

DIAGNOSTIC

Assessing the level of integration of ESG-related risks into enterprise risk management



How well are environmental, social and governance-related risks being integrated into my organization's enterprise risk management activities?

This diagnostic accompanies the guidance *Applying enterprise risk management to environmental, social and governance-related risks* (the "Guidance"). This guidance, developed by the World Business Council for Sustainable Development (WBCSD) in partnership with the Committee of Sponsoring Organizations of the Treadway Commission (COSO), helps companies to better understand their ESG-related risks and to manage and disclose them effectively.

This diagnostic tool helps companies to understand how well ESG-related risks are currently integrated into their ERM processes and structures.

Instructions

Work your way through the diagnostic to assess your level of maturity against each of the guidance chapters. Plot your rating in the table below to understand the level of integration for your company. Consider plotting desired maturity to identify gaps and areas for improvement (you can capture these on page 16 and 17).

	Basic 1	Developing 2	Established 3	Advanced 4	Leading 5
1. Governance and culture					
2. Strategy and Objective-setting					
3a. Identifies risk					
3b. Assesses and prioritizes risk					
3c. Implements risk responses					
4. Review and revision					
5. Information, communication and reporting					

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

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, WBCSD and COSO have partnered to develop guidance to help entities better understand the full spectrum of these risks and to manage and disclose them effectively.

The guidance has five chapters that mirror the five components of the COSO ERM Framework, Enterprise Risk Management - Integrating Strategy and Performance:



Applying the guidance can help a company to achieve:

- Enhanced resilience over the medium- and long-term by better anticipating and responding to a complex and interconnected array of risks
- A common language for articulating ESG-related risks
- Improved allocation of resources to respond to competing risks and priorities
- Enhanced pursuit of ESG-related opportunities by considering both positive and negative aspects of ESG-related risks
- Efficiencies of scale by managing ESG-related risks centrally and alongside other risks
- Improved disclosure and transparency

1. Governance and culture for ESG-related risks

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

Assess the level of maturity of your company's integration of ESG into governance and culture

Maturity Assessment			
	Basic 1	Developing 2	Established 3
Attributes	<ul style="list-style-type: none"> • None of the checklist activities have been performed • There is no or very limited board awareness of ESG-related risks • There are no defined roles, responsibilities or processes for managing ESG-related risks 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • The board is aware of a selection of ESG-related risks • Roles, responsibilities and processes for managing a selection of ESG-related risks are allocated and defined • The entity promotes internal and cross functional collaboration on ESG-related risks. For example, there is a sustainability representation on the risk committee



Which of the following activities does your company perform to integrate ESG into governance and culture?

- Map or define the organization’s mandatory or voluntary ESG-related requirements
- Consider opportunities for embedding ESG-related risk 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • The board has effective oversight of ESG-related risks (e.g., ESG is included in board charter, board committee responsible for ESG) • The board comprises appropriately qualified members, with skills sets that are relevant to understand and manage ESG-related risks • ESG-related risks, are integrated into the strategic planning and operational cycle • Roles, responsibilities and processes are defined and collaboration is promoted to support ERM

Maturity assessment for Governance and Culture

(1-5)

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



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, 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-related 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.



Assess the level of maturity of your company's integration of ESG into strategy and objective-setting

Maturity Assessment			
	Basic 1	Developing 2	Established 3
Attributes	<ul style="list-style-type: none"> • None of the checklist activities have been performed • The entity does not have an understanding of which ESG-related risks will impact their strategy or objectives • The entity does not have a defined risk appetite for ESG-related risks 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • The entity examines the internal and external business environment to understand ESG issues and risks (by conducting, for example megatrend analysis materiality assessments etc.) • Risk appetite (and tolerances) are defined or understood for key ESG-related risks



Which of the following activities does your company perform to integrate ESG into strategy and objective-setting?

- 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • The entity applies integrated thinking to understand ESG impacts and dependencies relating to a broad range of capitals (e.g., financial, natural, social) • A selection of ESG tools are used to understand the business context (e.g., ESG materiality assessment) • Risk appetites (and tolerances) are defined for most or all ESG-related risks

Maturity assessment for Strategy & Objective-setting



(1-5)

3. Performance for ESG-related risks

3a. Identifies risk

Risks are present in all business activities. They often come into focus due to changes in business strategy, objectives, context or risk appetite. 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
- 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

Assess the level of maturity of your company's integration of ESG into identifying risk

Maturity Assessment			
	Basic 1	Developing 2	Established 3
Attributes	<ul style="list-style-type: none"> • None of the checklist activities have been performed • The entity does not have an understanding of which ESG-related risks will impact their strategy or objectives • The entity does not have a defined risk appetite for ESG-related risks 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • Sustainability activities or analyses (e.g., ESG materiality assessment) are used to inform risk identification • ESG-related risks are defined but lack specificity and/or interconnections to other risks are not fully explore

Organizations use multiple approaches for identifying ESG-related risks: megatrend analysis, SWOT analysis, impacts and dependency mapping, stakeholder engagement and ESG-related materiality assessments. These tools can help identify and express ESG-related issues in terms of how a risk threatens achievement of an entity’s strategy and business objectives.

 **Which of the following activities does your company perform to integrate ESG into identifying 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • ESG-related risks, whether new or emerging, short-term or long-term, are integrated to the entity’s risk identification process • The company considers both the ‘down-side’ of ESG-related risk as well as any potential opportunities • ESG-related risks are defined precisely • The root causes of ESG-related risks and interconnections with other risks are understood

Maturity assessment for Identifying risk

(1-5)

3. Performance for ESG-related risks

3b. 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 to examine the extent to which identified risks impact the entity's strategy and business objectives, and prioritize accordingly. 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.

Assess the level of maturity of your company's integration of ESG into assessing and prioritizing risks

Maturity Assessment			
	Basic 1	Developing 2	Established 3
Attributes	<ul style="list-style-type: none"> • None of the checklist activities have been performed • There is no quantitative or qualitative assessment of ESG-related risks • There are no enterprise-wide criteria for prioritizing ESG-related risks 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • Some ESG-related risks have been assessed, either quantitatively or qualitatively • Risks are not always expressed in a common language to allow comparison and prioritization with other company risks

Applying ERM to ESG-related risks includes assessing risk severity in a language that management can use to prioritize risks. Leveraging ESG-related 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.

 **Which of the following activities does your company perform to integrate ESG into assessing and prioritizing risks?**

- 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • ESG-related risks impacts are well understood and expressed in relation to the impact on the company’s strategy and business objectives • The entity uses common language for expressing risk impact and prioritization • ESG-related risk prioritization criteria include considerations such as adaptability, speed of onset or vulnerability • Tools and methodologies are used to conduct quantitative and qualitative severity assessments

Maturity assessment for prioritizing risk

(1-5)

3. Performance for ESG-related risks

3c. 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.

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.

Assess the level of maturity of your company's integration of ESG into implementing risk responses

Maturity Assessment				
		Basic 1	Developing 2	Established 3
Attributes		<ul style="list-style-type: none"> • None of the checklist activities have been performed • The entity has not selected and implemented responses to ESG-related risks • There is little or no internal or external collaboration on responses for ESG-related risks 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • A business case and risk response are developed for some ESG-related risk have been selected • The organization promotes some informal internal collaboration around ESG-related risks • The entity is engaged in some external collaboration for a selection of ESG-related risks



Which of the following activities does your company perform to integrate ESG into implementing 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • A business case, management buy-in, and innovative risk responses have been selected and implemented for all ESG-related risks • Risk responses focus on both preserving value and also unlocking value through new opportunities • The company understands how ESG-related risks fits into the entity's overall risk portfolio • Internal and external engagement and collaboration is an essential part of ERM and innovation on risk responses

Maturity assessment for implementing risk responses

(1-5)

4. Review and revision for ESG-related risks



ERM 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. 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.



Assess the level of maturity of your company's integration of ESG into reviewing and revising

Maturity Assessment			
	Basic 1	Developing 2	Established 3
Attributes	<ul style="list-style-type: none"> • None of the checklist activities have been performed • The entity has little or no process to monitor ESG-related risks or the ERM process overall 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • Processes for identifying and managing ESG risks are conducted periodically (e.g., on an annual basis) • The entity has some process for monitoring ESG-related risks and the changing internal and external environment • Indicators, thresholds and targets established to monitor risk management for some ESG-related risks • The company pursues periodic improvement to the management of ESG-related risks (e.g., new technology, integrating lessons learned)



Which of the following activities does your company perform to integrate ESG into reviewing and revising?

- 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • ERM is a continuous process and the company is proactive in adapting to changes to the internal and external environment • All identified ESG-related risks are monitored on an ongoing basis, using indicators, thresholds and targets to inform decision making and make revisions as needed • The company pursues opportunities for ongoing improvement to the management of ESG-related risks

Maturity assessment for reviewing and revising

(1-5)

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



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 information to target audiences.



Assess the level of maturity of your company's integration of ESG into informing, communicating and reporting

Maturity Assessment			
	Basic 1	Developing 2	Established 3
Attributes	<ul style="list-style-type: none"> • None of the checklist activities have been performed • There is limited or no internal or external communication about ESG-related risks 		<ul style="list-style-type: none"> • Some of the checklist activities have been partially or fully performed • There is limited knowledge of the risk information needs for internal and external stakeholder • There is some internal communication about ESG-related risks for decision making (e.g., reporting to the board and management) • There is some external communication about ESG issues (e.g., sustainability report), however this is not framed in the context of the risk and opportunity • The company has some processes in place to enhance the quality of data for ESG risk disclosures



Which of the following activities does your company perform to integrate ESG into informing, communicating and reporting?

- 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

	Advanced 4	Leading 5
		<ul style="list-style-type: none"> • Most or all of the checklist activities have been performed or are in place • Internal communication about ESG-related risks occurs at all levels of the organization to promote awareness and decision-making • External disclosures are provided to stakeholders on a regular and timely basis to meet stakeholder information needs and support decision making • Disclosures align to ESG disclosure guidance or principles and there are processes to support accuracy, reliability and completeness of disclosures

**Maturity assessment
for informing, communicating
and reporting**



(1-5)



Action items for improvement at your company



Action items for improvement at your company

**World Business Council
for Sustainable Development**

Maison de la Paix,
Chemin Eugène-Rigot 2B,
1211 Geneva,
Switzerland
www.wbcsd.org

