., Will the supply channel be modified? Which areas will be flooded?).

Many organizations and investors already use scenario analysis for anticipating future states for other risks, including climate-related risk assessments as part of their risk management and strategic planning processes. Appendix VII contains references to entity examples and climate-related scenario analyses from the Intergovernmental Panel on Climate Change (IPCC) and International Energy Agency (IEA). These examples and those in the TCFD's *Technical Supplement: The use of scenario analysis in disclosure of climate-related risks and opportunities*[42] provide detailed information on applying scenario analysis to climate-related risks. This tool can also be applied to other ESG-related risks (e.g., regional water availability, outsourcing labor cost models), which could emerge in distinct ways over time.

Real estate company: Climate-related risk

A real estate company operating in a warm, coastal country identified acute and chronic physical risks related to climate change impacting its ability to achieve target profits. The company used scenario analysis to project the impacts to the company through 2050.

The company leveraged the 2-, 4- and 6-degree scenarios (2DS, 4DS and 6DS) from IEA and followed the *TCFD Technical Supplement: The use of scenario analysis in disclosure of climate-related risks and opportunities* to model the effects of sea level rise, severe storms and increased daily temperature on the value and availability of insurance available to protect fixed assets.



The results of the scenario modeling:

- The severity of physical climate-related risks led the company to determine that doing nothing would challenge the survival of the business. The scenarios provide the ability to discuss the potential impacts on the company and how the company should respond and shift strategy.
- The company prioritized the risks as high based on the coastal location.

ESG-specific tools

There is also a range of specific approaches that can support ESG-related risk assessments. The Natural Capital Protocol Toolkit or the Social & Human Capital Protocol Toolkit enables professionals to identify subject-matter-specific tools for quantifying ESG-related risks. Examples from the toolkits are included in Table 3b.10.

Table 3b.10: ESG-specific risk assessment tools

	Tools	Examples
Natural Capital Protocol Toolkit	Greenhouse Gas Protocol	Greenhouse Gas Protocol Corporate Accounting and Reporting Standard provides guidance to companies for calculating greenhouse gas inventories.[43]
	WBCSD Water Tool	The WBCSD Water Tool is a multifunctional resource for identifying and calculating exposure of corporate water risk and opportunities, including a workbook, (for site investors, key reporting indicators and metrics) a mapping functionality and Google Earth compatibility.[44]
	InVEST	InVEST (Integrated Valuation of Ecosystem Services and Trade-offs) is a suite of open-source software models to map and value the goods and services from nature that sustain and fulfill human life. InVEST enables decision-makers to assess impacts associated with management choices and future climate, to identify where investment in natural capital can enhance human development and ecosystems.[45]
	WRI Aqueduct	WRI Aqueduct is a risk mapping tool that helps companies understand where and how water risks and opportunities are emerging worldwide. The Atlas uses a peer-reviewed methodology to create customizable global maps of water risk.[46]
	World Bank Climate Change Knowledge Portal	The Climate Change Knowledge Portal is a central hub of information, data and reports about climate change around the world. It allows users to query, map, compare, chart and summarize key climate and climate-related information.[47]
Social & Human Capital Protocol Toolkit	B Analytics, Global Impact Investment Rating System (GIIRS)	GIIRS uses B Impact Assessment methodology to deliver an accounting of an investment portfolio's impact on workers, customers, communities and the environment.[48]
	Impact Measurement Framework	This collection of sector-specific frameworks identifies relevant socioeconomic impacts, indicators and metrics.[49]
	Organisation for Economic Co-operation and Development (OECD) Guidelines on Measuring Subjective Well-being	These guidelines provide advice on the collection and use of measures of subjective well-being. They are intended to provide support for national statistical offices and other producers of subjective well-being data in designing, collecting and publishing measures of subjective well-being. In addition, the guidelines are designed to be of value to users of information on subjective well-being.[50]

The ESG-specific tools set out in Chapter 2, Table 2.8, such as the Equator Principles, Environmental or Social Impact Assessments, may also support assessment of ESG-related risks.

2.2 Data, parameters and assumptions

The calculation of risk severity requires practitioners to make choices about data, parameters and assumptions. In making these decisions, companies can start with the following considerations in Table 3b.11 which are outlined in more detail on the next page.

Guidance

☐ Select and document data, parameters and assumptions

Table 3b.11: Considerations for data, parameters and assumptions

Aspect	Considerations
Data sets	• What primary or secondary data is available as an input to the measurement tool? • What tools and frameworks can be used to support ESG-related risk assessments? • What assumptions are inherent in the selected data? • How reliable is the data? • Does the data apply to the defined scope of the risk?
Timing	• What time period should the analysis consider (e.g., strategic plan; 5, 15 or 30 years)?
Scope	• At which organizational levels (e.g., divisions, functions and operating units) and value chain (inputs, operations and markets) is the analysis applied?
Discount rate	• How certain are the expected events and timing of cash flows used in the monetary estimate? • Are these estimates established with enough subject-matter expertise or historical evidence to apply a discount rate?

These considerations should be documented to help companies maintain a clear view of how the severity of a risk is being measured and allow the assessment to be replicated over time. Discussion and peer scrutiny of the risk assessment inputs are important to build consensus and allow assumptions to be challenged.

Data sets

Management relies on the availability and quality of data as an input into its risk severity assessments. Finding quality data sets for ESG-related assessments can be a challenge, especially for organizations quantifying an ESG-related risk for the first time. Unlike financial information which is subject to internal controls, ESG-related information does not always receive the same level of scrutiny. Table 3b.12 provides a starting point for management to identify the primary and secondary data available for a risk assessment.

Table 3b.12: Example data sources for ESG-related risk assessments

	Data sources	Examples
Primary	Internal organization data	Supplier spend, sales performance, water usage, greenhouse gas emissions
	Survey results	Employee, supplier or customer surveys
	Interviews or focus groups	In-depth conversations for at-risk groups, such as employees, NGOs or communities
Secondary	Big data and big indicators	Highly detailed, continuously produced global indicators that track change in the health of the Earth's most important systems in real time
	Academic research	Credible research into the nature and extent of an ESG problem, such as plastic waste or e-waste
	Interviews with third parties or subject-matter experts	Interviews may include the Delphi outputs (refer to Monte Carlo example above); NGOs can provide insight into communities that may be otherwise inaccessible to the organization
	Government or think tank data	Open data, household budget surveys, demographic health surveys or other collection databases
	Industry or peer organization data or reports	Sector-specific data such as energy, compliance or cost data or assumptions that can be derived from publicly available information (see Appendix VI)
	Existing analysis	Internal or external analysis completed for other purposes, such as supply chain interruptions or costs associated with food safety issues
	Output from tools referenced in the Natural Capital Protocol Toolkit and Social & Human Capital Protocol Toolkit	Information or results from using the tools (e.g., biodiversity footprint) that can be used as inputs into monetary risk assessment
	Social Value International (SVI) Global Value Exchange	An open source database of values, outcomes, indicators and stakeholders focused on social and environmental data

Each data source or selection has underlying assumptions. When preparing forecasts or valuations, practitioners will need to understand the assumptions embedded into the data selected and any subsequent limitations. For example:

- Emissions factors may be selected based on the energy source and country, which may not be as accurate for calculating greenhouse gas emissions for operations within a specific city.
- Water scarcity risk may be based on rainfall and watershed measurements that are not current.
- Population growth for Europe may be based on current birth rates but may not take into account migration.
- Proxy data for calculating well-being may be based on a particular region, demographic group or socioeconomic class.

Understanding the assumptions embedded in the data also helps inform when risk assessments need to be updated. For example, many greenhouse gas emissions factors are updated annually, which can lead to an update in the risk severity calculation. See Chapter 4 for more guidance on reviewing and revising risk assessments.

Data quality and reliability

When determining which ESG data to use, it is important to consider the quality and reliability – particularly for data that relates to new or emerging issues or risks. Care should be taken when using "off the shelf" data or models. In assessing data quality, management should ask the following questions to select high-quality data sources:

- Is the data of high enough quality to produce reliable results?
- Are controls in place for internally collected data?
- Is the data collected in accordance with a time-tested or industry standard?
- Is secondary data open-sourced or available for challenge?
- Is metadata available to perform analysis prior to using the data?
- What are the key assumptions in the model or data?
- Is expert judgment used in the model or method?

When management has concerns about the quality of data, it may be appropriate to validate the data. Validation methods include testing the data based on metadata (e.g., summary statistics), implementing internal controls, validating a subset of the data or performing analyses to assess reasonableness.

Timing

The COSO ERM Framework suggests that the time horizon used to assess risks should be the same as that used for the related strategy and business objectives.[51] However, environmental and social risks often manifest over a longer time horizon than the one, three or five year time frames typically used for strategy setting. Managing these risks requires making investment decisions today for longer-term capacity building, or developing adaptive strategies which may be at odds with the short-term results that companies feel pressure to deliver.

Further, by considering only the most urgent risks, entities may neglect the long-term value they can deliver as well as the possible benefits of responding to risks before they fully emerge. Climate change impacts, for example, may emerge any time over the next 50 years. By assessing the impact of transitional or physical risks now, an organization can plan to respond to the risk more gradually, whether that includes pursuing opportunities for low carbon products or services, or building resilience against severe weather impacts into its operations.

Scope

Scope defines the organizational boundaries (e.g., divisions, functions, operating units) and value chain boundaries (e.g., inputs, operations, markets) being measured for each risk. These boundaries affect the relative importance of each risk. For example, risks assessed as important at the operating unit level may be less important at a division or entity level. At higher levels of the entity, risks are likely to have a greater impact on reputation, brand and trustworthiness.[52]

Discount rate

When assessing financial risks, practitioners often apply discount rates based on the weighted average cost of capital to arrive at the present value of the potential risk impact. Discount rates imply a level of accuracy based on the timing of predicted cash flows. Therefore, estimates need to be established with enough subject-matter expertise or historical evidence to apply a discount rate. Because of the uncertainty of ESG-related risks, applying a discount rate may not be appropriate given the lack of precision in the predicted cash flows.

3. Prioritize the risk

An organization prioritizes risks to determine:

- The urgency required in the management response
- The types of action necessary
- The level of investment in the risk response

Guidance

☐ Leverage subject-matter expertise to prioritize ESG-related risks

Section 1.1 of this sub-chapter explores the prioritization criteria companies use to compare risks across the enterprise. As discussed, *impact* and *likelihood* are often used to prioritize risks into categories, based on the preferred risk severity measures. Typically, financial metrics are the preferred denominator; however, companies may also include additional considerations, such as vulnerability, velocity or resilience.
The example below is an additional example of risk prioritization using a tiered approach.

Solvay S.A — using a tiered approach to classify risks

Solvay uses two ratings to prioritize the company's risks: impact and level of control. In its external report, it disclosed a range of criticality that is applied to its top eight risks and linked to corresponding ESG materiality aspects. For each risk, an owner is assigned to respond to and monitor the risk. The risk owner maintains the risk description and tracks associated prevention and mitigation measures for executive management.[53]

Criticality level	Risk	Trend in criticality level	Corresponding materiality aspects
High ↓	Security	↓	No significant link
	Climate related physical risks	→	Greenhouse gas emissions Water and wastewater management
	Industrial safety	↘	Accident and safety management Employee health and safety
	Transport accident	↘	Waste and hazardous materials management
	Ethics and Compliance	→	Management of the legal, ethics & regulatory framework
	Climate transition risk*	N/A	Greenhouse gas emissions Energy management Sustainable business solutions
	Cyber-risk	↘	Data security and customer privacy
Moderate	Chemical product usage	↘	Hazardous materials management Sustainable business solutions

* Emerging risk: newly developing or changing risk that may, over the long term, have a significant impact which will need to be assessed in the future.

Many companies use the Delphi approach to support the prioritization process (see the expert input section above). Convening a group of executives with representation across the business enables risks to be debated, compared and voted on. It is often in this session where additional assessment criteria (such as resilience, velocity and adaptability) are captured and discussed.

The cross-functional nature of these panels means that, in many cases, executives involved in these discussions are less familiar with ESG-related risks. As a result, the importance of these risks may be discounted during the voting process. Risk owners, risk management and sustainability practitioners can address this by providing the executive team with context on ESG-related risks such as the impact of the risk on the organization's strategy, key performance indicators (KPIs), peer or industry practices or public commitments. The example below demonstrates how an organization's human rights expert can provide insight to the executive team on an ESG-related risk.

Apparel manufacturing company: Delphi approach for human rights-related risks

An apparel company uses the Delphi approach to prioritize risks with the executive committee, including representation from finance, supply chain and operations.

The human rights manager identified the risk of human rights impacts that threaten the company's reputation. The risk was not well understood at the executive level; therefore, to support the prioritization process, the company's human rights manager provided a fact sheet to educate the risk committee prior to the meeting. The expert also attended the meeting to answer any questions and provide additional commentary as needed. The fact sheet included the following relevant information:

- The voluntary commitments the company made in relation to human rights (e.g., UN Global Compact signatory)
- The company's requirement to assess and monitor supply chain activities for human rights violations for approximately USD$120 million of the company's contracts
- Customers accounting for 5% of revenue expressed human rights-related concerns in recent surveys
- Some institutional investors who comprise 20% of the company's market capitalization raised changes in the regulatory landscape as a major concern, for example the UK Modern Slavery Act

The resulting prioritization led to the addition of human rights risk on the risk inventory and specific roles and initiatives established for managing this risk across the entity's global operations and supply chain.

Managing bias

When identifying, assessing and prioritizing ESG-related risks, it is important to identify and challenge bias. In any given entity, it is not unusual to find evidence of dominant personalities that drive certain positions or opinions; overreliance on numeric metrics, financial performance or historical data for decision-making; anchoring to a particular risk event outcome or response; disproportionate weighting of recent events or short-term financial risks; or a tendency either toward risk avoidance or risk taking.

It is critical to identify and challenge these biases to support better decision-making. Table 3b.13 provides examples of types of bias relevant for ESG in ERM.

Guidance

- ☐ Identify and challenge organizational bias against ESG issues

Table 3b.13: Types of bias that can impact ESG in ERM

Type	Description
Availability bias	People tend to think events are more likely to occur if they have recently heard of them happening. Thus, people overestimate the risk of death from tornadoes, cancer or accidents and underestimate the risk from asthma or diabetes. This is because tornadoes, cancer and accidents get a lot of press and movie coverage.[54]
Confirmation bias	People tend to emphasize data that confirms their established beliefs or ideas and to discount information that conflicts with their beliefs. People also fall for the "false-consensus effect," assuming that others share their world view. For example, if they believe in global warming, they expect that most people agree. Yet those who question its existence also believe they hold the mainstream opinion.[55]
Groupthink bias	Groups can make faulty decisions because group pressures sometimes lead to a deterioration of mental efficiency, reality testing and moral judgment. A group is especially vulnerable to groupthink when its members are similar in background, insulated from outside opinions and there are no clear rules for decision-making.[56]
Illusion of control	People find comfort believing they can control the world around them, even when they cannot.[57] For example, an organization may believe it is mitigating climate-related risk by accounting for and reducing GHG emissions and energy use.
Overconfidence effect	People, especially specialists and experts, overestimate how much they know. Compounding the overconfidence effect is the tendency to underestimate the time and costs of projects.[58]
Status quo bias	In choosing among alternatives, individuals display a bias toward the status quo. ESG-related risks are often new and emerging, or unexpected; therefore, individuals are less likely to identify them.[59]

The following questions can help identify ESG bias in an organization:

- Do dominant personalities or positions of power focus the attention on specific risks or dismiss risks that are not ESG-related?
- Does management over rely on numeric evidence in prioritizing risks, overlooking ESG-related impacts and dependencies that are not easily quantified?
- Does management disregard contrary information, including that related to emerging or unfamiliar ESG-related issues?
- Does management use a short- to medium-term time horizon (18 to 36 months) that may not effectively capture potentially slower-moving ESG-related risks?
- Does management have a tendency for risk avoidance or risk taking, which could impact the treatment of ESG issues?
- Is management overconfident about the controls in place to manage risk, which could omit considerations for more severe but plausible scenarios for ESG issues?

A robust ERM process can help counteract bias. Beyond becoming aware, the following are some short-term strategies to help overcome these biases:

- **Practice open-mindedness:** Improve judgment and challenge the status quo by eliminating the influence of stereotypes, idiosyncratic associations and irrelevant factors.[60]
- **Develop cross-functional teams and obtain objective informed inputs:** Seek advice from both internal and external experts to obtain diverse perspectives on individual issues.[61]
- **Quantify risks and use common language:** Identify methods for communicating with cross-functional teams using a common language and consistent metrics for assessing risks.[62]
- **Provide reference points:** Ask questions using a frame of reference that can be well understood. For example, instead of asking colleagues to identify potential environmental risks, ask them to answer a question such as, “How will our supply chain be impacted by severe flooding or hurricanes?” or “What would be the costs to our supply chain if we can no longer access our facilities?”[63]

3c. Implements risk responses

Introduction

For risks identified in sub-chapter 3a, management should select and deploy an appropriate risk response, which may be to accept, avoid, pursue, reduce or share. As described in the COSO ERM Framework, when considering a response, management should consider attributes such as the severity and prioritization as well as the business context and associated business objectives.[1]



This sub-chapter relates to the following COSO ERM Framework principles:[2]

13 **Implements risk responses:** The organization identifies and selects risk responses.

14 **Develops portfolio view:** The organization develops and evaluates a portfolio view of risk.

As discussed in sub-chapter 3b, many ESG-related risks are inherently difficult to predict and have a lower likelihood of occurring – albeit with potentially significant impacts or a longer time horizon over which impacts materialize. For this reason, reducing or eliminating the potential impact or likelihood of the risk occurring may be a challenge. For these risks, entity responses may choose to focus on adaptive strategies and operational plans that build resilience to prepare organizations to address risks as they unfold.

Of particular importance is assigning clear ownership for each risk response to the appropriate risk owner. The risk owner is responsible for assembling resources for designing and implementing a risk response. Where appropriate, addressing risks and building resilience can be bolstered with a collaborative approach that engages subject-matter experts from inside and outside the organization. A cost-benefit analysis can help select the best response and obtain buy-in for implementation. It can then be used to review the risk response for efficacy (see Chapter 4 for guidance on review and revision).

This sub-chapter sets out the following actions to help risk management and sustainability practitioners develop and deploy responses to ESG-related risks:

- ☐ Select an appropriate risk response based on entity-specific factors (e.g., costs and benefits and risk appetite)
- ☐ Develop the business case for the response and obtain buy-in
- ☐ Implement the risk response to manage the entity's risk
- ☐ Evaluate risk responses at the entity level to understand the overall impacts to the entity risk profile

Internal control framework

Risk management practitioners should work in tandem with an entity's internal control structure. Internal controls encompass the entity's control environment, risk assessment, control activities, information and communication and monitoring. Embedding strong internal controls can support the effectiveness of ERM – although ERM is broader in scope.[3] Refer to the 2013 COSO *Internal Control – Integrated Framework* for further information.[4]

Choosing risk responses

For all risks identified, management selects and implements a risk response. According to the COSO ERM Framework, risk responses fall within the categories of accept, avoid, pursue, reduce and share.[5] Each of these is detailed below:

Accept: Take no action to change the severity of the risk

This response is appropriate when risks to the strategy and business objectives are within the risk appetite and not likely to become more severe. For example, a manufacturer may accept potential for human rights-related risk in the supply chain if the entity has no high-risk suppliers and has not received any public pressure on the issue. The risk may be seen as too low to justify the cost of a program beyond requesting supplier compliance statements.

Accepting a risk often leads to a need for close monitoring of the assumptions that led the organization to accept the risk. If these assumptions change, a different response may need to be deployed (see Chapter 4 for further detail on monitoring risks).

Avoid: Remove the risk

Organizations may have zero tolerance for certain ESG-related risks, which leads them to avoid the risk entirely or at least reduce the likelihood that it will occur. For example, in 2018 Swiss Re announced that it would not provide reinsurance to businesses with more than 30% exposure to thermal coal across all lines of business.[6] Similarly, an entity that supplies services to a government may cease doing business in the highest risk countries to avoid any possible links to corrupt business activities.

Pursue: Convert risks into opportunities

Risk responses often focus on preserving value, but in many cases responding to ESG-related risks can unlock value for entities. The Business and Sustainable Development Commission[7] reported in 2017 that the United Nations Sustainable Development Goals (SDGs) could unlock more than USD$12 trillion in business opportunities by 2030.[a] Some examples are outlined in Table 3c.1.

[a] The estimate in reported benefits was determined using the following study on advancing women's equality from McKinsey Global Institute: Woetzel, J., Madgavkar, A., Ellingrud, K., Labaye, E., Devillard, S., Kutcher, E., Manyika, J., Dobbs, R., and Krishnan, M., 2015. The Power of Parity: How advancing women's equality can add USD$12 trillion to global growth. McKinsey Global Institute.

Table 3c.1: Examples of responding to risks through innovation

ESG-related risk	Responses	Value created, preserved or realized
Scarcity of raw materials or excessive waste	• Following a circular economy model, the Timberland apparel company and the tire manufacturer and distributor Omni United teamed up to produce a line of tires capable of being recycled into footwear outsoles once they reach end-of-life.[8] • MUD Jeans identified an opportunity related to ownership for its products at end of life. Under a circular economy model, the company collects and recycles its products.[9] • Pathway 21, which was developed beginning with a pilot project created by the United States Business Council for Sustainability Development, initiated the materials marketplace to facilitate company-to-company industrial reuse. Through the cloud-based platform, industrial waste streams are matched with new product and revenue opportunities, enabling a shift towards a circular, closed-loop economy.[10]	• Increased availability of raw materials through reuse • Improved profitability through sourcing lower cost inputs • Improved reputation regarding material use and waste
Animal welfare	• Procter & Gamble (P&G) identified a risk related to performing research on animals. In response, the company developed more than 50 alternatives and non-animal testing methods and has invested more than USD$410 million in finding alternatives and seeking regulator acceptance around the world. P&G scientists invented the first non-animal alternative to skin allergy tests.[11]	• Improved its reputation with animal rights activists • Leadership in delivery of non-animal testing methods resulting in satisfied and loyal customers
Climate change	• An automobile company looks to reduce the greenhouse gas emissions of its products manufactures electric vehicles. • An energy company identifies pricing and availability risks related to conventional forms of energy and invests in renewable energy. • Microsoft, like a growing number of other companies, places a price on carbon for internal accounting purposes as part of its long-term risk management strategy. This enables the company to talk about carbon in the language of business and reward parts of the company that can demonstrate cost savings from lowering emissions.[12]	• Offered new, in-demand products • Enabled the company to meet rising customer demands for renewable energy
Employee retention	• The hospitality industry has historically experienced low employee retention. Hyatt pursued this risk and now experiences an average tenure of more than 15 years for more than 14,000 housekeeping employees.[13] The company offers a training program called "Change the Conversation," which is based on principles from the Stanford School of Design that emphasize listening. Employees are encouraged to find new, creative ways to solve problems and accomplish everyday tasks.[14]	• Improved employee retention • Reduced hiring and retention costs • Enhanced efficiency and productivity from employee innovation
Changing customer profile	• Westpac, an Australian bank, identified the rapidly changing shifts in societal demographics as one of the four issues material to its business. In anticipating the future needs of aging customers, Westpac developed new planning investment and insurance proceeds to increase financial security, including: - A product that allows customers to generate growth for retirement through their investment portfolio while preserving a minimum outcome at the end of an agreed term - A contact center for customers aged 50 or older - A life insurance product that provides customers with recommendations on life insurance tailored to their situation[15]	• Developed new products and services • Improved customer service • Captured new customers and retained existing customers

Reduce: Take action to reduce the severity of the risk

Organizations typically take this action when the risk severity is higher than the risk appetite. Organizations may accept some level of risk for ESG issues and then implement mitigation activities to reduce the residual risk to within the risk appetite. Some common elements of a risk reduction program include investments in:

- **Strategy:** Establish a new strategy, goal or target to reduce the risk
- **People:** Assemble a team to lead a new initiative or provide training and support to improve research and development of innovations with environmental benefits
- **Processes:** Establish a "code of conduct" within the entity or across the industry to establish standards and expectations; adopt certification, chain of custody and audit programs to manage risks and enhance transparency to stakeholders
- **Systems:** Implement management systems to provide ongoing monitoring of risks according to the code of conduct (or other standards as appropriate)

These changes can be made at the overall entity level or other functional or geographic level. When determining the appropriate actions, organizations should research and leverage guidance from NGOs (such as the UN Guiding Principles on Business and Human Rights),[16] published standards (such as the ISO Standards on Air Quality[17] or GHG Emissions)[18] and principles (such as the Equator Principles,[19] Principles of Responsible Investment (PRI)[20] and/or industry groups or certifications).

For example, consumer products companies can apply the Palm Oil Assessment Methodology developed by the World Resources Institute[21] to prioritize high-risk mills or geographies and create incentives to improve performance, which helps reduce the risk of deforestation on availability of raw materials. Unilever piloted this guidance to better understand its deforestation risk.[22] As a result, the company relaunched its 2016 Sustainable Palm Oil Sourcing Policy,[23] which describes its commitment to respecting human rights, adhering to national laws, becoming more inclusive of smallholder farmers and increasing the traceability of its supply chain. The company is taking initiatives to support local mills and smallholder farmers to produce palm oil according to the standards of no deforestation as well as the related issues of no development on peat and no exploitation of people or communities (NDPE).

Organizations can also explore options to reduce the impact or likelihood of a risk occurring. For examples, see Table 3c.2:

Table 3c.2: Examples of reducing ESG-related risks

Risk	Reduction response
Risk of increasing energy costs impacting operational costs	Switch fuel or adopt a renewable energy strategy to reduce reliance on fossil fuels that may be subject to a carbon tax
Risk of community and NGO activity impacting business continuity in the mining and extractives sector	Engage stakeholders through one-on-one dialogue, town hall meetings, grievance hotline and regular outreach to stay informed of community and NGO expectations and concerns and address these concerns through initiatives such as community investments, land rehabilitation, facility design or operational decisions
Risk of disruption to supply due to extreme weather	Diversify supplier base and work with critical or strategic suppliers (>25% source) to develop business continuity planning
Risk of using an unfamiliar supplier negatively impacting product quality	Develop and enforce the use of an approved supplier listing

Share: Transfer a portion of the risk or collaborate externally

Sharing ESG-related risks may eliminate some risk to individual companies for ESG-related risks, which may be too large or complex for one entity to manage.

In responding to certain risks, an appropriate share response includes an industry- or issue-specific collaboration with other businesses, professional bodies, governments, NGOs, regulators, suppliers, customers, communities or even competitors. A prominent example is the agreement made at the 2016 United Nations Framework Convention on Climate Change (UNFCC) Conference of the Parties Meeting 21 (COP 21) in which 174 countries and the European Union supported by business and NGOs committed to goals and regular reporting to address climate-related risks.[24]

Carefully managed sharing of information, expertise and priorities can result in collaborative and trusted relationships that yield outcomes for both the business involved in the collaboration as well as society. Sharing information, resources, activities and capabilities across sectors, issues and geographies helps achieve scale to realize sustained impact. Consider for example the issue of plastic waste in oceans. Addressing this issue requires cross-functional value chain involvement from chemical and petroleum companies, apparel companies, institutional investors, consumer products and packaging companies, governments and NGOs. The World Economic Forum argues that achieving the UN Sustainable Development Goals will require these kinds of cross-sector alliances.[25]

This is particularly the case for supply chain initiatives. Entities have recognized that addressing complex supply chain challenges requires teaming up with peers, academia, standard setters and non-profit organizations. Multi-stakeholder collaborations focused on specific sectors, geographies, issues and commodities have proliferated in recent years. Most industries have now developed groups that work together to create common standards, share information, share auditing processes, increase leverage with suppliers and provide industry-level guidance. Some examples of industry- or commodity-specific collaborations are listed in Table 3c.3.

Table 3c.3: Examples of industry or commodity-specific collaborations

Industry or commodity	Collaboration	Value created
Apparel	Sustainable Apparel Coalition	The Sustainable Apparel Coalition is the apparel, footwear and textile industry's foremost alliance for sustainable production. The coalition's focus is on building the Higg Index, a standardized supply chain measurement tool for all industry participants to understand the environmental, social and labor impacts of making and selling their products and services.[26]
Beef	Global Roundtable for Sustainable Beef	The Global Roundtable for Sustainable Beef (GRSB) is a global, multi-stakeholder initiative developed to advance continuous improvement in sustainability of the global beef value chain through leadership, science and multi-stakeholder engagement and collaboration.[27]
Beverage	Beverage Industry Environmental Roundtable	The Beverage Industry Environmental Roundtable (BIER) is a technical coalition of leading global beverage companies working together to advance environmental sustainability within the beverage sector.[28]
Electronics	Global e-Sustainability Initiative	The Global e-Sustainability Initiative (GeSI) is a leading source of impartial information, resources and best practices for achieving integrated social and environmental sustainability through its membership of information and communication technology companies.[29]
Extractives	Extractive Industries Transparency Initiative	The Extractive Industries Transparency Initiative (EITI) is the global standard to promote the open and accountable management of oil, gas and mineral resources. The EITI seeks to strengthen government and company systems, inform public debate and promote understanding. In each of the implementing countries, the EITI is supported by a harmonizing coalition of government, companies and civil society.[30]
Multiple	Asian Roundtable Task Force on Related Party Transactions	The Asian Roundtable Task Force on Related Party Transactions was established to develop a practical guide to monitoring related party transactions. The meeting identified concrete options for detecting and curbing abuse, such as harmonizing the definition, assessing strengths and weaknesses of various regulatory approaches and tightening enforcement as well as facilitating a change in culture and practices.[31]
Pharmaceutical	Good Pharma Scorecard	The Good Pharma Scorecard, developed by Bioethics International (BEI), sets standards to rank and audit pharmaceutical companies and new drugs on how the drugs are tested, marketed and made available to patients. The initiative convenes physicians, patients, academics, regulators and pharma – to raise the bar on ethics and patient-centricity in the industry.[32]

Conducting risk assessments and cross-company scenario planning enables policymakers and industries to proactively identify network vulnerabilities and confer on the design of new legislation and regulation. This also fosters collaboration between regulators and business to address any challenges associated with the implementation of legislation.

Using "context-based" goals in determining risk response

As mentioned in Chapter 2, sustainability literature discusses context in terms of how an organization contributes to the deterioration or improvement of ESG conditions, developments and trends at a local, regional or global level.[33] For example, a context-based water target for a company may account for:

- A scientific understanding of a basin's conditions
- Local and global policy objectives
- The needs and perspectives of various stakeholders while maintaining alignment to the business context and strategy[34]

Practitioners can also apply science-based emissions targets as context-based goals to climate change to help companies develop reduction strategies in line with their industry or economic contributions.[35] Additional resources to support entities to set context-based goals include the Context-Based Water Targets Group,[b] C-FACT,[c] BT-Climate Stabilisation Intensity,[d] the 3% Solution,[e] Context-Based Carbon Metric[f] or Science-Based Targets.[g] For more guidance on contextualizing strategy and goals – refer to "The Road to Context: Contextualizing your Strategy and Goals."[36]

[b] Developed in collaboration with the UN Global Compact's CEO Water Mandate, establishes a framework to support the development of contextual water goals.

[c] Developed by Autodesk, Corporate Finance Approach to Climate-Stabilizing Targets (C-FACT) uses the IPCC climate stabilization recommendation of reducing greenhouse gas emissions by 85% by 2050 as its foundation. The methodology consists of four steps that aim to enable companies to develop contextual greenhouse gas emissions goals that are verifiable, flexible and fair.

[d] Developed by the BT Group, the Climate Stabilisation Intensity (CSI) Target model uses the 2007 Bali Climate Declaration as a baseline to develop a straightforward calculation that illustrates the absolute GHG emissions reductions needed to achieve the declaration in relation to GDP. This enables companies to develop a greenhouse gas emissions goal that is aligned with their contribution to GDP.

[e] The WWF and CDP partnered to create the 3% Solution, an online calculator that helps companies apportion their responsibility for greenhouse gas emissions in a way that is aligned with current climate science data. By focusing on cost savings, the project tries to build a compelling business case for US companies to set ambitious carbon targets.

[f] Developed by the Centre for Sustainable Organizations in 2006 and was the first contextual greenhouse gas metric developed. It supports the inclusion of scopes 1, 2 and 3 emissions and can take individual organizational changes into account.

[g] Launched in 2015, the Science-Based Targets initiative is a partnership between CDP, UN Global Compact, World Resources Institute (WRI) and the WWF aimed at helping companies determine how much they must reduce their emissions to prevent the impacts of climate change.

In rare cases, the risk or set of risks may be so significant that management may consider pursuing an alternative business strategy as a response (either at the next strategy setting milestone or, rarely, in the immediate term). This is discussed in Chapter 2.

Choosing risk responses

According to the COSO ERM Framework, the appropriate risk response is based on consideration of a number of factors, such as:

Guidance

- ☐ Select an appropriate risk response based on entity-specific factors (e.g., costs and benefits and risk appetite)

- **Business context:** Risk responses are selected or tailored to the business context, which includes the industry, geographic footprint, regulatory environment and operating structure. For ESG-related risks, questions may include:
  - How will the risk response minimize or exacerbate the ESG-related impacts and dependencies of the entity?
  - Which controls and business processes are in place to address this risk?
  - How will the risk response make it easier or more difficult to meet organization objectives?
- **Costs and benefits:** Capturing the anticipated costs and benefits to an entity is particularly important for ESG-related risks to demonstrate the business case and obtain buy-in. The costs and benefits to society may also be considered when assessing potential response options.
- **Obligations and expectations:** Responses should align with generally accepted industry standards, stakeholder expectations on ESG-related issues and performance (particularly NGOs, customers, employees) and the entity's mission, vision and core values.
- **Prioritization of risk:** Organizations use the prioritization of risk (sub-chapter 3b) to inform the allocation of resources. For ESG-related risks, speed of onset and vulnerability may be important considerations when determining the appropriate response. For catastrophic and high risks, responses typically require action plans that consist of new investments in activities to reduce or pursue a risk. For medium and low risks, an organization may accept the risk and monitor it for significant changes.

Pro Paper & Packaging

See Appendix VIII for illustrative example of risk responses.

- **Risk appetite:** Risk responses should consider the risk appetite of the organization – to develop action plans that reduce residual risk severity to within their risk appetite. If risk severity is within the risk appetite, management may choose to accept the risk.
- **Risk severity:** Responses should reflect the size, scope and nature of the risk and its impact on the entity.

Some risk responses may require a focused approach, such as basic compliance risks (responding to regulation to report annual greenhouse gas emissions), supply chain risks (establishing expectations and ongoing assessment processes to monitor human rights-related supplier information risk) or health and safety risks (establishing a management system with policies, procedures and systems). For other risks, management may find it appropriate to combine multiple types of risk responses to address a particular risk. For example, when addressing climate-related risks and anticipated increases in severe weather, an organization may reinforce buildings that are susceptible to hurricanes (reduce) while at the same time purchase insurance policies on those buildings (share).

Building risk resilience

The nature and complexity of ESG-related risks mean that an organization may not always be able to identify all possible risks, may not be able to mitigate against all the potential impacts of a risk or may not be able to pursue all available opportunities stemming from a risk. Even with the best assessment tools, an organization may learn that while severe weather events are likely, the timing or location of a hurricane cannot be predicted. Similarly, an organization may develop a robust social compliance program and stakeholder engagement process yet still come under intense criticism from NGOs or customers due to erroneous claims, misinformation or shifting stakeholder expectations.[h]

[h] For example, consider the impacts of a 2010 Greenpeace campaign against Nestlé. Greenpeace released a video parody of the company's KitKat "Give me a break" candy bar ads. The video implied that Nestlé was killing orangutans by buying rainforest for palm oil. The activist organization launched a boycott of Nestlé - despite the fact that the company bought palm oil in the commodity market, not from a specific plantation (Sheffi, Y. (2015). "The Power of Resilience: How the Best Companies Manage the Unexpected." The MIT Press.)

In these cases, organizations should focus on using a suite of risk responses aimed at enhancing their resilience should the risk eventuate. For example, mitigating against the possibility of a negative social media campaign may not be possible. However, by designing a crisis management plan that establishes processes, pre-approved responses and escalation paths, an entity can prepare for such a campaign, if and when it is launched.

Entities can also use business continuity planning to prepare for the short-term impacts from unexpected risks and scenario planning to prepare for various scenarios that may arise from longer-term trends and associated threats and opportunities. Transparently communicating the entity's selected response to NGOs, customers, investors or other stakeholders can also serve to reduce the severity or likelihood of negative campaigns occurring in the first place. These mechanisms can also be used by organizations to plan for a range of scenarios of future ESG-related challenges or changes to customer expectations, so it can innovate and create or realize value from new products or services.

Collaborate cross-functionally

It is critical to involve the right stakeholders in developing and executing a risk response. Engaging subject-matter experts can lead to innovation and more strategic solutions. For example, consider the risk that the safety and environmental performance of a telephone product impacts the revenue of a technology company. A tactical response may focus on compliance testing at the end of the manufacturing process. A strategic approach may use cross-functional collaboration to identify opportunities along the value chain to intervene to address the risk (see Table 3c.4).

Table 3c.4: Example of using collaboration to achieve a strategic risk response

Compliance or tactical response	Strategic response
• Sample test the safety and environmental performance of a product at the end of the manufacturing process and conduct root cause analysis to identify major issues	• Consult with the end-user to understand needs relating to safety and performance • Consult with procurement and suppliers to find opportunities for enhanced safety or environmental improvement • Consult with the customer service team to understand and monitor customer complaints relating to safety and environmental performance • Collaborate with peers to develop cross-industry standards for product safety

Develop the business case and obtain buy-in

Due to potential biases against allocating resources for ESG-related risks versus other risks (e.g., financial risks), risk management and sustainability practitioners may need to develop a business case for adopting a particular risk response. As organizations pursue ESG strategies to address some of the significant impacts, investors in particular will be looking to understand why resources are being allocated to create value for the business in the short, medium and long term.[37]

Guidance

☐ Develop the business case for the response and obtain buy-in

A business case may include an overview of the risk, root cause, response options, cost benefit analysis, key assumptions, roles and responsibilities, change management and implementation timeline. An important feature is the cost-benefit analysis of different risk responses. This analysis considers costs and benefits to the business but may also consider costs and benefits to the business and society that stem from either changes in access or availability of an element of natural or social capital on which the business depends or the capital impacts resulting from the activities of the business (see Table 3c.5). As detailed in sub-chapter 3b, the *Natural Capital Protocol* and *Social & Human Capital Protocol* can support this analysis.

Table 3c.5: Example of costs and benefits to business and society

	Entity costs and benefits	Societal costs and benefits
Cost	• May include direct costs (e.g., establishing a program, wages, IT systems or infrastructure, contractors) and indirect costs (e.g., overhead) • May include opportunity costs associated with the use of resources	• May include social costs (e.g., job loss, costs of health care, increased prevalence of disease) • May include environmental costs (e.g., pollution, soil depletion, water scarcity, greenhouse gas emissions)
Benefit	• May include the financial and non-financial benefits associated with the strategy and objectives • May include revenue, reputation benefits and contribution to ESG-related targets or objectives • May include benefits of recommended responses relative to other options • May include cost savings and avoided costs	• May include social benefits (e.g., increase in leisure time, affordable housing, feelings of safety and security, lower rates of disease) • May include environmental benefits (e.g., value of benefits from a watershed, improved air and water quality, biodiversity)

Circular economy cost-benefit analysis

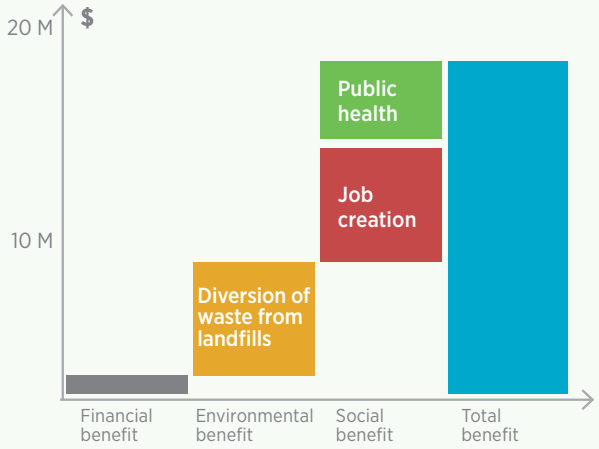
With growing regulatory risk in relation to e-waste, an electronics company explored the opportunity to implement a take-back scheme. Under the scheme, all products will be taken back from the customer for resale, recycling or disposal at end of life.

The company assessed the **financial benefit** to be **USD$0.7 million** resulting from increased revenue from the sale of recycled materials, reduced raw material costs and the cost to implement the reverse logistics.

Before deciding on whether to implement the scheme, the company also considered ESG-related costs and benefits to society. The significant costs and benefits included:

- The **environmental benefit** (to society) of approximately **USD$6 million** from diversion of customer products (waste) to landfills, which saves space in the landfill and therefore increases its life[38]
- The **social benefit** (to society) of approximately **USD$12 million** from job creation and promotion of public health from the responsible management of toxic chemicals such as lead and mercury found in electronics[39]

From this analysis, although the financial return was negligible, including the environmental and social benefits increased the **total benefit** of the program to **USD$18.7 million**. The company can also expect brand and reputational benefits associated with this program (although these were not quantified).



This analysis can support decision-making by capturing total environmental and social costs and benefits leading to additional value through the organization's license to operate, enhanced resilience and efficiency and sustainable growth. The COSO ERM Framework states that for an especially important strategy or business objective, there may not always be an optimal risk response from the perspective of costs and benefits – particularly a financial benefit.[40] In these circumstances it may be appropriate to incorporate this type of analysis into the business case.

Implementing the risk response

Once entities determine the approach, they implement their responses, which involve developing and executing an action plan for each risk response. At this point, the ERM process begins to influence day-to-day business decisions to preserve and potentially create value for an entity (see Table 3c.6).

Guidance

☐ Implement the risk response to manage the entity's risk

Table 3c.6: Examples of activities for implementing ESG-related risk responses

Proposed activity	Description
Assign a risk owner	• Assign a risk owner to be accountable for progress toward addressing each ESG-related risk. • The risk owner should have a team to support risk management plan development, implementation and monitoring progress.
Assemble cross-functional team	• Determine who needs to be involved in the risk response and implementation of the action plan. • While the risk owner should oversee the process, there should be management-level agreement on the functions that should contribute to the action plan and required level of effort. • A cross-functional oversight team, such as a sustainability council, could serve as an advisory board to help develop innovative, collaborative solutions to ESG-related risks. • Sustainability practitioners may: - Assist in developing cross-functional action plans. - Act as a risk owner or nominate a risk owner with appropriate cross-functional oversight. - Bring ESG knowledge, skills and capabilities when designing and implementing the response.
Obtain accurate and relevant information and inputs	• Discuss issues and potential solutions with employees involved in day-to-day operations. • Research leading practices at other organizations and within the organization itself. • Analyze data obtained during pilot tests or implementation.
Design risk responses to embed in decision-making processes	• Integrate risk and management considerations into planning and operational decision-making processes. • Incorporate risk responses into day-to-day decision-making. • Risk responses made at the entity level should be distilled to the managers at an operational level to make a consistent, desired impact.
Develop metrics to monitor the effectiveness of the risk response	• Consider the elements of the response that should be assessed periodically to ensure the risk is addressed in line with management's risk response decisions. • See Chapter 4 for additional guidance.
Communicate the risk response internally and externally	• For many ESG-related risks, both internal (e.g., senior management or the board) or external (e.g., investors, NGOs), stakeholders expect communication from the entity on the risk response. Sometimes this is due to regulatory requirements, such as the requirement to disclose how an organization is addressing supply chain risk of human trafficking) or to respond to an NGO or activist request for transparency on a specific risk (such as climate risk). • See Chapter 5 for additional guidance.

Develop a portfolio view

Risk responses are often developed at an individual risk level – even for a specific geography or business unit. However, risk and strategy managers need to take an entity-wide view of the risk profile in light of the risk responses. Management should consider how responses selected for an individual risk may have additive or offsetting impacts to the entity's overall risk portfolio. Risk responses designed for individual risks may also leave gaps in the overall risk coverage for the entity. Taking a portfolio view helps managers identify where gaps may exist and supports timely adjustments prior to finalizing risk responses.[41]

Risk management and sustainability practitioners need to understand the footprint of ESG-related risks within the entity's risk portfolio. Consider asking the following questions:

- What is the contribution of ESG-related risks to the overall company exposure?
- Which ESG-related risks are included in each risk category (e.g., strategic, operational, financial, compliance)?
- Where do the impacts occur (e.g., business unit versus geography)?
- Of these risks, which are systemic in nature and which are unique to an operating area?
- What needs to be known to better manage these risks?
- What interdependencies exist among risks that increase or decrease the overall severity to the company?

Guidance

☐ Evaluate risk responses at the entity level to understand the overall impacts to the entity risk profile

This view can also help risk management and sustainability practitioners, as well as risk owners, distinguish between local risks that are significant for one region versus those that will impact the entity as a whole.

4. Review and revision for ESG-related risks

Introduction

Chapters 2 and 3 focus on how organizations can leverage ERM activities to better understand and respond to ESG-related risks. ERM, however, is not a "one and done" activity. It is a dynamic process that requires ongoing review and revision of both individual risks and the ERM process overall. In many jurisdictions, monitoring the effectiveness of an entity's internal control and risk management process is required by regulation. For example, Norway's financial sector regulation on risk management requires the CEO to "continuously monitor changes in the entity's risks and ensure that the firm's risks are properly addressed in accordance with the board's guidelines."[1]



This chapter relates to the COSO ERM Framework component on reviewing and revising risk and the three associated principles:[2]

15 **Assesses substantial change:** The organization identifies and assesses changes that may substantially affect strategy and business objectives.

16 **Reviews risk and performance:** The organization reviews entity performance and considers risk.

17 **Pursues improvement in enterprise risk management:** The organization pursues improvement of enterprise risk management.

All entities experience continual changes to their internal and external environments. From these changes, new risks may arise, new data or assessment tools may emerge or risk responses may turn out to be ineffectual in addressing an identified risk or opportunity. By establishing indicators to review these activities, entities can recognize these changes before the risks lead to a negative impact on the business strategy or objectives and revise accordingly.

This chapter outlines the following actions to help risk management and sustainability practitioners review and revise responses to ESG-related risks:

- ☐ Identify and assess internal and external changes that may substantively affect the strategy or business objectives
- ☐ Review ERM activities to identify revisions to ERM processes and capabilities
- ☐ Pursue improvements in how ESG-related risks are managed by ERM

Assess substantial change

Compared to more traditional risks, ESG-related risks can change or evolve quickly due to changing demographics, emerging scientific data, new technology and innovation, growing stakeholder awareness and greater access to information and social media. In addition, the inherent nature of some ESG-related risks can make them more difficult to predict with accuracy – in particular the onset of climate-related risks. Due to these dynamic forces, organizations should continually monitor for substantial changes in the internal or external environment to determine if any of these shifts trigger a change in an entity's risk profile and require a response or decision from management. Table 4.1 sets outs examples of internal and external changes that may impact ESG-related risks.

Guidance

- ☐ Identify and assess internal and external changes that may substantively affect the strategy or business objectives

Table 4.1: Examples of substantial changes to the business context

Internal environment	External environment
• Changes in strategy or objectives • Rapid organizational growth • Organizational changes including change to leadership • Mergers and acquisitions • Innovation • Change in risk appetite	• New or pending regulations • Emerging technology • Changing stakeholder expectations • More frequent or extreme weather • Trends or strategies adopted by peer organizations • Shifts in global megatrends

For managing ESG-related risks, monitoring external shifts in the regulatory landscape is particularly important. For example, in recent years, large global companies have been closely monitoring the legislative and enforcement efforts focused on eliminating coerced labor from the world's supply chain of products[3] or changes in regulation in data privacy leading to the European Union's General Data Protection Regulation (GDPR).[4] Similarly, discussions with external stakeholders (regulators, customers, investors or peers) can reveal shifting trends and industry practices, such as changing demographics and customer preferences.

Chapter 2 outlines a variety of approaches that can support organizations in understanding changes to business context that may impact ESG-related risk performance.

Review ERM activities to respond to change

When significant changes in the internal and external environment are identified, or if the entity's performance is tracking outside of the acceptable level of variation, management may need to review or revise ERM processes or capabilities. Some examples of aspects of ERM that may require review are included below.

Guidance

- ☐ Review ERM activities to identify revisions to ERM processes and capabilities

Review governance and culture

ESG-related risk may lead an entity to consider the level of ESG awareness of the board or management structure and, if appropriate, introduce changes to the governance structure or processes. An entity may consider establishing a board committee to focus on ESG-related risks and issues or adding new board members with specific ESG-related knowledge (see Chapter 1 for guidance on approaches for enhancing ESG board awareness).

An organization may wish to review its culture if the entity is not embracing the actions required to address an ESG-related risk. For example, an organization that experienced a number of safety incidents or a catastrophic incident may decide to implement a "safety-first" culture.

Review strategy or business objectives

On rare occasions, should the performance of the entity result in a substantial deviation from the expected risk profile, the organization may choose to revise its strategy or change or abandon a business objective. For example in 2011, Asia Pulp and Paper's (APP) reputation was severely damaged after an aggressive Greenpeace campaign. The Indonesian business went from the world's biggest pulp and paper company to a brand better known for destroying pristine rainforest and driving species to the brink of extinction. Mattel, Disney and Unilever were among the 130 major companies to sever ties with APP. Within two years, APP developed a new strategy and that included a Deforestation Policy, goals that committed to help preserve high-carbon stock rainforests and greater transparency to stakeholders.[5]

See Chapter 2 for examples of organizations that have shifted strategy or objectives due to an ESG issue.

Review new or changing risks

Risk management and sustainability practitioners should stay alert to internal and external changes in the business context to monitor whether new ESG-related risks have emerged or substantially changed. When changes in the business context give rise to a new risk, or exacerbate or lessen the potential impact of an existing risk, risk management and sustainability practitioners should consider if action is warranted – such as a change to the risk inventory, a new risk assessment or investment in a risk response.

For example, as demonstrated recently in Cape Town, South Africa, water scarcity can have rapid and severe impacts.[6] Manufacturing companies may have been aware of their dependency on water for their South African operations but had not identified water scarcity as a significant risk. As water scarcity worsens, entities may upgrade the priority of the risk, developing water reduction programs and business continuity plans and establishing indicators to monitor water use and reservoir levels.

Review assessment approach or assumptions

As discussed in sub-chapter 3b, a risk severity assessment comprises the selected assessment approach and the data, parameters and assumptions underpinning the assessment. When new approaches or data becomes available, risk management and sustainability practitioners should consider whether the selected assessment approach is still the most appropriate.

For example, scenario analyses for climate-related risk incorporates a number of assumptions that may change over time. Some entities are currently adopting a 2°C scenario, based on a recommendation from the TCFD, as this provides a common reference point that is generally aligned with the objectives of the Paris Agreement and supports the evaluation of the potential magnitude and timing of transition-related implications. However, entities need to monitor trends and conditions to assess if there is a need to adjust this assumption over time. The TCFD recommends companies monitor the International Energy Agency (IEA), Deep Decarbonization Pathways Project (DDPP), International Renewable Energy Agency (IRENA) and Greenpeace scenarios to gauge the emergence or change of different pathways and the implications for the company.[7]

An organization may take the opportunity to either raise or lower the priority of identified risks to support reallocating resources. The change reflects a revised assessment of the prioritization criteria previously applied.

Review effectiveness of risk responses

Management reviews risk responses to understand how effectively they are addressing ESG-related risks, including whether the response brings the risk to within an acceptable level of performance. An organization may select indicators to monitor risk performance for ESG-related risks and set thresholds as alerts when risks tolerances are being exceeded and additional decision-making is required. The following example demonstrates how a business can set indicators and thresholds for ongoing risk review and revision.

Infosys Limited – monitoring water scarcity risk

Infosys, a multinational conglomerate, considers water scarcity a significant risk to its business operations in India. The company has implemented a monitoring process to identify factors in the external environment that could modify the risk severity assessment. Management identified the following enterprise-wide and campus-specific indicators:

- Water table levels for each geographic area
- Storage capacity of rainwater on each campus
- Availability and cost of water via water tankers for delivery

The risk owner reviewed and set thresholds for each of the above indicators. When indicator results exceeded an individual threshold, the risk owner alerted management for follow-up.[a]

Activity or outcome indicators can be used to monitor a risk and identify when revisions are required. Activity indicators allow organizations to assess the effectiveness of the implementation (such as the number of training events conducted), while outcome indicators focus on performance and overall risk exposure (such as the human rights performance of suppliers). Table 4.2 introduces activity and outcome indicators and shows how they may be used for monitoring an entity's supply chain program.

Pro Paper & Packaging

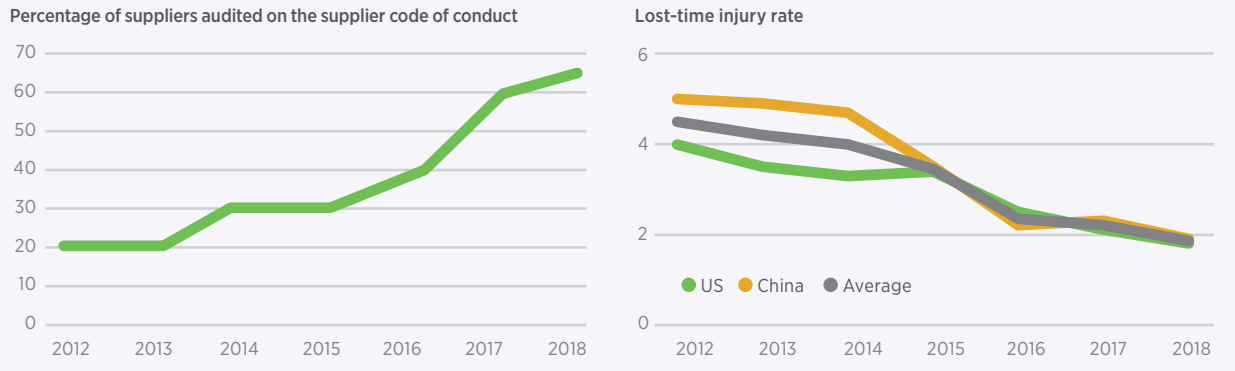
See Appendix VIII for illustrative example of setting thresholds to monitor ESG-related risks.

Table 4.2: Example activity and outcome indicators for monitoring a supply chain program

Activity indicators		Outcome indicators	
Inputs	**Processes**	**Outputs**	**Outcomes**
Resources used or spent on a business activity (e.g., cost of initiative)	Activities undertaken with the resources (e.g., number of training events)	The results from activities undertaken (e.g., number of participants trained)	Impact of the results or changes on social or environment capital (e.g., participants have better skills or are more employable and enter workforce)

Both activity and outcome indicators may be used to monitor trends over time. See Figure 4.1 for illustrative example trends of activity (percentage of supplier audits) and outcome (lost-time injury rate) trending.

Figure 4.1: Example trending of risk indicators (activity and outcome)



These indicators can be used to communicate to internal and external stakeholders how an organization is responding to a particular risk and the effectiveness of that risk response (see Chapter 5).

[a] A full case study is available at wbcsd.org. (WBCSD (2017). "Infosys: Mitigating water risk at India-based hubs.")

A selected risk response may also lead to unintended consequences by introducing new risks or risk consequences that have not been previously considered. For example, a beverage company may mitigate water scarcity risk by switching from reusable glass bottles to single-use plastic bottles reducing water use in production (required for initial cleaning of the glass bottles) and reducing reliance on scarce water resources. However, this may lead to an unintended, additional risk to the entity due to an increased focus on plastic waste from customers and NGOs.

Selecting indicators to monitor risk

To determine appropriate indicators to monitor a risk, risk management and sustainability practitioners may leverage the entity's key performance indicators (e.g., target employee retention, carbon intensity reduction target) or existing ESG-related frameworks used for sustainability reporting, such as the GRI. Although not designed to measure risks, the GRI indicators can provide example metrics used to review the organization response and performance.[8] The table below shows how GRI's water standard could be used for this purpose.

Example application of GRI to risk monitoring

	Description
Risk	Water scarcity impacts the entity's ability to operate.
Response	The entity is decreasing its water use, increasing its recycling and monitoring the water table to prevent further reductions.
Monitoring indicators	• Total water withdrawal by source and allocable share of water availability • Total water sources significantly affected by withdrawal • Total volume of water recycled and reused

Review changes to communication and reporting

The increased investor focus on ESG-related information, changing regulatory requirements and increased use of voluntary frameworks have led to changes in reporting and disclosure. Organizations may want to monitor the sufficiency and relevance of the ESG-related risk information they are collecting and reporting using approaches such as:

- Tracking ESG-related reporting requirements globally
- Monitoring new ESG-related reporting standards
- Benchmarking the organization's communication and reporting approach against peers or leading organizations
- Monitoring ESG-related shareholder resolutions or shareholder proposals, such as a proposal to set science-based emissions targets or appoint a human rights expert to the board
- Engaging stakeholders (internally and externally) on information needs

From these activities, an organization may determine if it needs to update its communications or reporting to better meet the expectations of its stakeholders or comply with jurisdiction requirements.

Timing of review activities

The timing of review activities varies by entity. While management often assesses each risk on an annual basis, significant changes may warrant interim action. Although some environmental risks, such as climate change, are not expected to impact organizations in the short term, frequent reviews of the anticipated physical and transitional impacts as well as assumptions and scenarios are warranted, as these are not necessarily predictable. For example, a megatrend analysis may be performed every three years, supplier risk assessments may be updated annually, while safety incidence or grievances would be monitored on a continuous basis. In addition, assessing the status and effectiveness of risk responses may need to be evaluated and communicated quarterly or semi-annually.

Roles and responsibilities for review activities

Risk owners are typically responsible for reviewing risk responses, developing indicators to review risks and tracking performance. Sustainability practitioners may support this with their knowledge of ESG issues. For example, a risk owner responsible for monitoring water scarcity may leverage a sustainability practitioner's knowledge of geography-specific water regulation and appropriate tools and resources for tracking water risk by region.

Pursuing improvement

Even those entities that have effectively integrated ESG-related risk management into ERM processes can continue to become more efficient. The COSO ERM Framework offers opportunities to revisit and improve efficiency in ERM – starting with the overall processes and structure and cascading to other ERM activities.[9] Some areas that provide opportunities to revisit efficiency of the management of ESG-related risks may include:

Guidance

☐ Pursue improvements in how ESG-related risks are managed by ERM

- **New technology:** ESG-related software platforms may offer an opportunity to compile higher-quality data (e.g., water, waste, greenhouse gas emissions, and safety incidents) in a centralized system. Data monitored through satellites (e.g., deforestation patterns) or social media platforms (e.g., shifting customer preferences or campaigns, union strikes) may be used to provide real-time information on risk performance to the organization.
- **Organizational change:** An organization that is expanding operations into emerging markets may expect to face more ESG-related risks (e.g., human rights) in the future and therefore may appoint a subject-matter expert to the board, executive or management team. Mergers and acquisitions may result in a new facility that does not immediately meet the standards or expectations of the organization.
- **Risk appetite:** Reviewing performance provides clarity on factors that affect the entity's risk appetite. It also gives management an opportunity to refine its risk appetite. For example, risk management and sustainability practitioners may implement a public deforestation policy for sourcing of palm oil. Once management is comfortable that the organization can comply with the commitments for one commodity, it may expand the policy to cover beef, pulp and paper, and soy.
- **Peer comparison:** Reviewing industry peers can help an organization determine if it is operating outside of industry performance boundaries. For example, a global food and beverage company discovered during a peer review that several competitors had established a strategy and targets for reducing sugar inputs across the product portfolio to meet a fast-growing customer segment. Consequently, the company reviewed and revised its strategy to increase its competitiveness and, therefore, performance in this customer segment.
- **Historical shortcomings:** Organizations that have failed to identify or manage ESG-related risks in the past may conduct a "lessons learned" exercise to understand how ESG can be better integrated throughout the ERM process.

5. Information, communication and reporting for ESG-related risks

The final chapter of this guidance relates to the communication and reporting of ESG-related risk information to stakeholders. Risk information serves as an input to many strategic, operational, investment or purchasing decisions made by both internal and external stakeholders. Organizations should leverage existing communication channels in order to provide timely, relevant and quality ESG-related information to target audiences.[1]



This chapter relates to the COSO ERM Framework component on Information, communication and reporting and the three associated principles:[2]

18 **Leverages information technology:** The organization leverages the entity's information and technology systems to support enterprise risk management.

19 **Communicates risk information:** The organization uses communication channels to support enterprise risk management.

20 **Reports on risk, culture and performance:** The organization reports on risk, culture and performance at multiple levels and across the entity.

The primary aim of internal communication and reporting is to provide decision-useful information on an entity's risk management approach and performance. Internal communication and reporting can enhance awareness of ESG-related risks to the appropriate level of the entity, communicate how well the risks are being managed and provide information to support better decision-making across the entity.

External communication and reporting on risk management are regulatory requirements in many jurisdictions, requiring entities to report on the risk management process and disclose key risks to a selection of defined stakeholders. An increase in demand for ESG-related information from investors is also driving organizations to voluntarily disclose ESG-related information publicly.

This chapter sets out the following actions to help risk management and sustainability practitioners communicate ESG-related risks internally and externally:

- ☐ Identify relevant information and communication channels for internal and external communication and reporting
- ☐ Communicate and report relevant ESG-related risk information internally for decision-making
- ☐ Communicate and report relevant ESG-related risk information externally to meet regulatory obligations and support stakeholder decision-making
- ☐ Continuously identify opportunities for improving the quality of ESG-related data reported internally and externally

Information and channels for communication and reporting

For ESG-related risks that have been identified and prioritized, information relating to those risks may be relevant to a range of internal stakeholders, including the board of directors, operational management and employees, as well as external stakeholders such as shareholders, regulators, customers, civil society and non-governmental organizations.[3] For each stakeholder group, the organization may consider:

- What ESG-related risk information is required for decision-making?
- Which ESG-related indicators and metrics are appropriate to provide decision-useful information?
- How frequently is the information required?
- Which channel and medium should be used to communicate the information?
- What are the appropriate escalation paths for a given risk?
- What controls or processes are in place to ensure data quality (e.g., controls over internal data, external assurance)?
- What is the most effective way to communicate the risk? Where possible, organizations should try to communicate risks in terms of how the risk impacts the entity's strategy and objectives (see sub-chapters 3a and 3b for additional guidance).

Guidance

☐ Identify relevant information and communication channels for internal and external communication and reporting

The risk owner is the central owner of risk information and communication. Risk owners can work with sustainability practitioners or other stakeholders to understand ESG-related information requirements and channels for communication. Sustainability practitioners are particularly involved in external communication of ESG-related risks, such as sustainability reports or climate-related disclosures.

Leverage information systems

While most global organizations use financial and operational data systems daily (e.g., accounting systems, enterprise resource planning (ERP) systems), information systems for capturing and reporting ESG-related information are less common. Nonetheless, organizations that use information systems to collect and aggregate ESG-related data across the entity may see improvements in the following:

- Monitoring and communication
- Data quality
- Visibility of risk across the entity
- Decision-making
- Timeliness
- Collaboration and cross-functional teaming

For example, an entity using an environmental health and safety (EH&S) software platform can compile data on health and safety incidents from multiple operating facilities shortly after they occur. Root cause can be determined and recorded in the system at the time of the incident. This information can then be compiled by the organization for trend analysis to understand the facilities with more significant or frequent safety issues. The facilities with similar safety issues can work with facilities that demonstrate leading practices to develop and implement practical solutions. Further, this information can be analyzed alongside other information management uses for decision-making when software platforms housing EH&S data are combined or in communication with existing software infrastructure.

Internal stakeholders: Communicating and reporting

Communication of risk information is critical to improving decisions relating to strategy-setting and day-to-day operations. Internal communication of ESG-related risks in particular can help to:

- **Inform the board of directors and management how ESG-related risks will impact the business strategy and objectives:** This can help the board and management to make informed decisions and seize opportunities.
- **Promote awareness of critical ESG-related risks to the entity:** Such awareness can support better day-to-day decision-making and allocation of adequate resources to address the risk.

Guidance

☐ Communicate and report relevant ESG-related risk information internally for decision-making

- **Encourage a culture of risk awareness and employee engagement throughout the organization:** For example, an airline may communicate aggregated safety data to employees to allow them to understand how they contribute to the airline's or airport's safety performance. A typical safety newsletter captures both leading (e.g., number of employees trained on safety) and lagging (e.g., incident rate) indicators.

Communication on risk varies depending on the audience (e.g., board of directors versus operational management) and information needs of each stakeholder (e.g., the need to understand the details of an entity's risk response versus overall effectiveness). Table 5.1 provides examples of the considerations that risk management and sustainability practitioners should consider when preparing communications for specific audiences based on the escalation paths defined by the organization.

Table 5.1: Internal stakeholder groups, information and communication

Stakeholder group	Example information needs	Example communication methods
Board of directors Provides strategic oversight for critical risks to the entity	• Significant changes to the internal and external business environment and the organization's approach to these changes • Risks that are falling outside the risk appetite or tolerance • Overall effectiveness of risk responses	• Board meeting pre-reads and presentations • External/third-party materials (e.g., industry, trade and professional journals, media reports, peer company websites, key internal and external indices)
Operational management Oversees day-to-day operations that incorporate risk responses	• Significant changes to the internal and external environment impacting strategy and risk appetite • Significant changes to a risk or risk profile • Status and effectiveness of risk responses	• Written internal documents (e.g., briefing documents, dashboards, performance evaluations, presentations, questionnaires and surveys, policies and procedures, FAQs) • Informal/verbal communications (e.g., one-on-one discussions, meetings)
Employees Perform day-to-day operations that incorporate risk responses	• Nature of the risk responses and impacts on roles and responsibilities • Importance of the risk response activities to the organization	• Training and seminars (e.g., live or online training, webcast and other video forms, workshops) • Materials, meetings or interactions • Electronic messages (e.g., emails, social media, text messages, instant messaging) • Public events (e.g., road shows, town hall meetings, industry/technical conferences)

External stakeholders: Communicating and reporting

External stakeholders are interested in understanding how an organization is managing its ESG-related risks to create and maintain shareholder value or address ESG issues that may impact society or the environment. While there are requirements for reporting risk-related information in many jurisdictions, organizations also recognize the benefits in communicating and reporting ESG-related risks externally to demonstrate responsibility, accountability and corrective action on risks that stem from impacts and dependencies the entity has identified.

As such, external communications and disclosure on ESG-related risks should align to an entity's mandatory and voluntary reporting obligations.

Mandatory reporting obligations

In preparing external communications on ESG-related risks, organizations should start with understanding the risk and ESG reporting requirements for their jurisdiction. This includes understanding the entity's requirements for reporting:

- Significant or material risks (e.g., SEC-registered companies are required to report material risk factors in their annual 10-K/20F)
- Individual ESG-related risks that meet the organization's criteria for materiality and disclosure in legal filings (e.g., chemical companies including: health and safety concerns as a material risk factor)
- ESG issues that contribute to other material risks (e.g., severe weather which may contribute to business continuity and could be included in the description of the risk in legally mandated disclosures)
- ESG-related risks or issues that are required to be disclosed under a separate requirement, such as France's Article 173-VI, which requires asset management companies and institutional investors to describe methods for incorporating ESG factors into the investment strategy and means employed to support the energy and ecological transition[4]

Guidance

☐ Communicate and report relevant ESG-related risk information externally to meet regulatory obligations and support stakeholder decision-making

Chapter 1 provides additional detail on the role of fiduciary duties for reporting ESG-related risks as well as ESG-related regulatory requirements. Additional voluntary frameworks for reporting ESG-related issues can be found in Appendix III. Jurisdiction requirements for reporting risk factors and ESG-related risk factors are summarized in Appendix II.

Voluntary communication and reporting

In addition to mandatory disclosure requirements, most entities have external stakeholders that have an interest in their activities, which require broader communication and disclosures. Stakeholders may include investors, suppliers, customers or community groups.

Many considerations affect the decisions organizations make about external reporting of ESG information. Various possibilities are available to companies when considering which ESG information they should report and how and where the information should be reported as well as for which audiences.

In one EY study, 81% of institutional investors stated that companies do not adequately disclose the ESG-related risks that could affect their current business models – with 60% calling for companies to disclose these risks more fully.[5]

To understand what assumptions inform the conclusions made and what purposes and audience the information is intended to serve, organizations should identify their stakeholders, understand their ESG-related priorities and information needs, and determine an approach for communication. Table 5.2 provides examples of information expectations of external stakeholders and methods for communicating with them.

Table 5.2: External stakeholder groups, information and communication

Stakeholder group	Example information needs	Example communication methods
Investors Provide capital to the entity with an expectation of financial returns	• Entity's approach for managing significant changes to the internal and external environment leading to ESG-related impacts or dependencies • Understanding of how the entity identifies, assesses and manages its ESG-related risks (e.g., climate-related risks)[6]	• Annual general meeting of shareholders • Annual report, risk filing or 10-K • Integrated report • Proxy
Suppliers Supply goods or services to the entity	• Entity's standards for suppliers which may include areas such as ethics, integrity, legal standards, compliance, health and safety and environment • Supplier performance against the entity's ESG-related standards	• Supplier code of conduct • Report card, including, for example, quality, delivery, quantity delivered, performance history, incident report and comments • Management meetings[7]
Customers Purchases the entity's goods or services	• Information on how the product was made (e.g., ingredients, country of origin, factory information) • Information on how to use the product and whether it may impact the consumer's health and safety (e.g., side effects of pharmaceuticals)	• Responsible marketing practices (e.g., promoting accurate facts about the product) • Product labeling (e.g., nutrition facts) • Licensed, certified or authorized retailers (e.g., pharmacists) • Focus groups
NGOs and communities Hold entities accountable for impacts on their interest groups (e.g., environment, society)	• Entity's approach for mitigating against negative impacts to NGO interests (e.g., deforestation from palm oil extraction) • Understanding of how the entity benefits the local and global environment and society (e.g., volunteer hours, employee monetary contributions to cancer research)	• Annual general meeting of shareholders • Integrated report • Sustainability report • Website • One-on-one engagement or facilitated stakeholder meetings

Chapter 2 describes how an ESG materiality assessment and stakeholder engagement can provide insights into these issues and the potential risks that may arise. For some companies, particularly those in the extractives industries, failing to understand, engage and report on ESG issues or risks can exacerbate a risk or be a risk itself. A *Harvard Business Review* article documented a study of 19 publicly traded junior[a] gold-mining companies for which one-third of their market capitalization was found to be a function of their stakeholder relations. The article stated that refusing to engage with disagreeable protesters or activists is not always an effective strategy for managing social risk. The authors recommend establishing a process to understand the concerns and objectives of those opposing business activities rather than withdrawing, disengaging or refusing to comment.[8]

The example below details the California Public Employees' Retirement Systems (CalPERS) approach to understanding stakeholder needs and integrating this into decision-making and reporting.

CalPERS engages stakeholders to understand their most pressing issues

In 2016, the California Public Employees' Retirement Systems (CalPERS) conducted an external stakeholder engagement to inform its upcoming strategic plan as well as identify challenges that may threaten the organization or present barriers to reaching its goals and objectives.

CalPERS met with a variety of stakeholders, including employer associations, labor associations, pension funds and state legislatures. From this engagement, CalPERS identified multiple areas for improving its approach to engagement, such as being more aggressive on health care purchasing to reduce costs and improve access to quality health care. The stakeholders also identified key challenges, including threats to cybersecurity and the rising cost of health care.[9] These concerns were incorporated in CalPERS' new strategic plan, which was then communicated back out to stakeholders.[10]

[a] A junior mining company is small company that is developing or seeking to develop a natural resource deposit or field.

Many voluntary frameworks have been developed and are widely used to meet the ESG-related reporting needs of external stakeholders. Table 5.3 details some of the guidance used to support the disclosure of ESG-related risks and the organization's management of those issues.

Table 5.3: Existing guidance to support external ESG-related risk disclosures

Framework	Addresses financial filings, annual reports or ESG-specific reports[b]	Description
CDSB Framework	Financial filings and annual reports	• Recommends reporting requirements for disclosing environmental information in mainstream reports where that information is material to an understanding of companies' financial risks and opportunities, as well as the resilience of their business models • Aligns with TCFD recommendations[11]
GRI	ESG-specific reports	• Provides a widely adopted framework for reporting material economic, environmental, social and governance issues • Advises reporting on topics that present risks to a company's business model or reputation[12]
<IR> Framework	Annual reports	• Provides a framework for integrated reporting on all six capitals (i.e., financial, manufactured, intellectual, human, social and relationship, and natural) • Advises entities to disclose the specific risks that affect the ability to create value over the short, medium and long term and how the organization manages them[13]
Recommendations of the TCFD	Financial filings	• Recommends voluntary disclosures for companies to report on governance, risk management and impacts of climate change on the organization • Includes industry-specific guidance[14]
SASB Implementation Guide and Reporting Guidelines	Financial filings	• Provides a framework for management to assess financial materiality[c] of sustainability issues, considering risk, for inclusion in financial reports • Recommends minimum disclosure requirements by sustainability issue • Includes industry-specific guidance[15]
Sustainable Development Goals[16]	ESG-specific reports	• Offers goals and targets that organizations can consider in presenting their impacts[16]

[b] ESG-specific reports refer to annual sustainability reports made publicly available.

[c] SASB applies the US Supreme Court definition of materiality which is the "substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available."

The following example shows how Solvay S.A. decided to disclose ESG-related risks to investors.

Solvay S.A. ESG-related risk disclosures[17]

Solvay's disclosures illustrate how companies can disclose their ESG-related risks to investors. As shown in the table below, Solvay discloses climate transition as an emerging risk alongside its other main risks: security, climate-related physical risks, industrial safety, transport accident, ethics and compliance, climate transition risk, cyber risk and chemical product usage. For each of these risks, Solvay provides a description, the corresponding materiality aspects (and UN SDGs where applicable) and prevention and mitigation actions, starting with main actions.

Climate transition – emerging risk (aligned with U.N. SDG 13: Climate Change)	
Description	The lack of a group strategy to address climate-related transition risks (as defined by TCFD), wider environmental challenges, and future resource scarcity could cause damage to Solvay's reputation, business losses, undervaluation and difficulty attracting long-term investors.
Prevention and mitigation	• Solvay's strategy focuses on businesses with higher added value and less environmental exposure. • Every year, the Sustainable Portfolio Management (SPM) tool assesses the environmental exposure of our sales and our innovation projects portfolio. SPM includes climate-related criteria aligned on 2°C scenarios. • The Carbon Intensity action plan has a 40% reduction target for 2025 (reference year 2014).[d]
Main actions	• Appointed an Executive Committee Supervisor for climate and started work on a comprehensive climate strategy roadmap • Launched a new plan and 2020 targets for air emissions (SOx, NOx, VOC), water usage and hazardous waste • Reaffirmed commitment to continuously improve energy efficiency • Improved the CO_2 footprint of energy mix through initiatives such as conversion to biomass firing or renewable electricity sourcing • Reduced GHG emissions released from chemical processing operations • Applied an internal carbon price (€25/metric ton of CO_2e) to GHG emissions in all investment decisions • Included a metric on GHG intensity in senior management remuneration

Quality of reported ESG information

As the growth in mandatory and voluntary ESG reporting continues, entities are realizing that decision-makers using ESG information must have confidence in its relevance and reliability. In fact, 69% of portfolio managers and research analysts believe it is important that ESG disclosures be subject to independent verification.[18] Regardless of whether an entity is obtaining assurance on its ESG information, improving the quality of data is critical for providing accurate data to internal and external decision-makers.

In 2017, 85% of S&P 500 companies issued self-proclaimed "sustainability reports" — more than ever before.[19] Yet frequently, internal stakeholders (e.g., management, staff, board members) and external stakeholders (e.g., investors, analysts, NGOs, regulators) alike still do not have the same level of confidence in the reliability and quality of available sustainability information as compared with historical financial information. For example, 42% of institutional investors have said they find non-financial information is often inconsistent, unavailable or not verified.[20]

Internally and externally reported ESG information requires an appropriate level of internal control to ensure that the information and data is accurate, reliable timely and complete, and is decision-useful. COSO's *Internal Control-Integrated Framework*[21] can support risk management and sustainability practitioners in ensuring that such information is controlled. Table 5.4 sets out data governance considerations that may help to achieve confidence in information and can be applied to all information, including material ESG data.

Guidance

- ☐ Continuously identify opportunities for improving the quality of ESG-related data reported internally and externally

[d] 2017 main actions included: In September 2018, launched a new long-term target committing to reduce its absolute greenhouse gas (GHG) emissions of operations by 1 Mt CO_2 by 2025, compared with the 2017 level, at constant scope, disconnecting its GHG emissions from its growth prospects

Table 5.4: Data governance considerations to support quality ESG information[22]

Internal	External
In reviewing management of key sustainability information for internal reporting, an organization may wish to consider the following factors related to its data governance and management practices: • Does the organization's creation, collection, validation, storage, use, archiving and deletion of sustainability-related data assets adhere to its data governance policy or strategy to support responsible management? • Is relevant, reliable sustainability information integrated into existing management reporting systems, processes and reports? If so, is management actively using this information to run its operations? If not, why not? • Is data lineage (the connection to its original sources) maintained throughout the information systems and supply chain? • Does the organization leverage technology to establish and maintain data lineage, access information and connect to source data? If not, can it readily do so? • Are relevant connections and dependencies maintained/preserved between sustainability information and other types of information? • How often is key sustainability data collected? Can it be collected and reported internally in a timely and cost-effective manner? • When appropriate, is material sustainability information integrated into the key analyses supporting management decisions, such as those related to resource allocation, product development, mergers and acquisitions, compliance and risk management? • Are employee and supply chain partner incentives aligned with the organization's sustainability reporting objectives?	In reviewing data management practices for sustainability-related KPIs specific to external sustainability reporting objectives, an organization may wish to consider the following factors: • Is key sustainability information integrated into existing reporting systems and/or ERP platforms? If not, can it be readily incorporated? Or can effective controls be built around current or other reliable systems and platforms? • Have consistent, formal policies been established across the organization to help ensure reliable sustainability data collection, validation, analysis and reporting/communication? • Has the organization established and communicated clear ownership of and accountability for the collection, validation and reporting/communication of key sustainability information? • Are the organization's sustainability reporting and communication processes well documented, including controls to prevent or detect misstatements? • Have internal audit, the compliance team, the CFO team and/or relevant third parties such as the external assurance provider been engaged to review the quality of key sustainability information, supporting processes and the system of internal control? • Is there confidence in data quality?

Extract from: Leveraging the COSO Internal Control – Integrated Framework to Improve Confidence in Sustainability Performance Data

An increasing number of entities are obtaining independent, third-party assurance statements on their ESG information under the AICPA Attestation Standards or the International Standard on Assurance Engagements (ISAE) 3000. Of the top 250 global entities, more than two-thirds (67%) obtain assurance on ESG information.[23] Entities obtaining assurance on ESG information can choose between two levels of assurance:

- Reasonable assurance that consists of a rigorous examination indicating whether the information is free from material misstatement (considered investor-grade information)
- Limited assurance that consists of more limited procedures that result in a meaningful but lower level of assurance than reasonable assurance

While most entities that seek assurance on their reported ESG information do so on a voluntary basis, requirements for verification and/or assurance are expanding. For example, some regulations involve independent verification of greenhouse gas reporting (e.g., the Accreditation and Verification Regulation of the EU Emissions Trading System (EU ETS)[24] and British Columbia's Greenhouse Gas Emission Reporting Regulation).[25] Others apply to ESG information more broadly. For example, the International Council on Mining & Metals (ICMM)[26] requires its members to obtain assurance on their sustainability reports. Some countries, such as Italy and France, are starting to require assurance with the adoption of the EU's Directive on Non-financial Reporting.[27]

Glossary

Adaptability: The capacity of an entity to adapt and respond to risks.

Actual residual risk: The risk remaining after management has taken action to alter its severity.

Business context: The trends, events, relationships and other factors that may influence, clarify or change an entity's current and future strategy and business objectives.

Business objectives: Those measurable steps the organization takes to achieve its strategy.

Complexity: The scope and nature of a risk to the entity's success.

Core values: The entity's beliefs and ideals about what is good or bad, acceptable or unacceptable, which influence the behavior of the organization.

Corporate governance: The set of relationships between the company's management, board, shareholders and other stakeholders that provide the structure through which objectives of the company are set.

Culture: The attitudes, behaviors and understanding about risk, both positive and negative that influence the decisions of management and personnel and reflect the mission, vision and core values of the organization.

Data: Raw facts that can be collected together to be analyzed, used or referenced.

Dependencies: Resources (e.g., human, social, natural) that businesses need in order to create and sustain value.

Enterprise risk management (ERM): The culture, capabilities and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving and realizing value.

Entity: Any form of for-profit, not-for-profit or governmental body. An entity may be publicly listed, privately owned, owned through a cooperative structure, or any other legal structure.

Environmental, social and governance (ESG):[a] Encompasses the environmental, social and governance issues that are prominent on investors' and other stakeholders' agendas.

ESG-related risks: Commonly referred to as sustainability, non-financial or extra-financial risks, the environmental, social and governance risks and/or opportunities that may impact an entity.[b]

External environment: Anything outside of the entity that influences the ability to achieve strategy and business objectives.

External stakeholders: Any parties not directly engaged in the entity's operations but who are affected by the entity; directly influence the entity's business environment, or influence the entity's reputation, brand and trust.

Extra-financial: A wide range of issues that are likely to have short-, medium- and long-term effect on business performance. Extra-financial issues typically exist beyond the traditional range of variables that are considered as part of investment decision-making processes. Extra-financial factors include, but are not limited to, corporate governance, intellectual capital management, human rights, occupational health and safety and human capital practices, innovation, research and development, customer satisfaction, climate change, and natural resource management, consumer and public health, reputation risk and the broader environmental and social impacts of corporate activity such as biodiversity impacts and community impacts.[c]

Financial capital: The traditional yardstick of performance; includes funds obtained through financing or generated by means of productivity.

Governance: The systems and processes that ensure the overall effectiveness of an entity – whether a business, government or multilateral institution.

Governing body: The process used by an organization to engage relevant stakeholders for the purpose of achieving agreed outcomes (may include board, supervisory board, board of trustees, general partners or owner).

Human capital: The knowledge, skills, competencies and other attributes embodied in individuals that are relevant to economic activity.[d]

[a] KPMG (2017). "ESG, strategy and the long view: A framework for board oversight."
Retrieved from assets.kpmg.com/content/dam/kpmg/lu/pdf/lu-en-esg-strategy-framework-for-board-oversight.pdf

[b] Although these terms are used interchangeably, this 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, which was not previously considered by the organization.

[c] Radley Yeldar. (2012). "The value of extra-financial disclosure: What investors and analysts said." Commissioned by Accounting for Sustainability, GRI and Radley Yeldar. Retrieved from globalreporting.org/resourcelibrary/The-value-of-extra-financial-disclosure.pdf

[d] This is the OECD definition of human capital, which is used in the draft "Social & Human Capital Protocol" due for publication in 2019. This definition of human capital is similar to that used by the <IR> Framework, which is defined as "people's competencies, capabilities and experience, and their motivations to innovate."

Impact: The result or effect of a risk. There may be a range of possible impacts associated with a risk. The impact of a risk may be positive or negative relative to the entity's strategy or business objectives.

Information: Processed, organized and structured data concerning a particular fact or circumstance.

Inherent risk: The risk to an entity in the absence of any direct or focused actions by management to alter its severity.

Integrated thinking: The active consideration by an organization of the relationships between its various operating and functional units and the capitals that the organization uses or affects. Integrated thinking leads to integrated decision-making and actions that consider the creation of value over the short, medium and long term.

Intellectual capital: Accounts for the intangibles associated with brand and reputation, in addition to patents, copyrights, organizational systems and related procedures.

Internal control: A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance. (For more discussion, see Internal Control—Integrated Framework.)

Internal environment: Anything inside of the entity that influences the ability to achieve strategy and business objectives.

Internal stakeholders: Parties working within the entity such as employees, management and the board.

Likelihood: The possibility that a given event will occur.

Megatrends: Large, transformative global forces that define the future by having far-reaching impact on business, economies, industries, societies and individuals.

Materiality assessment (or ESG materiality assessment): The process of identifying, refining and assessing potential environmental, social and governance issues that could affect your business and/or your stakeholders, and condensing them into a short-list of topics that inform company strategy, targets, and reporting.

Mission: The entity's core purpose, which establishes what it wants to accomplish and why it exists.

Natural capital: The stock of renewable and non-renewable natural resources (e.g., plants, animals, air, water, soils, minerals) that combine to yield a flow of benefits to people.[e]

Non-financial: According to the EU Non-Financial Reporting Directive on non-financial risks, includes environmental matters, social and employee aspects, respect for human rights, anti-corruption and bribery issues and diversity on boards of directors.

Operating structure: The way the entity organizes and carries out its day-to-day operations.

Opportunity: An action or potential action that creates or alters goals or approaches for creating, preserving and realizing value.

Organization: The term used to collectively describe the board of directors, management and other personnel of an entity.

Organizational sustainability: The ability of an entity to withstand the impact of large-scale events.

Performance management: The measurement of efforts to achieve or exceed the strategy and business objectives.

Persistence: How long a risk impacts an entity.

Portfolio view: A composite view of risk the entity faces, which positions management and the board to consider the types, severity and interdependencies of risks and how they may affect the entity's performance relative to its strategy and business objectives.

Recovery: The capacity of an entity to return to tolerance.

Risk: The possibility that events will occur and affect the achievement of strategy and business objectives. NOTE: "Risks" (plural) refers to one or more potential events that may affect the achievement of objectives. "Risk" (singular) refers to all potential events collectively that may affect the achievement of objectives.

Risk appetite: The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.

Risk capacity: The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives.

[e] This definition was obtained from the Natural Capital Coalition's "Natural Capital Protocol." This definition is similar to that used by the <IR> Framework, which is defined as "all renewable and nonrenewable environmental resources and processes that provide goods or services that support the past, current or future prosperity of an organization."

Risk inventory: All risks that could impact an entity.

Risk management practitioner: For the purposes of this guidance, includes those with a direct role in the ERM, however, the guidance is applicable to anyone with responsibilities to manage risk (including operational management, risk owners, line management).

Risk profile: A composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity and interdependencies of risks and how they may affect performance relative to the strategy and business objectives.

Severity: A measurement of considerations such as the likelihood and impact of events or the time it takes to recover from events.

Speed of onset or velocity: The time it takes for a risk event to manifest itself or the time that elapses between the occurrence of an event and the point at which the company first feels its effects.

Social and relationship capital: Networks together with shared norms, values and understandings that facilitate cooperation within or among groups.[f]

Stakeholders: Parties that have a genuine or vested interest in the entity.

Stakeholder engagement: The process used by an organization to engage relevant stakeholders for the purpose of achieving agreed outcome.

Strategy: The organization's plan to achieve its mission and vision and apply its core values.

Sustainability:[g] A business approach that creates long-term shareholder value by embracing opportunities and managing risks deriving from economic, environmental and social developments.

Sustainability practitioner: For the purposes of this guidance, sustainability practitioners primarily include those with a direct role in a sustainability function; however, the guidance is relevant to anyone impacted by ESG-related considerations.

SWOT analysis: Uses a two-by-two framework to define the strengths, weaknesses, opportunities and threats a company is facing.

Target residual risk: The amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.

Tolerance: The boundaries of acceptable variation in performance related to achieving business objectives.

Uncertainty: The state of not knowing how or whether potential events may manifest.

Vision: The entity's aspirations for its future state or what the organization aims to achieve over time.

[f] This is the OECD definition of social capital which is used in the draft "Social & Human Capital Protocol" due for publication in 2019. This definition is similar to that used by the <IR> Framework, which is defined as "the institutions and the relationships within and between communities, groups of stakeholders and other networks, and the ability to share information to enhance individual and collective well-being."

[g] RobecoSAM. "Corporate Sustainability." Retrieved from sustainability-indices.com/sustainability-assessment/corporate-sustainability.jsp

Acknowledgements

World Business Council for Sustainable Development

Principal Contributors

- Rodney Irwin, Managing Director of Redefining Value & Education
- Mario Abela, Director of Redefining Value
- Lois Guthrie, Director, Redefining Value
- Eva Zabey, Director, Redefining Value
- Juliet Taylor, Manager Redefining Value and Climate & Energy
- Eleanor Leach, Associate, Redefining Value
- Austin Kennedy, Associate, Redefining Value

EY

Principal Contributors

- Velislava Ivanova, EY Americas Leader Climate Change & Sustainability Services
- Brendan LeBlanc, Partner
- Craig Faris, Consultant Risk Advisory Services
- Rich Goode, Executive Director
- Lauren Rogge, Senior Manager
- Anne Munaretto, Senior Manager
- Margaret Weidner, Manager
- Susan Bailey, Senior Consultant

We would like to express our sincere thanks to the following:

- The generosity of the Gordon and Betty Moore Foundation
- The Advisory Committee who helped with feedback from the public consultation period:
  - Co-chair, Rodney Irwin, World Business Council for Sustainable Development (WBCSD), Managing Director of Redefining Value & Education
  - Co-chair, Sandra Richtermeyer, Dean - Manning School of Business University of Massachusetts Lowell
  - Paul Sobel, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Chairman
  - Desiré Carroll, American Institute of CPAs (AICPA), Senior Manager
  - Sarah Ovuka, Financial Executives International (FEI), Professional Accounting Fellow
  - Geneva Claesson, Partner, Sustainability & Climate Change, Deloitte LLP
  - Rick Funston, Funston Advisory Services LLC, Managing Partner
  - Robert Hirth, Protiviti Inc., Sr. Managing Director, and COSO Chair emeritus
  - Krisann Kleibacker Lee, Cargill, Inc., Senior Lawyer
  - Geoff Lane, PricewaterhouseCoopers (PwC), Partner Sustainability and Climate Change
  - Randy Miller, Funston Advisory Services LLC, Principal
  - Sreeparna Mitra, EY, Principal Advisory Services
  - Bill Murphy, KPMG, Partner, Governance Risk & Assurance Services and Canadian Leader, Sustainability Services
  - Lucy Nottingham, Marsh & McLennan Companies, Inc., Director, Global Risk Center
  - Gloria Santona, Baker McKenzie, Of Counsel
  - Mark Weick, The Dow Chemical Company, Lead Director, Sustainability and Enterprise Risk Management

- We would like to thank the representatives from the following companies that participated in the interviews, surveys and workshops that influenced this publication:
  - Aditya Birla Group
  - Akipeo Inc.
  - CLP Holdings Limited (CLP)
  - The Dow Chemical Company
  - Eastman Chemical Company
  - EDP - Energias de Portugal, S.A
  - Eni S.p.A.
  - Environmental Resources Management Limited (ERM)
  - Eskom SA
  - Givaudan International SA
  - Hankook Tire Co. Ltd.
  - Hitachi Ltd.
  - Infosys Limited
  - Institute and Faculty of Actuaries (IFoA)
  - Insurance Institute of Switzerland (IIS)
  - Mitsubishi Corporation
  - Monsanto Company[a]
  - Nestlé S.A.
  - NYU Stern, Center for Sustainable Business
  - Olam International Ltd.
  - Royal Philips N.V.
  - Saudi Basic Industries Corp. (SABIC)
  - Siam Cement Group Public Company Limited (SCG)
  - State Street Global Advisors (SSGA)
  - Stora Enso
  - Sumitomo Chemical Company Ltd.
- Representatives from the WBCSD member companies that participated in the risk management sessions at the Liaison Delegate meetings in Montreux, Switzerland (April 2017) and Mexico City (October 2017)
- Sergio Analco | Branding + Design for his work on the design and production of this document

About the World Business Council for Sustainable Development (WBCSD)

The World Business Council for Sustainable Development (WBCSD) is a global, CEO-led organization of over 200 leading businesses working together to accelerate the transition to a sustainable world. We help make our member companies more successful and sustainable by focusing on the maximum positive impact for shareholders, the environment and societies. Our member companies come from all business sectors and all major economies, representing a combined revenue of more than USD$8.5 trillion and with 19 million employees. Our Global Network of almost 70 national business councils gives our members unparalleled reach across the globe. WBCSD is uniquely positioned to work with member companies along and across value chains to deliver high-impact business solutions to the most challenging sustainability issues. wbcsd.org

About the Committee of Sponsoring Organizations of the Treadway Commission (COSO)

This project was supported by the COSO, which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is private sector initiative, jointly sponsored and funded by:

- American Accounting Association (AAA)
- American Institute of CPAs (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- The Institute of Internal Auditors (IIA)

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities. 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. For more information about our organization, please visit ey.com.

[a] Monsanto Company was acquired by Bayer AG on June 7, 2018, and is now an indirect wholly-owned subsidiary of Bayer AG.

Appendices

Appendix I: Project background and approach for developing the guidance

The business case for integrating ESG into ERM

In January 2017, WBCSD published a report, *Sustainability and enterprise risk management: the first step towards integration*, examining the state of integration of ESG-related risks and ERM.[1] The report compared the sustainability and risk disclosures of 170 WBCSD member companies, and found that, on average, only 29% of the areas deemed to be "material" in a sustainability report were disclosed in a company's legal risk filing. Notably, 35% of member companies did not disclose *any* of the sustainability risks (i.e., ESG-related risk) identified in their sustainability reports in their legal filings.[a]

Discussions and surveys revealed that more than 70% of risk management and sustainability practitioners believed that "risk management practices [were] not adequately addressing sustainability risks." Practitioners pointed to a range of internal organizational forces and innate features of sustainability risks impacting the effective management of sustainability risks. Of these, the most prominent reasons included:[b]

- Some companies have limited knowledge of sustainability, which inhibits the capture of emerging sustainability risks.
- Sustainability risks are often more challenging to quantify than traditional risks.
- The sustainability risk outlook timeline is longer than that of traditional risks.
- Sustainability reports and mainstream corporate risk disclosures have different audiences and purposes.

COSO and WBCSD Collaboration

In April 2017, recognizing the benefits of mutual cooperation to their respective members and for business in general, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the World Business Council for Sustainable Development (WBCSD) signed a Memorandum of Understanding (MoU) aimed at working together to help businesses identify and prioritize issues related to sustainability and enterprise risk management.

The result of this collaboration is this guidance, designed to support entities in applying enterprise risk management to environmental, social and governance-related risks.

The guidance: *Applying enterprise risk management to environmental, social and governance-related risks*

WBCSD led the development of the guidance, supported by the COSO Board and EY as a principal contributor. The guidance development team collaborated with risk management and sustainability practitioners to gain insights into current challenges and support development of content, case studies and examples for the preliminary draft. The preliminary draft guidance was released in February 2018.

From February 7 to June 30, 2018, COSO and WBCSD conducted a public consultation process on the preliminary draft guidance. Through formal feedback letters, an online survey and emails, more than 40 respondents from academia, non-governmental organizations, reporting organizations, intergovernmental organizations, practitioners, professional organizations and professional services firms and consultancies provided input for updating the guidance. An advisory committee was established comprised of 16 risk management and sustainability practitioners, professional services and sponsoring organizations to support the consultation process.

The guidance development project team reviewed all comments received, considered the merits of feedback and opinions and debated and agreed modifications at an in-person meeting with the advisory committee. An updated draft capturing this input was approved by WBCSD and COSO.

[a] WBCSD expanded this research to 369 companies in 2017 and found similar results. The results showed that 31% of the material sustainability issues were disclosed to investors as risks factors. Further, 31% of companies had no alignment between the risk deemed "material" in the sustainability report and the legal filing.

[b] Prominence determined based on level of agreement of interviewees and sustainability professional feedback from the Pathways to Impact Conference.

Appendix II: Examples of risk and governance disclosure requirements

Many countries and stock exchanges establish annual reporting requirements for companies to disclose information related to potential risk factors, including ESG-related risks, and governance practices. An analysis was conducted in 2017 to identify disclosure requirements of 15 countries selected based on gross domestic product (GDP), company disclosure practices and geographic location. Both national laws and stock exchange[c] requirements were assessed.

The analysis revealed that 13 of 15 countries analyzed required annual risk factor disclosures, either through national laws or stock exchange-specific requirements. Eight of these 13 countries explicitly identified at least one environmental, social or governance component that should be considered in preparing risk factor disclosures. Furthermore, 14 of 15 countries required annual governance disclosures through country laws or stock exchange requirements.

Risk disclosure requirements, including specific requirements related to ESG matters, are presented below in Table II.1. Governance disclosure requirements are presented in Table II.2.

Table II.1 Risk disclosure requirements[d]

Jurisdiction	Requirements	Authoritative literature	
Country	**Risk factor disclosure[e]**	**ESG-specific risk factor disclosure[f]**	**Example citations**
Australia	Yes	Yes	Australian stock exchange (ASX) Corporate Governance Council Principles & Recommendations: Principle 7 (recommendation 7.4)
Brazil	Yes	No	Chairperson of the Securities Commission of Brazil (CVM) Instruction No. 480
Canada	Yes	Yes	Form 51-102F2, Annual Information Form, Section 5.2; Form 51-102F1, Management's Discussion and Analysis, Section 1.2
China	No	No	
France	Yes	Yes	Article L225-100; Article L225-100-2
Germany	Yes	Yes	Commercial Code / Corporate law (HGB), §§289, 289a-e HGB, 315, 315a-c HGB
India	Yes	Yes	Companies Act 2013, Section 134. Financial statement, (3)
Japan	Yes	No	Financial Instruments and Exchange Act (FIEFA), Articles 5, 24 Cabinet Office Ordinance on the Disclosure of Corporate Affairs (Cabinet Ordinance); Article 8(1), Article 15/Form 2 33; Form 3 13
Netherlands	Yes	Yes	Dutch Civil Code, Book 2 Legal Persons, Title 9 financial statements and directors' report; Financial Supervision Act; Dutch Corporate Governance Code (December 8, 2016) of the Monitoring Committee
Norway	Yes	No	Norwegian Act on Securities Trading 2007: Section 5-5 Annual financial reports; Norwegian Accounting Act, Section 3
Singapore	No	No	
South Africa	Yes	No	King IV Report on Corporate Governance for South Africa 2016: Principle 11
Thailand	Yes	No	Regulations of the Stock Exchange of Thailand. Re: Preparation and Submission of Financial statements, Financial reports and Operating results of Listed Companies
UK	Yes	Yes	Companies Act 2006 c. 46 Part 15 CHAPTER 4A, Section 414C(2)(b), 414C(4)(b), 414C(7), 414CB(1)(2)(d)
USA	Yes	Yes	17 CFR 229.503; SEC Regulation S-K guidance, SS 229.503 (c); Item 303(a)(3)(ii)

[c] In cases where there exist multiple stock exchanges within a country, the top two largest stock exchanges were included in the analysis.

[d] Note: The EU has issued the non-financial reporting directive, (Directive 2014/95/EU), which mandates large companies to report on policies related to the environment, social responsibility, human rights, anti-corruption/bribery, and diversity in relation to boards and the disclosure of ESG-related risks. EU Member States have adopted it as part of country law. For more information on this directive, refer to: ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en

[e] Annual requirement to publicly disclose risk factors that exceed a specified threshold

[f] Requirements specify considering at least one environmental, social or governance-related risk in selecting risk factors for annual disclosure.

Table II.2 Governance disclosure requirements

Jurisdiction	Requirements	Authoritative literature
Country	**Specific governance disclosure requirement?**[9]	**Example citations**
Australia	Yes	Australia Corporations Act 2001, Volume 1, Chapter 2D, 2G, 2H, 2J
Brazil	No	
Canada	Yes	Canada Business Corporations Act: Part 5, Part 7, Part 8; National Instrument 58-101; National policy 58-201
China	Yes	Code of Corporate Governance for Listed Companies in China
France	Yes	French Commercial Code, Articles L. 225-37-2 to L. 225-37-5
Germany	Yes	German Commercial Code, Section 289F, Corporate Governance Statement
India	Yes	Securities and Exchange Board of India Regulations, 2015, Section 34, Chapter II
Japan	Yes	Financial Instruments and Exchange Act (FIEFA), Articles 5, 24 Cabinet Office Ordinance on the Disclosure of Corporate Affairs (Cabinet Ordinance); Article 8(1), Article 15/Form 2 57; Form 3 37
Netherlands	Yes	Dutch Corporate Governance Code (December 8, 2016) of the Monitoring Committee
Norway	Yes	Norwegian Accounting Act, Section 3-3c
Singapore	Yes	Singapore Companies Act (2006); Singapore Exchange Listing Rules, Report of the Committee and Code of Corporate Governance
South Africa	Yes	Companies Act 2008: Part F - Governance of Companies
Thailand	Yes	Corporate Governance Code for Listed Companies 2017
UK	Yes	Companies Act 2006 c. 46 Part 15 Chapter 5, Sections 416 (1), (3); 418 (2), 419A; Disclosure and Transparency Rules of the Financial Conduct Authority, DTR 7.1, 7.2
USA	Yes	SEC Regulation S-K, 17 CFR §229.407

[9] Annual requirement to disclose information related to company governance practices, such as the organization of executive bodies and ethics procedures for management.

Appendix III: Example voluntary frameworks and commitments

The following is a selection of voluntary frameworks, standards and commitments that can serve as a starting point for mapping voluntary ESG requirements of the entity.

Table 1.3: Example voluntary frameworks and commitments

Framework or codes	Governing body	Expectation	How framework addresses ESG and governance
B-Corp[2]	B Lab	Certification	For-profit companies certified by the nonprofit B Lab must meet standards of social and environmental performance, accountability and transparency.
CDSB Framework for reporting environmental information, natural capital and associated business impacts[3]	Climate Disclosure Standards Board (CDSB)	Guidance/ alignment	Sets out an approach to reporting environmental information in mainstream reports where that information is material to an understanding of companies' financial risks and opportunities, as well as the resilience of their business models.
Ceres Principles[4]	Ceres	Guidance/ alignment	Guidelines formalizing companies' dedication to environmental awareness and accountability as well as active commitment to the ongoing process of continuous improvement, dialogue and comprehensive, systematic public reporting.
Equator Principles[5]	Association of member Equator Principles Financial Institutions	Signatory/ membership	Financial institutions perform annual reporting to the Equator Principles Association asserting their adoption of a risk management process for determining, assessing and managing environmental and social risk in projects.
Global Reporting Initiative (GRI)[6]	Global Sustainability Standards Board	Guidance/ alignment	Codified global standards for sustainability reporting.
IFC Performance Standards[7]	International Finance Corporation (IFC)	Policy/ standard	Define IFC client responsibilities for managing ESG risks across 8 categories (Risk, Labor, Resource Efficiency, Community, Land Resettlement, Biodiversity, Indigenous People and Cultural Heritage).
International Integrated Reporting Council (IIRC)[8]	Global coalition of regulators, investors, etc.	Guidance/ alignment	Principles and frameworks for integrated reporting, which includes a broad base of capitals, to create long-term value.
Luxembourg Finance Labelling Agency (LuxFLAG)[9]	LuxFLAG	Labelling	Agency aiming to promote the raising of capital for the Responsible Investment sector by awarding a recognizable label to eligible investment vehicles. Its objective is to reassure investors that the applicant invests, directly or indirectly, in the Responsible Investment sector.
Natural Capital Protocol[10]	Natural Capital Coalition	Guidance/ alignment	A framework designed to help generate trusted, credible, and actionable information that business managers need to inform decisions. The Protocol aims to support better decisions by including how we interact with nature, or more specifically natural capital, in decision making.
OECD Guidelines for Multinational Enterprises[11]	Organisation for Economic Co-operation and Development (OECD)	Guidance/ alignment	Recommendations from governments to multinational enterprises in the form of non-binding principles and standards for responsible business conduct in a global context consistent with international laws and standards.
Principles for Responsible Investment[12]	United Nations	Signatory	CEO-level commitment for institutional investors to incorporate ESG factors into investment and ownership decisions.
SASB Conceptual Framework (CF)[13] and Standards (S)[14]	Sustainability Accounting Standards Board	Guidance/ alignment	Industry-specific financially material sustainability topics and metrics designed to ensure the delivery of material, decision-useful ESG information to the capital markets in a way that is cost effective.
Social & Human Capital Protocol[15,h]	Social & Human Capital Coalition	Guidance/ alignment	Contributes to the vision of mainstreaming the measurement of social and human impacts by providing a consistent process to guide companies through the journey of measuring, valuing and better managing social and human capital and providing a framework for collaborative action towards harmonized and standardized approaches.
Sustainable Development Goals[16]	United Nations	Guidance/ alignment	Set of 17 Global Goals with 169 targets covering a broad range of sustainable development issues to which companies can align.
Task Force for Climate-Related Disclosures[17]	Financial Stability Board	Guidance/ alignment	Guidance on voluntary climate-related financial disclosures focused on governance, strategy, risk management and metrics and targets.
UN Global Compact[18]	United Nations	Signatory/ membership	CEO-level commitment to ten principles focused on human rights, labor, environment and anti-corruption.
UN Guiding Principles on Business and Human Rights[19]	United Nations	Guidance/ alignment	Guidelines to advance human rights in business and eradicate abuse, specifically focusing on corporate transparency and accountability.
UNEP Finance Initiative Principles for Sustainable Insurance[20]	United Nations	Guidance/ alignment	Global framework for the insurance industry to address ESG risks and opportunities.

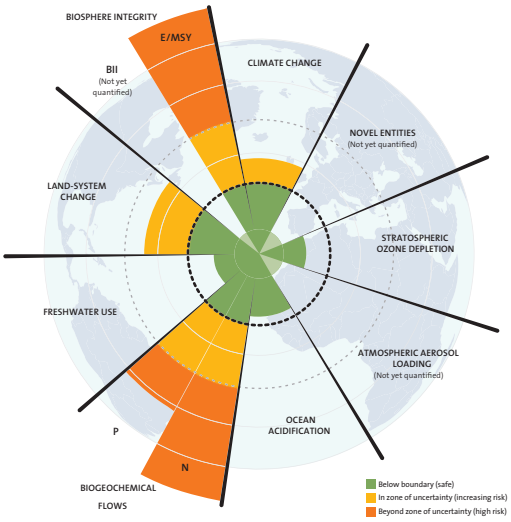
[h] The final Social & Human Capital Protocol is due for final publication in 2019.

Appendix IV: Additional ESG-specific resources for understanding the business context[21]

(Extracted from the Embedding Project – The Road to Context: Contextualising Your Strategy and Goals)The

Planetary boundaries framework

The Planetary Boundaries framework, developed by Johan Rockström and colleagues, identifies nine tightly coupled processes that regulate the stability and resilience of the Earth's ecological system boundaries and, for each of these systems, attempts to quantify the boundaries at which human survival is threatened.[22] Several companies have found that the framework helps to introduce the idea of "thresholds" that have the potential to create real strategic constraints as they limit access to resources or increase weather-related risks. The framework has also been useful in sparking a conversation about the limits to growth. As these conversations progress, however, some of the issues will need to be reframed from planetary boundaries into thresholds. For instance, in many cases, it is a challenge to discuss a planetary boundary for water. Instead, companies will need to contemplate watershed level and even seasonal thresholds for water quantity and water quality in the areas where they operate. Nevertheless, at early stages, this framework can provide a strong conceptual anchor point.



Credits: Azote images for Stockholm Resilience Centre

Adapted from stockholmresilience.org/research/planetary-boundaries/planetary-boundaries/about-the-research/the-nine-planetary-boundaries.html

The doughnut of social and planetary boundaries

While the Planetary Boundaries framework focuses primarily on environmental thresholds, Kate Raworth has proposed The Doughnut model that adds an inner ring (The Social Foundation) to the Planetary Boundaries framework. Together with the Planetary Boundaries framework, this can be useful in helping to introduce the role companies play in maintaining and enhancing social resilience or conversely, how their actions contribute to social instability in the regions where they operate.

Appendix V: Example responsible, accountable, consulted, informed (RACI) matrix

The following is an example of a RACI matrix highlighting some common roles within an organization and their involvement throughout the ERM process.

ERM components		Board and sub-committee	Executive committee	ERM Director or CRO	Risk owners (includes sustainability for ESG-specific risks)	Sustainability practitioners
Governance and Culture		Accountable for setting the tone for governance, culture and risk appetite	Responsible for design and facilitation of the end-to-end ERM process	Responsible for design and facilitation of the end-to-end ERM process and lifecycle	Informed of the ERM process to support management of ESG issues	Informed of the governance model and process to support management of ESG issues
Strategy and Objective-Setting		Consulted and made aware of significant changes to the internal and external environment	Accountable for setting the business strategy, objectives and risk appetite	Responsible for facilitating the process for examining the business context and strategy	Consulted on the internal and external changes to identify shifts that may result in risks	Consulted on the internal and external changes and ESG-related impacts and dependencies
Performance	**Identify risks that will impact the business strategy and objectives**	Consulted and made aware of the critical risks impacting the strategy and approve selected risk responses	Accountable for identifying and disclosing the material risks that will impact the business strategy	Responsible for facilitating the process for identifying business impacts	Responsible for supporting risk identification and understanding	Consult with risk owners to support identification and understanding of ESG-related risks
	Assess and prioritize the severity of identified risks		Accountable for assessing and prioritizing key risks and opportunities	Responsible for leveraging tools for risk assessment and prioritization	Responsible for assessing the risk severity on the business and strategy	Consult with risk owners on the tools and knowledge to support quantification and prioritization of ESG-related risks
	Develop and implement responses to prioritized risks		Accountable for appropriate allocation of resources to manage prioritized risks	Responsible for coordinating the development of risk responses for each risk area	Responsible for developing appropriate responses to address the risk and implement the response	Consult with risk owners to develop responses to prioritized risks
Review and Revision		Consulted on the status of risks and the ERM process	Accountable for monitoring the ERM activities and ensuring risks stay within the company risk appetite	Responsible for developing a consolidated view of metrics to monitor risks	Responsible for developing metrics to monitor risks and business context for when the risk shifts outside tolerance levels	Consulted on appropriate metrics for monitoring ESG-related risks and determine aspects to report on to internal and external stakeholders
Information, Communication and Reporting		Consulted on ERM activities and processes disclosed externally	Accountable for communications of ERM activities and processes internally and externally	Responsible for developing internal and external communications on ERM activities and processes	Responsible for providing inputs for internal and external communications on ERM activities and processes	Consulted on the inputs for internal and external communications on ESG-related aspects of ERM activities and processes

Appendix VI: Example precedent event reference table

This table is designed as a starting point for companies to consider events that have occurred at other companies as data inputs for forecasting models. The references here provide an overview of the event and impact. Further research and comparability to the company's specific circumstances would be required.

ESG risks	Reference to example precedent events	Impact
Environmental		
Severe weather	• Impact of catastrophic flooding and drought on cotton crop yields and price (2010)[23]	• Next clothing brand had to raise prices 5%-8% • H&M share prices fell 2.5%[24]
	• Impact of Texas drought and China's adverse weather conditions on cotton crop (2011)	• Gap lowered its annual profit forecast by 22% during its Q1 2011 update due in part to cotton prices. • Polo Ralph Lauren posted a 36% decline in net income in the first quarter, citing higher input costs as the primary driver[25]
	• Impact of coastal wetlands in northeastern USA on regional flood damages by Hurricane Sandy and local annual flood losses in New Jersey (2012)	• The presence of wetlands helped avoid USD$625 million in direct flood damages[26]
Water contamination	• Oil spill in the Gulf of Mexico (2010)	• As of 2018, BP had paid more than USD$65 billion in clean-up costs and legal fees linked to the largest environmental disaster in U.S. history where 11 rig workers were killed[27]
	• Allowance of water contamination from hydraulic fracturing	• Cabot Oil and Gas paid USD$4.2 million to two families for contaminating their water[28]
	• Spill of coal ash waste (2015)	• Duke Energy Corp agreed to pay USD$102 million in federal penalties: USD$68 million in fines and USD$34 million for environmental and conservation efforts in North Carolina and Virginia[29]
Water scarcity	• Groundwater extraction above legal limits	• Coca-Cola was forced to close its bottling factory where it produced 600 polyethylene terephthalate (PET) bottles of soft drinks per minute[30]
Biodiversity	• Violations of national law on biodiversity in Brazil (2017)	• 35 different companies (mostly cosmetic and pharmaceutical multinationals) were found responsible, totaling about USD$44 million in fines[31]
	• Restoration of biodiversity, nature and landscapes (French National Assembly bill)	• Any act committed by an individual is punishable by a fine of up to 150,000 euros (750,000 euros for an organized group) and two years' imprisonment[32]
Social		
Human rights	• Poor worker conditions in factories (1990's and early 2000's)	• Nike's defense of these claims resulted in a settlement payment of USD$1.5 million[33,34]
	• Workers being paid less than the legal minimum wage	• 7-Eleven paid at least USD$26 million in back pay to 680 workers[35]
Labor rights	• Employee strike for labor rights improvements	• A major, world-class mining project with capital expenditure of USD$3-$5 billion will suffer costs of roughly USD $20 million per week of delayed production in Net Present Value (NPV) terms, largely due to lost sales[36]
Occupational health and safety	• Workplace-related injuries, illnesses and deaths	• The following studies report average direct and indirect costs: - National Safety Council Injury Facts[37] - PBS Costs of Occupational Injuries and Illnesses (US-specific)[38]
	• Factory collapse resulting in over 1,100 workers killed and 1,000 injured	• The International Labor Organization raised USD$15 million of the USD$40 million target to compensate impacted families of the Rana Plaza factory collapse[39]
Community	• Dam collapse killing 19 people and sending iron ore mining debris through a southeast region of Brazil	• Samarco (Value and BHP) paid USD$6.2 billion settlement[40]
Food safety	• Food contamination led to E. coli (2015)[41]	• Chipotle's stock price, which was increasing at the time, fell from USD$750 per share to USD$440 per share over a six-month period[42]
	• Pet food contamination resulted in dog deaths (2014)[43]	• Petco halted the sale of Chinese-made dog treats, which impacted 1,300 stores and sales on Petco.com[44]
Product safety	• Lithium ion batteries caught fire (2006)	• Dell/Sony recalled 4.1 million batteries at a cost of USD$400 million[45]
	• Lead paint on children's toys (2007)	• Mattel recalled 967,000 toys, its 17th recall in ten years[46]
	• Delay of reporting ignition switch defect (2014)	• The National Highway Traffic Safety Administration charged GM with USD$35 million in civil penalties[47]
	• Overheating and catching fire of cell phones (2016)	• Samsung issued an initial recall of 2.5 million devices[48]
Consumer safety	• Lack of oversight for trading operations (2013)	• JPMorgan Chase generated about USD$6 billion in losses due to complex derivatives • It agreed to pay USD$920 million in fines to regulators[49]
Governance		
Bribery and corruption	• Bribery payments	• Criminal and civil penalties are imposed on companies for offenses defined by the US Foreign Corrupt Practices Act[50] • In 2016, the Serious Fraud Office secured its first conviction under the section 7 of the UK Bribery Act 2010 which resulted in a financial penalty of about USD$2.7 million[51]
Falsification of emissions tests	• Falsification of emissions tests on vehicles (2016)	• As of 2018, Volkswagen has paid U.S. authorities USD$25 billion in fines, penalties and restitution[52]

Appendix VII: Scenario analysis reference table

The resources included in the table below provide insights for developing climate change and energy focused scenario analyses. Managers should consider these resources for the principles and methodologies that can apply to other ESG-related risks.

Resources	Applicable use
TCFD Technical Supplement: The Use of Scenario Analysis in Disclosure of Climate-Related Risks and Opportunities[53]	• Describes how to build climate change scenarios that are plausible, distinctive, consistent, relevant and challenging • The parameters, assumptions, analytical choice and impacts walk managers through the key considerations for developing scenarios
IEA[54]	• Provides new and current policy scenarios based on plans announced by countries on energy and their implementation • Designs energy technology scenarios for limiting greenhouse gas emissions based on 2-, 4- and 6- degree scenarios
IPCC[55]	• Special Report on Emissions Scenarios (SRES) covers a wide range of the main driving forces of future emissions, from demographic to technological and economic developments • These scenarios include the range of emissions of all relevant sources of greenhouse gases and sulfur and their driving forces
Shell[56]	• Scenarios developed annually for a range of issues, including how the world could meet energy demand while reducing net carbon emissions to zero and energy scenarios for the future • The purpose is to ask "what if" to consider events that may be remote possibilities to stretch thinking
Statoil[57]	• Energy scenarios considering greenhouse gas emissions, global climate policy, energy demand, global oil and gas markets, and renewable energy (2017)
BHP[58]	• Climate change scenario analysis, including in a 2-degree Celsius worldu
ConocoPhillips[59]	• Corporate supply and demand carbon scenario
Glencore[60]	• Climate change scenarios with discussion of assumptions for delayed action, committed action and ambition action
World Resources Institute Aqueduct Water Risk Atlas[61]	• Water risk mapping tool that helps entities identify and assess water risks at a global scale
TCFD Knowledge Hub[62]	• Powered by the Climate Disclosure Standards Board (CDSB) to support businesses implementing the TCFD recommendations • Resources include existing legislation and regulations, frameworks, standards, guidance, research papers, tools and webinars

Appendix VIII: Example of applying ERM to ESG-related risks

This guidance has shown how to apply ERM to ESG-related risks. Consider the example of Pro P&P as a summary of key actions for each chapter. Though this example does not provide an exhaustive list of a company's risks or actions, it is an illustrative example of how risks flow from an organization's strategy and objectives.

Pro Paper & Packaging

Vision and strategy

Pro Paper & Packaging (Pro P&P) will be the **leading paper and packaging business** in Europe, the Americas and the Asia-Pacific region. Pro P&P will be a **committed partner to our customers** with a comprehensive product offering, leveraging our global footprint and scale, **streamlined processes and technology** to drive excellent returns, create value for shareholders and be recognized as a **leader in sustainability** and an employer of choice.

Strategy and objective-setting		Performance			Review and revision	Information, communication and reporting
		Identifies risk	Assesses and prioritizes risk	Implements risk responses		
Objective: Customer focus	• Leveraging scale and brand-based value propositions to be a market leader in Europe, the Americas and Asia-Pacific segments • Supplier of choice with strategic customers	• The possibility that end-user customer preferences for products with less environmental impact and enhanced recycling and reuse properties will challenge long-term contracts with customers, impacting sales, revenue and market leadership	• Severity: Reduced revenue of USD$80 to $100 million per annum by 2022 (with 70% probability) 🟡	• Implements Risk Responses • Invest USD$18 million into research and development for new products that use alternatives to fiber and petroleum as raw materials • Develop a customer engagement tool to maintain an understanding of changing customer preferences, including preferences for sustainable products	• Indicator: Percentage of customers requesting FSC/PEFCx certified products • Threshold: >25% • Decision: Increase investment and resource allocation for procuring certified products	• Internal: Dashboard showing customer requests for FSC/PEFCx certified products; briefing documents showing market demand for products • External: The organization updates its labeling to clarify to customers the use of FSC/PEFCx certified products
Objective: Recognized brand	• Differentiated position driven by brand drivers: - Price competitiveness - Product sustainability - Responsiveness and customer service - Innovation	• The possibility that NGO-related campaigns relating to ESG performance will erode brand recognition as a product with strong sustainability performance	• Severity: Reduced market capitalization of 32% or USD$760 million 🔴	• Establish a grievance process to allow supplier code of conducts violations (e.g., human rights, environmental, safety) to be reported and addressed	• Indicator: Number and size of NGO requests and campaigns against the company • Threshold: Two large campaigns and/or >10% in revenue loss • Decision: - Reassess risk, response and adequacy - Convene a targeted problem-solving session with the NGO	• Internal: Meetings presenting findings of stakeholder engagement activities, results of monitoring NGO requests and campaigns • External: The entity reports the risk in its legal filing – Changing consumer preferences, innovation and competitiveness could hurt our business. It provides information on how the risk is managed by the organization
Objective: Strong growth	• Solidify position in winning segments and customers • Enter into developing markets through channel strategies • Embed merger and acquisitions capability to support growth with acquisitions that focus on innovation, scale and market leadership	• The possibility that geopolitical issues in emerging markets will reduce access to a skilled, efficient and engaged workforce impacting productivity and sales	• Reduced sales revenue of USD$6.5 million for 2018-19 • Increased labor cost of USD$20 million per year from 2019 onward 🟢	• Engage in regular formal and informal training • Conduct monitoring of geopolitical situations in countries of operation and ensure operations are diversified across multiple geographies	• Indicator: Employee turnover • Threshold: >12% • Indicator: Employee absenteeism • Threshold: >4% • Indicator: Reports of employee stress • Threshold: >15% • Decision: Consider on-site employee housing and alternative strategies	• Internal: Briefing documents showing workforce composition in relevant markets, dashboard of indicators and thresholds • External: The organization obtains awards recognizing it as a positive place to work – e.g., lists of best companies to work for in local and global markets
Objective: Operational excellence	• Optimized footprint to support market focus and cost competitiveness • Manufacturing and process excellence • Procurement supporting cost and customer value propositions	• The possibility that severe weather events (e.g., cyclones, floods) will disrupt the supply chain	• Transitional climate-related risks reduce revenue by - Scenario A: USD$70-$100 million loss due to damage, reduced revenue of USD$300 million, increase in insurance premiums of 8%, closure of three facilities - Scenario B: USD$100-150 million loss due to damage, reduced revenue of USD$500 million, increase in insurance premiums of 12%, closure of seven facilities 🟡	• Conduct scenario planning to monitor the impact of changing weather patterns on the supply chain • Conduct business continuity planning to ensure alternative suppliers and operators are in place in the event of a major disruption • Monitor weather changes and events to substitute suppliers as appropriate • Purchase insurance to cover losses in the event of severe weather	• Indicator: Severe weather events • Threshold: 1) Storm severity frequency increases over five years 2) Two category 4 storms occur within any three years • Decision: - Activate alternative sourcing plans - Evaluate alternative pricing scenarios and customer sensitivities for sharing cost impacts	• Internal: Briefing document summarizing scenario analyses, meetings with subject matter resources to understand underlying assumptions and implications for the business • External: Reporting of risk factor in legal filing – Climate change and severe weather events may disrupt our supply chain and access to raw materials. It provides information on how the risk is managed by the organization
Objective: Sustainability leadership	Recognized as: • A global safety leader and zero-injuries workplace • An employer of choice • Continuously improving social and environmental performance across sites through the supply chain and life cycle of products	• The possibility that the safety performance of companies acquired as part of the growth strategy will be sub-standard and lead to impacts on employee morale • The possibility that human rights issues in the supply chain (e.g., forced labor, child labor) will lead to reputational impacts and loss of customers	• Reduced revenue and increased costs of USD$13.6 million are a result of negative impacts on the workforce and production efficiency • Contracts to the value of USD$2.3 million are at risk due to requirements of three customers that their suppliers adopt rigorous code of conduct practices relating to the eradication of human trafficking 🟢	• Develop and implement an externally accredited safety management system and conduct regular audits of company-owned operations • Re-evaluate company M&A due diligence processes to better identify and address ESG-related issues prior to transactions • Develop a human rights policy and implement a monitoring program	• Indicator: Completion of acquired companies' policies and supplier audits on occupational health and safety and human rights • Threshold: <75% • Indicator: Unfavorable audits in acquired company • Threshold: >10% • Decision: - Establish special audit response action team to triage issues and develop urgent responses - Place management of units with poor audit responses on probationary status with financial implications	• Internal: Immediate notification to senior management when injuries or fatalities occur; dashboard for monitoring human rights issues in the supply chain (including policy contents and results of audits) • External: The organization holds meetings with NGOs and local communities regarding its impact to its employees and the local community

Prioritization: 🔴 High 🟡 High-Moderate 🟢 Moderate

References

Introduction

1 MSCI (2018, April). “ESG Ratings Methodology: Executive Summary.” Retrieved from https://www.msci.com/documents/10199/123a2b2b-1395-4aa2-a121-ea14de6d708a

2 Robeco. “ESG definition.” Retrieved from https://www.robeco.com/me/key-strengths/sustainability-investing/glossary/esg-definition.html

3 COSO (2017, June). “Enterprise Risk Management: Integrating with Strategy and Performance.” p. 9

4 Unilever. “Our strategy for sustainable growth.” Retrieved from Unilever: https://www.unilever.com/sustainable-living/our-strategy/

5 Unilever. “Defining our material issues.” Retrieved from Unilever: https://www.unilever.com/sustainable-living/our-approach-to-reporting/defining-our-material-issues/index.html

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

7 Society for Corporate Governance and BrownFlynn (2018, June), “ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals.” p. 6.

8 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

9 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

10 KPMG (2017). “ESG, strategy and the long view: A framework for board oversight.” p. 5

11 Society for Corporate Governance and BrownFlynn (2018, June). “ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals.” p. 10

12 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

13 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

14 “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

15 NASDAQ(2018). “ESG Reporting Guide: A voluntary support program for the Nordic and Baltic markets.” Retrieved from https://business.nasdaq.com/esg-guide

16 TCFD (2017, June). “Recommendations of the Task Force on Climate-related Financial Disclosures.” Retrieved from https://www.fsb-tcfd.org/publications/final-recommendations-report/

17 WBCSD (2017, January 18). “Sustainability and enterprise risk management: the first step towards integration.” Retrieved from WBCSD: http://www.wbcsd.org/Projects/Non-financial-Measurement-and-Valuation/ResourcesSustainability-and-enterprise-risk-management-The-firststep-towards-integration

18 COSO (2017, June). “Enterprise Risk Management: Integrating with Strategy and Performance.” p. 10

19 COSO (2017, June). “Enterprise Risk Management: Integrating with Strategy and Performance.” p. 3

20 COSO (2017, June). “Enterprise Risk Management: Integrating with Strategy and Performance.”

21 MSCI (2018, April). “ESG Ratings Methodology: Executive Summary.” Retrieved from https://www.msci.com/documents/10199/123a2b2b-1395-4aa2-a121-ea14de6d708a

1. Governance and culture for ESG-related risks

1 United Nations Global Compact. “Governance.” Retrieved from https://www.unglobalcompact.org/what-is-gc/our-work/governance

2 COSO (2017, June). “Enterprise Risk Management: Integrating with Strategy and Performance.” p. 27

3 Institute of Directors Southern Africa (2016). “King IV: Report on Corporate Governance for South Africa 2016.” Retrieved from https://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king_iv/King_IV_Report/IoDSA_King_IV_Report_-_WebVe.pdf

4 Deloitte (2016). King IV: Bolder than Ever. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/za/Documents/governance-risk-compliance/DeloitteZA_KingIV_Bolder_Than_Ever_CGG_Nov2016.pdf

5 The Associated Press (2015, April 13). “Ex-Egg Industry Executives Jailed in Salmonella Outbreak.” Retrieved from The New York Times: https://www.nytimes.com/2015/04/14/business/ex-egg-industry-executives-jailed-in-salmonella-outbreak.html

6 Dobush, G. (2018, Aug. 1). “Just as Chipotle Comes Back from Its E.Coli Meltdown, It Has Yet Another Food Safety Scare.” Retrieved from Fortune: http://fortune.com/2018/08/01/chipotle-ecoli-food-safety-scare-ohio/

7 Smith, M., Hartocollis, A. (2018, May 16). “Michigan State’s $500 Million for Nassar Victims Dwarfs Other Settlements.” Retrieved from The New York Times: https://www.nytimes.com/2018/05/16/us/larry-nassar-michigan-state-settlement.html

8 Block, D.; Gerstner, A. (2016). “One-Tier vs. Two-Tier Board Structure: A Comparison between the United States and Germany.” Retrieved from Penn Law: Legal Scholarship Repository: http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1001&context=fisch_2016 p. 6, 23

9 “Non-financial reporting.” Retrieved from European Commission: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en

10 Dodd-Frank: U.S. Securities and Exchange Commission. (2017, Mar. 14). “Fact Sheet – Disclosing the Use of Conflict Minerals.” Retrieved from https://www.sec.gov/opa/Article/2012-2012-163htm---related-materials.html

11 Lacey Act. Retrieved from U.S. Fish & Wildlife Service International Affairs: https://www.fws.gov/international/laws-treaties-agreements/us-conservation-laws/lacey-act.html

12 Morris, J., Baddache, F. (2012, July). The Five W's of France's CSR Reporting Law. Retrieved from BSR: https://www.bsr.org/reports/The_5_Ws_of_Frances_CSR_Reporting_Law_FINAL.pdf

13 Modern Slavery Act 2015. Retrieved from The National Archives: http://www.legislation.gov.uk/ukpga/2015/30/contents/enacted

14 Australian Government Federal Register of Legislation. Retrieved from: https://www.legislation.gov.au/Details/C2007A00175

15 Accord on Fire and Building Safety in Bangladesh. Retrieved from: http://bangladeshaccord.org/

16 Roundtable on Sustainable Palm Oil. Retrieved from https://www.rspo.org/about

17 Marine Stewardship Council. Retrieved from https://www.msc.org/

18 The Aquaculture Stewardship Council. Retrieved from https://www.asc-aqua.org/

19 COSO (2017, June). “Enterprise Risk Management: Integrating with Strategy and Performance.” p. 27

[20] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 4

[21] About Stora Enso. Retrieved from Stora Enso: http://www.storaenso.com/about/history

[22] Purpose and Values. Retrieved from Stora Enso: http://www.storaenso.com/about/purpose-and-values

[23] KPMG (2017). "ESG, strategy and the long view: A framework for board oversight."

[24] Network for Business Sustainability (2010, November 30). "Embedding Sustainability in Organizational Culture: A How to Guide for Executives." Retrieved from https://nbs.net/p/executive-report-organizational-culture-2dd32ad5-1786-4e3c-bb36-27c4f1a386f1

[25] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 28

[26] Wachtell, Lipton, Rosen and Katz (2018). "ESG and Sustainability: The Board's Role." Retrieved from http://www.wlrk.com/webdocs/wlrknew/WLRKMemos/WLRK/WLRK.26006.18.pdf

[27] Stora Enso. (2017). "Sustainability and ethics committee." Retrieved from Stora Enso: http://www.storaenso.com/investors/governance/board-of-directors/global-responsibility-and-ethics-committee

[28] Mondi. "Board committees." Retrieved from Mondi: https://www.mondigroup.com/en/corporate-governance/board-committees/

[29] ExxonMobil (2017, January 25). "Susan Avery Elected to ExxonMobil Board." Retrieved from https://news.exxonmobil.com/press-release/susan-avery-elected-exxonmobil-board

[30] KPMG (2017). "ESG, strategy and the long view: A framework for board oversight." p. 18

[31] Wachtell, Lipton, Rosen and Katz (2018). "ESG and Sustainability: The Board's Role." Retrieved from http://www.wlrk.com/webdocs/wlrknew/WLRKMemos/WLRK/WLRK.26006.18.pdf

[32] Asset Management Working Group of the United Nations Environment Programme Finance Initiative (2014, June). "Integrated Governance: A new model of governance for sustainability." Retrieved from United Nations Environment Programme (UNEP): http://www.unepfi.org/fileadmin/documents/UNEPFI_IntegratedGovernance.pdf

[33] National Association of Corporate Directors and Its Strategic Content Partners (2017). "Governance Challenges 2017: Board Oversight of ESG." Retrieved from http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/nacd-governance-challenges-2017.pdf

[34] National Association of Corporate Directors and Ernst & Young LLP (2014). "Oversight of Corporate Sustainability Activities." Retrieved from https://www.ey.com/Publication/vwLUAssets/NACD-EY-taking-sustainability-awareness-to-the-board-level/%24FILE/NACD-EY-taking-sustainability-awareness-to-the-board-level.pdf

[35] Ceres and KKS Advisors (2018). "Systems Rule: How Board Governance Can Drive Sustainability Performance."

[36] Eccles, R., Youmans, T. (2015). "Materiality in Corporate Governance: The Statement of Significant Audiences and Materiality." Retrieved from Harvard Business School: https://www.hbs.edu/faculty/Publication%20Files/16-023_f29dce5d-cbac-4840-8d5f-32b21e6f644e.pdf

[37] DiPietro, B. (2018, May 15). "Companies find value in combining compliance, sustainability." Retrieved from WSJ: https://blogs.wsj.com/riskandcompliance/2018/05/15/companies-find-value-in-combining-compliance-sustainability/#coral_toggle_BL-252B-15236

2. Strategy and objective-setting for ESG-related risks

[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] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 45

[3] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 3

[4] Ocean Tomo (2015). "Annual Study of Intangible Asset Market Value." Retrieved from http://www.oceantomo.com/intangible-asset-market-value-study/

[5] EY (2017). "Integrated Reporting: Linking strategy, purpose and value." Retrieved from EY: https://www.ey.com/Publication/vwLUAssets/EY-integrated-reporting-linking-strategy-purpose-and-value/$FILE/EY-integrated-reporting-linking-strategy-purpose-and-value.pdf p. 6

[6] Integrated Reporting Council and EY (2013, July). Value Creation Background Paper. Retrieved from Integrated Reporting: http://integratedreporting.org/wp-content/uploads/2013/08/Background-Paper-Value-Creation.pdf

[7] International Integrated Reporting Council (IIRC). (2013, December). The International Integrated Reporting <IR> framework. Retrieved from IIRC: http://integratedreporting.org/wp-content/uploads/2013/12/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-2-1.pdf

[8] (2018, June 30). "Value through Focus and Discipline: Sasol Limited Integrated Report." Retrieved from https://www.sasol.com/sites/default/files/financial_reports/Sasol%20IR_Web.pdf pp. 8-9

[9] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." pp. 46-47

[10] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 46

[11] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 74

[12] International Integrated Reporting Council (IIRC). (2013, December). The International Integrated Reporting <IR> framework. Retrieved from IIRC: http://integratedreporting.org/wp-content/uploads/2013/12/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-2-1.pdf p. 32

[13] EYGM Limited (2015). "Megatrends 2015: making sense of a world in motion." Retrieved from: http://www.ey.com/Publication/vwLUAssets/ey-megatrends-report-2015/$FILE/ey-megatrends-report-2015.pdf p. 2

[14] World Economic Forum (2017, January 11). "The Global Risks Report 2017, 12th Edition." Retrieved from World Economic Forum: http://www3.weforum.org/docs/GRR17_Report_web.pdf

[15] Global Opportunity Network (2017). "Global Opportunity report 2017." Retrieved from Global Opportunity Network: http://www.globalopportunitynetwork.org/report-2017/

[16] "Insurance Research: Conning Library." Retrieved from Conning: https://www.conning.com/products/insurance-research

[17] "Biotechnology Industry Analysis Reports." Retrieved from Biotechnology Innovation Organization: https://www.bio.org/bio-industry-analysis-published-reports

[18] Accenture (2017). Driving the Future of Payments: 10 Megatrends. Retrieved from https://www.accenture.com/t20171012T092426Z__w__/us-en/_acnmedia/PDF-62/Accenture-Driving-the-Future-of-Payments-10-Mega-Trends.pdf

[19] Deloitte (2018). The rise of the social enterprise: 2018 Deloitte Global Human Capital Trends. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/HCTrends2018/2018-HCtrends_Rise-of-the-social-enterprise.pdf

[20] EYGM Limited (2016). "The upside of disruption: megatrends shaping 2016 and beyond." Retrieved from EY: http://cdn.ey.com/echannel/gl/en/issues/business-environment/2016megatrends/001-056_EY_Megatrends_report.pdf

[21] KPMG (2018). Emerging Trends in Infrastructure. Retrieved from https://home.kpmg.com/xx/en/home/insights/2018/01/emerging-trends-in-infrastructure.html

[22] (2015). McKinsey Special Collections: Trends and global forces. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/Strategy%20and%20corporate%20finance%20special%20collection/Final%20PDFs/McKinsey-Special-Collections_Trends-and-global-forces.ashx

[23] PwC. "Megatrends." Retrieved from PwC: https://www.pwc.nl/en/topics/megatrends.html

[24] KPMG. (2016). "Global Metals and Mining Outlook 2016." Retrieved from https://home.kpmg.com/content/dam/kpmg/xx/pdf/2016/08/kpmgmetals-mining-outlook-2016.pdf

[25] Office of the National Economic and Social Development Board. Retrieved from http://www.nesdb.go.th/nesdb_en/main.php?filename=develop_issue

[26] Allianz (2018). "Allianz Risk Barometer: Top Business Risks for 2018." Retrieved from Allianz: https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

[27] Metzger, E., Putt del Pino, S., Prowitt, S., Goodward, J., Perera, A. (2012). sSWOT: A Sustainability SWOT. Retrieved from: World Resources Institute: http://pdf.wri.org/sustainability_swot_user_guide.pdf

[28] (2016). "Natural Capital Protocol." Retrieved from Natural Capital Coalition: www.naturalcapitalcoalition.org/protocol

[29] (2016). "Social Capital Protocol." Retrieved from Social & Human Capital Coalition: https://www.wbcsd.org/Programs/People/Social-Impact/Social-and-Human-Capital-Protocol

[30] (2016). "Natural Capital Protocol." Retrieved from Natural Capital Coalition: www.naturalcapitalcoalition.org/protocol

[31] Butler, S. (2014, April 16). "Compensation fund for Bangladesh's Rana Plaza victims barely one-third full." Retrieved from The Guardian: https://www.theguardian.com/world/2014/apr/16/compensation-fund-victims-bangladesh-rana-plaza-one-third-full

[32] Westerman, A. (2017, April 30). "4 Years After Rana Plaza Tragedy, What's Changed For Bangladeshi Garment Workers?" Retrieved from NPR: http://www.npr.org/sections/parallels/2017/04/30/525858799/4-years-after-rana-plaza-tragedy-whats-changed-for-bangladeshi-garmentworkers

[33] (2014, June 21). "Coca-Cola forced to close India bottling factory over excessive water use, pollution." Retrieved from RT: https://www.rt.com/ news/167012-coca-cola-factory-closed-india/

[34] Reuters. (2017, August 11). "Union federation accuses copper miner Freeport of treating 'fired' workers 'with contempt'". https://www.business-humanrights.org/sites/default/files/documents/Freeport-McMoRan-response-Aug-2017.pdf

[35] Freeport-McMoRan Inc. (2017, August 27). https://www.reuters.com/article/indonesia-freeport-strike/union-federation-accuses-copper-miner-freeport-of-treating-fired-workers-with-contempt-idUSL4N1KX1OM

[36] Corkery, M. (2016, Oct. 14). "Wells Fargo Says Customers Shied Away After Scandal." Retrieved from The New York Times: https://www.nytimes.com/2016/10/15/business/dealbook/wells-fargo-says-customers-shied-away-after-scandal.html

[37] McGrath, M. (2016, September 8). "Wells Fargo Fined $185 Million For Opening Accounts Without Customers' Knowledge." Retrieved from Forbes: https://www.forbes.com/sites/maggiemcgrath/2016/09/08/wells-fargo-fined-185-million-for-opening-accounts-without-customers-knowledge/#7b35583451fc

[38] Egan, M. (2017, March 29). "Wells Fargo customers in $110 million settlement over fake accounts." Retrieved from CNN: http://money.cnn.com/2017/03/29/investing/wells-fargo-settles-fake-account-lawsuit-110-million/index.html

[39] WBCSD (2018). "Reporting matters: Six years on: the state of place."

[40] Accountability. Retrieved from http://www.accountability.org/standards/

[41] Ceres. "The Ceres Roadmap for Sustainability." Retrieved from Ceres: https://www.ceres.org/roadmap

[42] WBCSD. (2016, August). "Guidelines for Environmental and Social Impact Assessment (ESIA)." https://www.wbcsd.org/Sector-Projects/Cement-Sustainability-Initiative/Resources/Guidelines-for-Environmental-and-Social-Impact-Assessment-ESIA

[43] GRI Standards. Retrieved from GRI: https://www.globalreporting.org/standards/

[44] Business & Human Rights Resource Center. Retrieved from Business & Human Rights Resource Centre: https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-due-diligence

[45] Integrated Reporting. (2016, October). Creating value: The cyclical power of integrated thinking and reporting. Retrieved from International Integrated Reporting Council: http://integratedreporting.org/wp-content/uploads/2017/05/CreatingValue_IntegratedThinkingK1.pdf

[46] Sustainability Accounting Standards Board Standards. Retrieved from Sustainability Accounting Standards Board (SASB): https://www.sasb.org/

[47] SASB. "Approach to Materiality & Standards Development – Staff Bulletin." Retrieved from https://library.sasb.org/materiality_bulletin/

[48] "Materiality." Retrieved from GRI G4: https://g4.globalreporting.org/how-you-should-report/reporting-principles/principles-for-defining-report-content/materiality/Pages/default.aspx

[49] Accountability Standard AA1000. Retrieved from http://www.accountability.org/standards/ p. 18

[50] UN Global Compact and Pacific Institute. "CEO Water Mandate." Retrieved from https://ceowatermandate.org/

[51] CDP. Retrieved from https://www.cdp.net/en

[52] Center for Sustainable Organzations. Retrieved from http://www.sustainableorganizations.org/

[53] Bertels, S., Dobson, R. (2017, May 8). The Road to Context: Contextualising Your Strategy and Goals. Retrieved from Embedding Project: https://embeddingproject.org/resources/the-road-to-context

[54] The Equator Principles. Retrieved from http://equator-principles.com/

[55] World Business Council for Sustainable Development and World Resources Institute (2015). "The Greenhouse Gas Protocol: A Corporate Accounting Standard Revised Edition." Retrieved from Greenhouse Gas Protocol: http://www.ghgprotocol.org/corporate-standard

[56] Future-Fit Business Benchmark. Retrieved from http://futurefitbusiness.org/

[57] (2011). "Guiding Principles on Business and Human Rights." Retrieved from Business & Human Rights Resource Centre: https://business-humanrights.org/en

[58] Life Cycle Initiative. "Life Cycle Sustainability Assessment." Retrieved from http:// www.lifecycleinitiative.org/starting-life-cycle-thinking/life-cycle-approaches/life-cyclesustainability-assessment/

[59] Thomas, M., McElroy, M. The Multicapital Scorecard. Retrieved from http://www.multicapitalscorecard.com/

[60] Net Positive Project. Retrieved from https://www.netpositiveproject.org/

[61] "The Natural Capital Protocol Toolkit." Retrieved from Natural Capital Coalition: http://naturalcapitalcoalition.org/protocol/protocol-toolkit/

[62] "Social & Human Capital Protocol Toolkit." Retrieved from WBCSD: http://social-capital.org/toolkit?id=18

[63] Rockström, J. et al. (2009). Nature. Vol. 461. Retrieved from http://www. nature.com/news/specials/planetaryboundaries/index.html pp. 472 – 475

[64] Alliance for Water Stewardship. Retrieved from http://a4ws.org/

[65] Oxfam (2012). A Safe and Just Space for Humanity: Can We Live within the Doughnut? Accessed at: https://www.oxfam.org/sites/www.oxfam.org/files/dp-a-safe-and-justspace-for-humanity-130212-en.pdf

[66] Living Planet Index. Retrieved from http://www.livingplanetindex.org/home/index

[67] WRI Aqueduct: Measuring and Mapping Water Risk. Retrieved from World Resources Institute: http://www.wri.org/our-work/project/aqueduct

[68] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 45

[69] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 4

[70] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 11

[71] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." pp. 62-63

[72] Gold Coast Waterways Authority. (2017, May). "Risk Appetite Statement." Retrieved from: https://gcwa.qld.gov.au/wp-content/uploads/2017/05/GCWA-Risk-Appetite-Statement.pdf

[73] "Skanska: Addressing Human Rights Risks." Retrieved from UN Global Compact – Sustainable Supply Chains: Resources & Practices: http://supply-chain.unglobalcompact.org/site/article/67

[74] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 57

[75] Danone (2017). "Our Vision." Retrieved from https://www.danone.com/about-danone/sustainable-value-creation/our-vision.html

[76] Anderson, R. (1999). Mid-Course Correction: Toward a Sustainable Enterprise, the Interface Model.

[77] Dobson, R. and Bertels, S. (2017) The Road to Context: Contextualising your Strategy & Goals Casebook. Retrieved from Embedding Project: https://embeddingproject.org/system/attachments/documents/000/000/078/original/EP_The_Road_to_Context_Guidebook.pdf?1527885106

[78] "Income Position Statement." Retrieved from Mars: https://www.mars.com/global/about-us/policies-and-practices/income-position-statement

3. Performance for ESG-related risks

[1] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 65

3a. Identifies risk

[1] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 65

[2] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 67

[3] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 68

[4] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 68

[5] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 69

[6] Task Force on Climate-related Financial Disclosure (TCFD). (2017). "Recommendations of the Task Force on Climate-related Financial Disclosures." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/wp-content/uploads/2017/06/FINAL-TCFD-Report-062817.pdf p. 21

[7] Allianz. (2018). "Allianz Risk Barometer: Top Business Risks for 2018." Retrieved from Allianz: https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

[8] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 3

[9] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 70-71

3b. Assesses and prioritizes risks

[1] COSO ((2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 65

[2] Whelan, T.; Zapaa, B.; & Babic, N. (2017, August). "Deforestation-free Supply Chains: Financial Impact for Brazilian Beef Production." Retrieved from NYU Stern: http://www.stern.nyu.edu/sites/default/files/assets/documents/Beef%20in%20Brazil%20Report%2009.17.pdf

[3] Whelan, T.; Zapaa, B.; & Babic, N. (2017, August). "Deforestation-free Supply Chains: Financial Impact for Brazilian Beef Production." Retrieved from NYU Stern: http://www.stern.nyu.edu/sites/default/files/assets/documents/Beef%20in%20Brazil%20Report%2009.17.pdf

[4] Whelan, T.; Zapaa, B.; Zeidan, R.; & Fishbein, G. (2017, October 13). "How to Quantify Sustainability's Impact on Your Bottom Line." Retrieved from Harvard Business Review: https://hbr.org/2017/09/how-to-quantify-sustainabilitys-impact-on-your-bottom-line

[5] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 74

[6] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 74

[7] 2016). "Powering your world: Integrated report." Retrieved from Eskom: https://dc.sourceafrica.net/documents/117902-Eskom-Integrated-Report-2016.html

[8] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 77

[9] Borsa, L., Frank, P., Doran, H. (2014). "How can resilience prepare companies for environmental and social change?" Retrieved from PwC: https://www.pwc.com/gx/en/governance-risk-compliance-consulting-services/resilience/publications/pdfs/resilience-social.pdf

[10] Kaplan, R. and Mikes, A. (2012 June). Strategic Planning: Managing Risks: A New Framework. Retrieved from Harvard Business Review: https://hbr.org/2012/06/managing-risks-a-new-framework

[11] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 79

[12] Energy and innovation. Retrieved from Shell: http://www.shell.com/energy-and-innovation/the-energy-future/scenarios/new-lenses-on-the-future/earlier-scenarios.html

[13] CPA Australia, KPMG Australia and GRI Focal Point Australia (2014). "From Tactical to Strategic: How Australian businesses create value from sustainability," GRI Focal Point Australia, Sydney. Retrieved from Global Reporting: https://www.globalreporting.org/resourcelibrary/GRI2014TacticaltoStrategic.pdf

[14] CPA Australia, KPMG Australia and GRI Focal Point Australia (2014). "From Tactical to Strategic: How Australian businesses create value from sustainability," GRI Focal Point Australia, Sydney. Retrieved from Global Reporting: https://www.globalreporting.org/resourcelibrary/GRI2014TacticaltoStrategic.pdf

[15] World Economic Forum (2018, January 17). "The Global Risks Report 2018, 13th Edition." Retrieved from World Economic Forum: reports.weforum.org/global-risks-2018/ Figure IV

[16] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 75

[17] (2016). "Natural Capital Protocol." Retrieved from Natural Capital Coalition: https://naturalcapitalcoalition.org/natural-capital-protocol/

[18] (2017). "Social Capital Protocol." Retrieved from WBCSD: https://www.wbcsd.org/Programs/People/Social-Impact/Social-and-Human-Capital-Protocol

[19] jetBlue, the Ocean Foundation, ATKearney (2014). "EcoEarnings: A Shore Thing." Retrieved from jetBlue: https://www.jetblue.com/p/ecoearnings_report.pdf

[20] Shift and Institute for Human Rights and Business (IHRB) (2013). "Oil and Gas Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights." European Commission. Retrieved from IHRB: https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/O&G/EC-Guide_O&G.pdf

[21] Shift and Institute for Human Rights and Business (IHRB) (2013). "Oil and Gas Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights." European Commission. Retrieved from IHRB: https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/O&G/EC-Guide_O&G.pdf

[22] "UN Guiding Principles." Retrieved from https://www.ungpreporting.org/

[23] "Assess: Moving from reactive to proactive." Retrieved from Shift: https://www.shiftproject.org/resources/respect/assess/

[24] Shift (2014, January). "Business and Human Rights Impacts: Identifying and Prioritizing Human Rights Risks." Retrieved from: https://www.shiftproject.org/resources/publications/business-human-rights-impacts-identifying-prioritizing-risks/

[25] UN Global Compact Network Japan (UNGCJN) and EYGM Limited (2016). "Business and Human Rights: Corporate Japan Rises to the Challenge." Retrieved from UNGCJN: http://ungcjn.org/common/frame/plugins/fileUD/download.php?type=contents_files&p=elements_file_2563.pdf&token=625ea8f0a5e047e63bb2fc7ea070d7d926e84268&t=20171122162509

[26] International Finance Corporation (IFC) (2012, Jan. 1). "Performance Standards on Environmental and Social Sustainability." Retrieved from IFC: https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/policies-standards/performance-standards

[27] "The Natural Capital Protocol Toolkit." Retrieved from Natural Capital Coalition: http://naturalcapitalcoalition.org/protocol/protocol-toolkit/

[28] "Social & Human Capital Protocol Toolkit." Retrieved from WBCSD: http://social-capital.org/toolkit?id=18

[29] Porro, Bruno and Schaad, Werner (2004). "The Risk Landscape of the Future." Swiss Re.

[30] (2016). "Natural Capital Protocol." Retrieved from Natural Capital Coalition: https://naturalcapitalcoalition.org/natural-capital-protocol/ p. 80

[31] Davis, R., & Franks, D. (2014). "Costs of Company-Community Conflict in the Extractive Sector." Harvard Kennedy School, Shift, The University of Queensland Australia. Retrieved from CSR Initiative at the Harvard Kennedy School: https://sites.hks.harvard.edu/m-rcbg/CSRI/research/Costs%20of%20Conflict_Davis%20%20Franks.pdf p.8

[32] (2016). "Natural Capital Protocol." Retrieved from Natural Capital Coalition: https://naturalcapitalcoalition.org/natural-capital-protocol/

[33] (2017). "Social Capital Protocol." Retrieved from WBCSD: https://www.wbcsd.org/Programs/People/Social-Impact/Social-and-Human-Capital-Protocol

[34] EYGM Limited (2016). "Total Value: Impact valuation to support decision-making." Retrieved from EY: https://webforms.ey.com/Publication/vwLUAssets/EY-total-value/$FILE/EY-total-value.pdf p. 17

[35] Trucost (2015, May). "Trucost's Valuation Methodology." Retrieved from http://www.gabi-software.com/fileadmin/GaBi_Databases/Thinkstep_Trucost_NCA_factors_methodology_report.pdf

[36] ICF GHK and Economics for Environment Consultancy (2013, December 20). Retrieved from Food Standards Agency: https://www.food.gov.uk/sites/default/files/media/document/868-1-1610_20131219_FSA_WTP_Final_Report_v3_Clean_Version.pdf

[37] Dholakia, U. (2016, August 9). "A Quick Guide to Value-Based Pricing." Retrieved from Harvard Business Review: https://hbr.org/2016/08/a-quick-guide-to-value-based-pricing

[38] "Benefit Transfer Method." Retrieved from Ecosystem Valuation.

[39] Olson, P. (2006). "Sony Also Burned by Dell Debacle." Forbes. Retrieved from https://www.forbes.com/2006/08/16/sony-dell-image-cx_po_0816sony.html

[40] Task Force on Climate-related Financial Disclosure (TCFD). (2017). "Recommendations of the Task Force on Climate-related Financial Disclosures." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/wp-content/uploads/2017/06/FINAL-TCFD-Report-062817.pdf p. 25

[41] Kaplan, R., Mikes, A. (2012, June). "Managing Risks: A New Framework." Retrieved from Harvard Business Review: https://hbr.org/2012/06/managing-risks-a-new-framework

[42] Task Force on Climate-related Financial Disclosure (TCFD). (2017). "Recommendations of the Task Force on Climate-related Financial Disclosures. Financial Stability Board. https://www.fsb-tcfd.org/wp-content/uploads/2017/06/FINAL-TCFD-Report-062817.pdf

[43] World Business Council for Sustainable Development and World Resources Institute. (2015). "The Greenhouse Gas Protocol: A Corporate Accounting Standard Revised Edition. Retrieved from Greenhouse Gas Protocol: http://www.ghgprotocol.org/corporate-standard

[44] WBCSD. "Global Water Tool." Retrieved from WBCSD: http://www.wbcsd.org/Clusters/Water/Resources/Global-Water-Tool

[45] "InVEST: Integrated valuation of ecosystem services and tradeoffs." Retrieved from Natural Capital Project: https://www.naturalcapitalproject.org/invest/

[46] "WRI Aqueduct: Measuring and Mapping Water Risk." Retrieved from World Resources Institute: http://www.wri.org/our-work/project/aqueduct

[47] "Climate Change Knowledge Portal." Retrieved from World Bank: http://sdwebx.worldbank.org/climateportal/

[48] "GIIRS Impact Rated." Retrieved from B Analytics: http://b-analytics.net/giirs-funds

[49] "Initiative for Global Development." Retrieved from: http://www.igdleaders.org/advisory/igd-impact/

[50] OECD (2013). "Guidelines on Measuring Subjective Well-being." OECD Publishing, Paris. Retrieved from: http://www.oecd.org/statistics/oecd-guidelines-on-measuring-subjective-well-being-9789264191655-en.htm

[51] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 74

[52] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 72

[53] Solvay. (2016). "2016 Annual Integrated Report." Retrieved from Solvay: http://annualreports.solvay.com/2016/en/risks/main-risks.html

[54] Slovic P. (2000). The Perception of Risk. Earthscan.

[55] Dobelli, R. (2013). The Art of Thinking Clearly. HarperCollins.

[56] Janis, I. Cengage Learning. (1982). Groupthink: Psychological studies of policy decisions and fiascoes.

[57] Dobelli, R. (2013). The Art of Thinking Clearly. HarperCollins.

[58] Dobelli, R. (2013). The Art of Thinking Clearly. HarperCollins.

[59] Samuelson, W.; and Zeckhauser, R. (1988, Vol. 1). "Status Quo Bias in Decision Making. Journal of Risk and Uncertainty," Volume 1, 7-59." Retrieved from Harvard John F. Kennedy School of Government: https://sites.hks.harvard.edu/fs/rzeckhau/SQBDM.pdf.

[60] Soll J., Milkman, K.L., Payne, J.W. (2015, May). "Outsmart Your Own Biases." Retrieved from Harvard Business Review: https://hbr.org/2015/05/outsmart-your-own-biases

[61] USC Marshall School of Business. "How to Reduce Bias In Decision-Making." A Part of the Comprehensive and Fully Integrated Framework for Critical Thinking." Retrieved from: http://info.marshall.usc.edu/faculty/critthink/Supplemental%20Material/Reducing%20Bias.pdf

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

[63] Borsa, L., Frank, P., Doran, H. (2014). "How can resilience prepare companies for environmental and social change?" Retrieved from PwC: https://www.pwc.com/gx/en/governance-risk-compliance-consulting-services/resilience/publications/pdfs/resilience-social.pdf

3c. Implements risk responses

[1] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 81

[2] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 65

[3] McNally, J. (2013). "The 2013 COSO Framework & SOX Compliance." Retrieved from COSO: https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf p .7

[4] COSO (2013). Internal Control – Integrated Framework. Retrieved from https://www.coso.org/Pages/ic.aspx

[5] COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 81

[6] SwissRe. (2018, July 2). "News release: Swiss Re establishes thermal coal policy to support transition to a low-carbon economy." http://www.swissre.com/media/news_releases/nr_20180702_swiss_re_establishes_thermal_coal_policy.html

[7] Business and Sustainable Development Commission. (2017, January). "Better Business, Better World." Retrieved from http://report.businesscommission.org/uploads/BetterBiz-BetterWorld_170215_012417.pdf

[8] Timberland (2015). "Timberland Tires." Retrieved from https://www.timberlandtires.com/our-story/

[9] About. Retrieved from MudJeans: http://www.mudjeans.eu/

[10] Pathway 21. About us. Retrieved from The Materials Marketplace: http://materialsmarketplace.org/#about

[11] Additional information. Retrieved from P&G. https://us.pg.com/policies-and-practices/animal-welfare-policy/

[12] DiCaprio, T. (2015, March). "Making an impact with Microsoft's carbon fee: Inspiring a virtuous cycle of environmental investment and action." Retrieved from Microsoft: https://www.microsoft.com/en-us/environment/carbon

13 Hyatt (2017). "Our People." Retrieved from https://thrive.hyatt.com/en/thrive/our-people.html

14 Solomon, M. (2015, May 11). "To Transform Your Company's Culture, Change Your POV: Hyatt CEO's Perspective." Retrieved from Forbes: https://www.forbes.com/sites/micahsolomon/2015/05/11/transform-your-corporate-culture-by-changing-your-pov-the-hyatt-ceo-interview/

15 CPA Australia, KPMG Australia and GRI Focal Point Australia (2014) "From Tactical to Strategic: How Australian businesses create value from sustainability." Retrieved from Global Reporting: https://www.globalreporting.org/resourcelibrary/GRI2014TacticaltoStrategic.pdf

16 Shift and Institute for Human Rights and Business (IHRB) (2013). "Oil and Gas Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights." European Commission. Retrieved from IHRB: https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/O&G/EC-Guide_O&G.pdf

17 ISO/TC 46 Retrieved from https://www.iso.org/committee/52702.html

18 ISO 14054 Retrieved from https://www.iso.org/standard/38381.html

19 Equator Principles. Retrieved from Equator Principles: http://www.equator-principles.com/

20 PRI. Retrieved from UN Principles for Responsible Investment: https://www.unpri.org/

21 Lake, S., Rosenbarger, A., Winchester, C. (2016). "Palm Risk Assessment Methodology: Prioritizing Areas, Landscapes, and Mills." Retrieved from World Resources Institute: http://www.wri.org/sites/default/files/Palm_Risk_Assessment_Methodology_Prioritizing_Areas_Landscapes_And_Mills.pdf

22 WRI (2016, June 8). "Release: For the First Time, Companies Can Gauge Deforestation Risk by Evaluating Palm Oil Mills." Retrieved from https://www.wri.org/news/2016/06/release-first-time-companies-can-gauge-deforestation-risk-evaluating-palm-oil-mills

23 Unilever (2016). "Unilever Sustainable Palm Oil Sourcing Policy – 2016." Retrieved from https://www.unilever.com/Images/unilever-palm-oil-policy-2016_tcm244-479933_en.pdf

24 United Nations Climate Change (2016, April 22). 175 States Sign Paris Agreement. Retrieved from https://unfccc.int/news/175-states-sign-paris-agreement

25 Albrectsen, A. (2017, January 31). "Why collaboration will be key to achieving the Sustainable Development Goals." Retrieved from the World Economic Forum: https://www.weforum.org/agenda/2017/01/realising-the-potential-of-cross-sector-partnerships/

26 Sustainable Apparel Coalition. Retrieved from https://apparelcoalition.org/

27 Global Roundtable for Sustainable Beef. Retrieved from https://grsbeef.org/

28 Beverage Industry Environmental Roundtable. Retrieved from http://www.bieroundtable.com/

29 Global e-Sustainability Initiative. Retrieved from http://gesi.org/

30 Extractives Industries Transparency Initiative (EITI). Retrieved from https://eiti.org/

31 Asian Roundtable Task Force on Related Party Transactions. Retrieved from OECD: http://www.oecd.org/daf/ca/corporategovernanceprinciples/asianroundtabletaskforceonrelatedpartytransactions.htm

32 "Good Pharma Scorecard." Retrieved from Bioethics International:https://bioethicsinternational.org/good-pharma-scorecard/

33 McElroy, M. & Thomas, M. (2015, June). "The Multicapital Scorecard." Sustainability Accounting, Management and Policy Journal. Volume 6, Issue 3. Retrieved from: http://www.multicapitalscorecard.com/wp-content/uploads/2015/08/The_MultiCapital_Scorecard.pdf

34 Pacific Institute. (2017, April). Exploring the case for corporate context-based water targets. Retrieved from Pacific Institute: http://pacinst.org/wp-content/uploads/2017/04/context-based-targets.pdf

35 McElroy, M. (2015, May 25). "Science- vs. Context-Based Metrics – What's the Difference?" Retrieved from Sustainable Brands: http://www.sustainablebrands.com/news_and_views/new_metrics/mark_mcelroy/science-_vs_context-based_metrics_%E2%80%93_what%E2%80%99s_difference

36 Dobson, R. and Bertels, S. (2017) "The Road to Context: Contextualising your Strategy & Goals Casebook. Embedding Project."

37 CPA Australia, KPMG Australia and GRI Focal Point Australia (2014). "From Tactical to Strategic: How Australian businesses create value from sustainability. Retrieved from Global Reporting: https://www.globalreporting.org/resourcelibrary/GRI2014TacticaltoStrategic.pdf

38 Younie, M. (2012, August). "Diversion of Waste: The Business Case for Going Green." Retrieved from Government Finance Officers Association: http://www.gfoa.org/sites/default/files/GFR_AUG_12_65.pdf

39 "Why should you recycle E-waste?" Retrieved from Kansas Department of Health and Environment.

40 COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." pp. 82-83

41 COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." pp. 84

4. Review and revision for ESG-related risks

1 Organisation for Economic Co-operation and Development. (2004). "OECD Corporate Governance: Risk Management and Corporate Governance." Retrieved from OECD: http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf p. 37-40

2 COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 89

3 Funk, T. Marcus and Chelsea Curfman. (2016, February 8). "The Emerging Compliance 'Hot Topic' for 2016: Regulations Regarding Trafficked, Coerced Labor." Retrieved from Supply Chain Brain: https://www.supplychainbrain.com/articles/23234-the-emerging-compliance-hot-topic-for-2016-regulations-regarding-trafficked-coerced-labor

4 "2018 reform of EU data protection rules." Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5 https://www.theguardian.com/sustainable-business/2015/jun/12/turning-a-bad-reputation-round-can-take-years-of-good-leadership

6 Murphy, P. (2018, January 2018). "In less than 3 months, a major international city will likely run out of water." Retrieved from CNN: https://www.cnn.com/2018/01/24/africa/cape-town-water-crisis-trnd/index.html

7 Task Force on Climate-related Financial Disclosure (TCFD). (2017). "Technical Supplement: The Use of Scenario Analysis in Disclosure of Climate-related Risks and Opportunities." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/publications/final-technical-supplement/

8 Global Reporting Initiative (GRI) Standards. Retrieved from GRI Standards: https://www.globalreporting.org/standards/

5. Information, communication and reporting for ESG-related risks

1 COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 97

2 COSO (2017, June). "Enterprise Risk Management: Integrating with Strategy and Performance." p. 97

3 AccountAbility. AA1000 Accountability Principles. Retrieved from https://www.accountability.org/standards/

4 (2016, October). "Article 173-VI: Understanding the French regulation on investor climate reporting." Retrieved from: Forum Pour L'Investissement Responsable: http://www.frenchsif.org/isr-esg/wp-content/uploads/Understanding_article173-French_SIF_Handbook.pdf p. 12

5 EYGM Limited (2017). "Is your nonfinancial performance revealing the true value of your business to investors?" Retrieved from EY: EY - https://www.ey.com/Publication/vwLUAssets/EY_-_Nonfinancial_performance_may_influence_investors/$FILE/ey-nonfinancial-performance-may-influence-investors.pdf p. 7

6 Task Force on Climate-related Financial Disclosure (TCFD) (2017). "Recommendations of the Task Force on Climate-related Financial Disclosures." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/wp-content/uploads/2017/06/FINAL-TCFD-Report-062817.pdf

7 Liker, J., Choi, T. (2004, Dec.). "Building Deep Supplier Relationships." Retrieved from Harvard Business Review: https://hbr.org/2004/12/building-deep-supplier-relationships

8 Dorobantu, S., Flemming, D. (2017, Nov. 10). "It's Never Been More Important for Big Companies to Listen to Local Communities." Retrieved from Harvard Business Review: https://hbr.org/2017/11/its-never-been-more-important-for-big-companies-to-listen-to-local-communities

9 CalPERS (2016, June 6). "External Stakeholder Engagement Report." Retrieved from CalPERS: https://www.calpers.ca.gov/docs/board-agendas/201606/full/item02-01-ws.pdf

10 CalPERS (2017). 2017-22 "Strategic Plan." Retrieved from CalPERS: https://www.calpers.ca.gov/docs/forms-publications/2017-22-strategic-plan.pdf

11 (2018). CDSB Framework. Retrieved from CDSB.net: http://www.cdsb.net/what-we-do/reporting-frameworks/environmental-information-natural-capital

12 Global Reporting Initiative (GRI) Standards. Retrieved from GRI Standards: https://www.globalreporting.org/standards/

13 International Integrated Reporting Council (IIRC) (2013, December). "The International Integrated Reporting <IR> framework."

14 Task Force on Climate-related Financial Disclosure (TCFD) (2017). "Recommendations of the Task Force on Climate-related Financial Disclosures." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/wp-content/uploads/2017/06/FINAL-TCFD-Report-062817.pdf

15 Sustainability Accounting Standards Board Standards. Retrieved from Sustainability Accounting Standards Board (SASB): https://www.sasb.org/

16 The SDGs. Retrieved from United Nations Global Compact: https://www.unglobalcompact.org/sdgs/about

17 Solvay (2017). "2017 Annual Integrated Report." Retrieved from Solvay: http://annualreports.solvay.com/2017/en/servicepages/downloads/files/entire_solvay_ar17.pdf p. 83

18 CFA Institute (2017). "Environmental, social and Governance (ESG) survey." Retrieved from: https://www.cfainstitute.org/-/media/documents/survey/esg-survey-report-2017.ashx

19 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

20 EYGM Limited (2017). "Is your nonfinancial performance revealing the true value of your business to investors?" Retrieved from EY: EY - https://www.ey.com/Publication/vwLUAssets/EY_-_Nonfinancial_performance_may_influence_investors/$FILE/ey-nonfinancial-performance-may-influence-investors.pdf p. 18

21 COSO (2013). "Internal Control —Integrated Framework." Retrieved from COSO: https://www.coso.org/Pages/ic.aspx

22 Herz, R., Brad, M., and Thomson, J. (2017). "Leveraging the COSO Internal Control – Integrated Framework to Improve Confidence in Sustainability Performance Data 2017." Retrieved from IMA: https://www.imanet.org/-/media/73ec8a64f1b64b7f9460c1e24958cf7d.ashx pp. 47-48

23 KPMG (2017). "The Road Ahead: The KPMG Survey of Corporate Responsibility Reporting 2017." Retrieved from KPMG: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/10/kpmg-survey-of-corporate-responsibility-reporting-2017.pdf p. 26

24 (2013, January 22). "Participating in the EU Emissions Trading System (EU ETS)." Retrieved from https://www.gov.uk/guidance/participating-in-the-eu-ets

25 Osler, Hoskin & Harcourt LLP (2018, April). "Carbon and greenhouse gas legislation in British Columbia." Retrieved from Osler: https://www.osler.com/en/resources/regulations/2015/carbon-ghg/carbon-and-greenhouse-gas-legislation-in-british-c

26 IICM. Retrieved from https://www.icmm.com/en-gb/about-us/member-commitments/assurance

27 (2018, April 23). "Member State implementation of EU NFI Directive." Retrieved from Accountancy Europe: https://www.accountancyeurope.eu/publications/member-state-implementation-eu-nfi-directive/

Appendices

1 WBCSD (2017, January 18). "Sustainability and enterprise risk management: the first step towards integration." Retrieved from WBCSD: http://www.wbcsd.org/Projects/Non-financial-Measurement-and-Valuation/ResourcesSustainability-and-enterprise-risk-management-The-firststep-towards-integration

2 What are B Corps? Retrieved from Certified B Corporations: https://www.bcorporation.net/

3 CDSB (2018, April). "CDSB Framework for reporting environmental information, natural capital and associated business impacts: Advancing and aligning disclosure of environmental information in mainstream reports." Retrieved from https://www.cdsb.net/sites/default/files/cdsb_framework_2.1.pdf

4 "The Coalition for Environmentally Responsible Economies (CERES) Principles." Retrieved from http://www.gdrc.org/sustbiz/ceres-principles.html

5 "Environmental and social risk management for projects." Retrieved from Equator Principles: http://www.equator-principles.com/

6 "Global Reporting Initiative (GRI) Standards." Retrieved from GRI Standards: https://www.globalreporting.org/standards/

7 International Finance Corporation (IFC) (2012, Jan. 1). "Performance Standards on Environmental and Social Sustainability." Retrieved from IFC: https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/policies-standards/performance-standards

8 International Integrated Reporting Council (IIRC). (2013, December). "The International Integrated Reporting <IR> framework." Retrieved from IIRC: http://integratedreporting.org/wp-content/uploads/2013/12/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-2-1.pdf

9 LUXFLAG: Supporting Sustainable Finance. Retrieved from https://www.luxflag.org/pages/home.html

10 (2016). "Natural Capital Protocol." Retrieved from Natural Capital Coalition: www.naturalcapitalcoalition.org/protocol

11 OECD (2008). "OECD Guidelines for Multinational Enterprises." Retrieved from http://www.oecd.org/investment/mne/1922428.pdf

12 PRI. Retrieved from UN Principles for Responsible Investment: https://www.unpri.org

13 SASB (2018). "Conceptual Framework." Retrieved from https://www.sasb.org/standards-setting-process/conceptual-framework/

14 SASB. Current Standards. Retrieved from https://www.sasb.org/standards-overview/download-current-standards/

15 (2017). "Social Capital Protocol." Retrieved from WBCSD: https://www.wbcsd.org/Programs/People/Social-Impact/Social-and-Human-Capital-Protocol/Resources/Social-Capital-Protocol

16 "Sustainable Development Goals: 17 Goals to Transform Our World." Retrieved from the United Nations: http://www.un.org/sustainabledevelopment/sustainable-development-goals/

17 Task Force on Climate-related Financial Disclosure (TCFD) (2017). "Recommendations of the Task Force on Climate-related Financial Disclosures." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/wp-content/uploads/2017/06/FINAL-TCFD-Report-062817.pdf

18 United Nations Global Compact. Retrieved from United Nations: https://www.unglobalcompact.org/

19 (2011). "Guiding Principles on Business and Human Rights." Retrieved from Business & Human Rights Resource Centre: https://business-humanrights.org/en

20 "The PSI Initiative." Retrieved from Principles for Sustainable Insurance and UNEP Finance Initiative: http://www.unepfi.org/psi/vision-purpose/

21 Bertels, S., Dobson, R. (2017, May 8). The Road to Context: Contextualising Your Strategy and Goals. Retrieved from Embedding Project: https://embeddingproject.org/resources/the-road-to-context

22 Rockström, J. et al. (2009). Nature. Vol. 461. pp. 472 – 475. Retrieved from http://www.nature.com/news/specials/planetaryboundaries/index.html

23 Barton, B., Adrio, B., Hampton, D., & Lynn, W. (2017). "The Ceres Aqua Gauge: A Framework for 21st Century Water Risk Management."

[24] Retrieved from Ceres: https://www.ceres.org/sites/default/files/reports/2017-03/Ceres_AquaGauge_All_101113.pdf p. 16

[25] Barton, B., Adrio, B., Hampton, D., & Lynn, W. (2017). "The Ceres Aqua Gauge: A Framework for 21st Century Water Risk Management." Retrieved from Ceres: https://www.ceres.org/sites/default/files/reports/2017-03/Ceres_AquaGauge_All_101113.pdf p. 16

[26] Narayan, S., Beck, M., Wilson, P., Thomas C., Guerrero, A., Shepard, C., Reguero, B., Franco, G., Ingram, J. & Trespalacios, D. (2017, August 31). "The Value of Coastal Wetlands for Flood Damage Reduction in the Northeastern USA." Retrieved from Scientific Reports: https://www.nature.com/articles/s41598-017-09269-z

[27] Bousso, R. (2018, January 16). "BP Deepwater Horizon costs balloon to $65 billion." Retrieved from Reuters: https://www.reuters.com/article/us-bp-deepwaterhorizon/bp-deepwater-horizon-costs-balloon-to-65-billion-idUSKBN1F50NL

[28] Smith, M. (2016, March 10). "The Company Responsible for Poisoning a Pennsylvania Town's Water Will Pay Families $4.2M." Retrieved from Vice News: https://news.vice.com/article/the-company-responsible-for-poisoning-a-pennsylvania-towns-water-will-pay-families-42m

[29] Cama, T. (2015, May 14). "Utility agrees to pay $102 million penalty for water pollution." Retrieved from: http://thehill.com/policy/energy-environment/242134-utility-agrees-to-102m-penalty-for-water-pollution

[30] (2014, June 21). "Coca-Cola forced to close India bottling factory over excessive water use, pollution." Retrieved from RT: https://www.rt.com/news/167012-coca-cola-factory-closed-india/

[31] Andrade, R. (2012, July 20). "Brazil fines 35 firms US$44 million for biopiracy." Retrieved from SciDev.Net: http://www.scidev.net/global/biodiversity/news/brazil-fines-35-firms-us-44-million-for-biopiracy.html

[32] Crnojevic, M. (2016, July 29). "French biodiversity bill adopted; online wildlife crime fines increased significantly." Retrieved from International Fund for Animal Welfare: http://www.ifaw.org/united-states/news/french-biodiversity-bill-adopted-online-wildlife-crime-fines-increased-significantly

[33] Teather, D. (2005, April 14). "Nike lists abuses at Asian factories." Retrieved from The Guardian: https://www.theguardian.com/business/2005/apr/14/ethicalbusiness.money

[34] Girion, L. (2003, September 13). "Nike Settles Lawsuit Over Labor Claims." Retrieved from LA Times: http://articles.latimes.com/2003/sep/13/business/fi-nike13

[35] Ferguson, A., & Danckert, S. (2016, August 27). "An inconvenient year for 7-Eleven." Retrieved from The Sydney Morning Herald: http://www.smh.com.au/business/retail/an-inconvenient-year-for-7eleven-20160826-gr1xff.html

[36] Davis, R., & Franks, D. (2014). "Costs of Company-Community Conflict in the Extractive Sector." Retrieved from CSR Initiative at the Harvard Kennedy School: https://sites.hks.harvard.edu/m-rcbg/CSRI/research/Costs%20of%20Conflict_Davis%20%20Franks.pdf

[37] (2013). "National Safety Council Injury Facts®: 2013 Edition." Retrieved from National Safety Council: http://www.mhi.org/downloads/industrygroups/ease/technicalpapers/2013-National-Safety-Council-Injury-Facts.pdf

[38] Leigh, J., Markowitz, S., Fahs, M., Landrigan, P. (2000). Excerpted with permission from Costs of Occupational Injuries and Illnesses (University of Michigan Press, 2000). Retrieved from http://www.pbs.org/wgbh/pages/frontline/shows/workplace/etc/cost.html

[39] Butler, S. (2014, April 16). "Compensation fund for Bangladesh's Rana Plaza victims barely one-third full." Retrieved from The Guardian: https://www.theguardian.com/world/2014/apr/16/compensation-fund-victims-bangladesh-rana-plaza-one-third-full

[40] Darlington, S. (2016, March 2). "$6 billion settlement reached in Brazil mining disaster." Retrieved http://money.cnn.com/2016/03/02/news/world/brazil-mining-disaster-settlement/index.html

[41] Berfield, S. (2015, December 22). "Inside Chipotle's Contamination Crisis." Bloomberg Businessweek, https://www.bloomberg.com/features/2015-chipotle-food-safety-crisis/.

[42] Retrieved from Yahoofinance.com

[43] Walsh, B. (2014, May 21). "China's Food Safety Problems Go Deeper Than Pet Treats." Retrieved from Time: http://time.com/107922/china-pet-food-contamination-recall-video/

[44] Lee, J. (2014, May 21). "PetSmart, Petco to stop selling dog and cat treats made in China." Retrieved from USA Today: https://www.usatoday.com/story/news/nation-now/2014/05/21/petco-dog-treats-china/9367449/

[45] Olson, P. (2006). "Sony Also Burned by Dell Debacle." Forbes. Retrieved from https://www.forbes.com/2006/08/16/sony-dell-image-cx_po_0816sony.html

[46] Story, L. (2007). "Lead Paint Prompts Mattel to Recall 967,000 Toys." Retrieved from The New York Times: http://www.nytimes.com/2007/08/02/business/02toy.html

[47] Basu, T. (2014, March 31). "Timeline: A History Of GM's Ignition Switch Defect." Retrieved from NPR: http://www.npr.org/2014/03/31/297158876/timeline-a-history-of-gms-ignition-switch-defect

[48] Moynihan, T. (2017, January 22). "Samsung finally reveals why the note 7 kept exploding." Retrieved from Wired: https://www.wired.com/2017/01/why-the-samsung-galaxy-note-7-kept-exploding/

[49] Isidore, C., & O'Toole, J. (2013, September 19). "JPMorgan fined $920 million in 'London Whale' trading loss." Retrieved from CNN: http://money.cnn.com/2013/09/19/investing/jpmorgan-london-whale-fine/index.html

[50] Guerrero, J. & Williams, N. (2015, December 1). "United States: The High Cost Of An FCPA Violation." Retrieved from Mondaq: http://www.mondaq.com/unitedstates/x/424428/White+Collar+Crime+Fraud/The+High+Cost+of+an+FCPA+Violation

[51] (2016, May 5). "First ever corporate conviction under the UK Bribery Act." Retrieved from Walker Morris: https://www.walkermorris.co.uk/publications/brief-walker-morris-legal-update-may-2016/first-ever-corporate-conviction-uk-bribery-act/

[52] Parloff, R. (2018, February 6). "How VW Paid $25 Billion for 'Dieselgate' — and Got Off Easy." Retrieved from Fortune: http://fortune.com/2018/02/06/volkswagen-vw-emissions-scandal-penalties/

[53] Task Force on Climate-related Financial Disclosure (TCFD). (2017). "Technical Supplement: The Use of Scenario Analysis in Disclosure of Climate related Risks and Opportunities." Financial Stability Board. Retrieved from TCFD: https://www.fsb-tcfd.org/publications/final-technical-supplement/

[54] "Scenarios and projections." Retrieved from International Energy Agency: https://webstore.iea.org/world-energy-outlook-2017

[55] Nakicenovic, N., & Swart, R. (2000). "Emissions Scenarios." Geneva: Intergovernmental Panel on Climate Change (IPCC).

[56] Shell Scenarios. Retrieved from Shell: http://www.shell.com/energy-and-innovation/the-energy-future/scenarios.html

[57] (2017). "Energy Perspectives 2017: Long-term macro and market outlook." Retrieved from Statoil: http://www.shell.com/energy-and-innovation/the-energy-future/scenarios.html

[58] "Climate Change: Portfolio Analysis." Retrieved from BHP Billiton: http://www.bhp.com/~/media/5874999cef0a41a59403d13e3f8de4ee.ashx

[59] "Climate Change Strategy." Retrieved from ConocoPhillips: http://www.conocophillips.com/sustainable-development/environment/climate-change/climate-change-strategy/Pages/carbon-scenarios.aspx

[60] "Planning for Climate Change." Retrieved from Glencore: http://www.glencore.com/sustainability/climate-change/planning-for-climate-change/

[61] "Aqueduct Water Risk Atlas." Retrieved from http://www.wri.org/resources/maps/aqueduct-water-risk-atlas

[62] TCFD Knowledge Hub. Retrieved from https://www.tcfdhub.org/

Disclaimer

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

October 2018

COSO | wbcsd

coso.org wbcsd.org