Organic learning lessons: Looking to ERM to set ESG programs for success

ERM programs inherently have similar characteristics to ESG - a transversal and shared accountability requiring significant coordination and commitment. Senior Leaders can look to their ERM functions / programs to draw on organization specific lessons to set their ESG programs for success.

Often overlooked and under-prioritized so-called ‘black-swans’ or large stress events are no longer ‘once in a lifetime events’ but rather expected to occur at shorter intervals. Recent ongoing geopolitical, health and supply chain events demonstrate how closely intertwined and borderless the world has become. Whatever industry, size or geographic location, any event or localized change(s) can spread and have global knock-on effects.

And yet, our society has also long ached from risk myopia, challenged in the face of uncertainty and the realm of possible, and more prone to focus, if not react, to today’s real and immediate pains rather than anticipating and preparing for future plausible or emerging risks such as those associated with evolving Environment, Social and Governance (ESG) topics. The pace society has been acknowledging ESG challenges has only recently accelerated. ESG risks, and climate risk in particular, are now becoming central to the overall exposure of organizations. The World Economic Forum’s Global Risk Reports had consistently included ESG as a rising and important matter for leaders across the world: from 2018 to 2021, 5 of the top 10 risks were closely linked to environmental factors. In 2022, the top 8 most severe global scale risks were environmental or social-related, with climate action failure taking the top spot. Though the business impacts of ESG inaction are not always clear, we now know this is no longer a choice or even a viable option: tomorrow’s challenges (e.g. biodiversity loss) are today’s priority.

Global or local disclosure standards (e.g. TCFD[1], SASB[2], GRI[3]) have flourished over the years to further educate, guide and/or prescribe ESG practices and climate sustainability, culminating with the recent creation of the International Sustainability Standards Board. Investors and consumers are also increasingly factoring ESG into their investing and purchasing decisions. Pressures are mounting and yet, many organizations are still grappling with how to best define, integrate and operationalize ESG. Some seek external benchmarking (i.e. to social-proof and ‘learn from others’) to help inform ESG program design. There may yet be an opportunity for organizations to reflect internally and seek meaningful ‘lessons learned’. We believe the Enterprise Risk Management (ERM) maturity journey that many organizations have undergone parallels that of ESG. ERM inherently possesses similar characteristics – a highly transversal, multi-dimensional, forward-looking, and shared program.

As such, we have summarized shared design questions and ERM lessons learnt, that organizations can draw from as they look to set their ESG programs for success:

01 Purpose & mandate

What is the purpose and mandate of the program and function?

02 Linkage with strategy & performance

How do we ensure the program is linked to performance and not a parallel process?

03 Structure & resourcing

How do we best structure and resource the function to deliver on its mandate?

04 Accountability & ownership

The program has transversal impacts across the organization, how can a single function own it?

05 Harmonizing and integrating with the business:

How do we ensure the program is ‘part of the business’ and not duplicating existing activities performed across the organization?

06 Progressive & iterative

Do we build our programs, processes and initiatives all at once?

1. TCFD: Task Force on Climate-Related Financial Disclosures
2. SASB: Sustainability Accounting Standards Board
3. GRI: Global Reporting Initiative

01 Purpose & mandate	02 Linkage with strategy & performance	03 Structure & resourcing	04 Accountability & ownership	05 Harmonizing and integrating with the business	06 Progressive & iterative
ERM context					
There is no one-size fits all approach to ERM. Depending on industries, some organizations expect their ERM function to be a central risk hub that set risk standards, independently challenge / partner with the business on risk assessments and provide additional risk advisory and insights. Others rely on their ERM function to simply quarterback the end-to-end risk management and reporting processes. Yet, the successfulness of an ERM program is arguably less attributable to its maturity or sophistication, than the clarity and consensus over its mandate and expected value. Without purpose, there is no target to aim for. And to avoid mandate drift, Management and the Board should set the tone and articulate a clear ERM ambition and delivery model.	COSO defines ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". One ERM conundrum is hoping to apply a forward outlook and enhance business processes whilst applying a 'post-mortem' ERM process, where risks are assessed only after decisions have been made. Not only counterproductive, this design fault puts the entire ERM program at risk due to process parallelism, rear-looking risk assessments and duplicates efforts with other existing programs and initiatives. ERM has a strategic vocation and should originate from the early stage of strategy-setting, and subsequently cascade down to the organization. ERM should be formally integrated into the strategy planning process to ensure risks and material factors clearly acid-test and inform strategy design.	ERM had long been positioned as a middle management function, somehow buried several layers below the leadership team. Often, and especially in the non-financial industry, ERM practitioners were double hatting with other accountabilities and driving ERM from the "corner of their desk". Recently, ERM has been elevated in the hierarchy and has progressively taken a 'front seat'. To drive the risk agenda, organizations have enabled it with the authority, stature, structure and support from Management and the Board.	One of the oldest risk management adages has been that "risk is everyone's responsibility'. Whilst ownership of the ERM program must be clearly assigned, there should be little to no 'silo' in risk management. Risks are by nature highly inter-connected and transversal, and should be managed accordingly. Risk ownership may be allocated to drive accountability, direction and consistency in managing the underlying risk, yet everyone in the organization has a role to play.	There is little value setting an ERM process that adds another administrative layer or that simply duplicates existing programs. ERM should set the 'top of the house' risk architecture and ultimately provide structure, help harmonize and aggregate various risk management practices across the organization (e.g. health & safety, project or vendor management). Organizations are in the midst of setting the common foundational pillars of their various risk and control programs. They are looking at ways to instil one enterprise-wide risk language, bridges all functions, avoids redundancies and inconsistent risk data, and provides a 'single source of truth' all the way up to the Board.	Organizations have over time, through experience, built and solidified their capabilities in managing more traditional or 'known' risks such as credit, market or health & safety risks. The rapidly evolving operating environment and risk landscape, further fueled by the pandemic, has more recently elevated new risks to the top of the Management and Board agenda, such as climate change, health and wellbeing, remote-working or supply chain. Risk management has been a continuous journey and organizations have continuously revisited, upscaled and refined their ERM program to ensure that it had continuously provided value and helped build resilience.
Similarities between ERM and ESG					
Like ERM, the design of an ESG program must be bespoke to the industry, organization's business model and the operating context. Similarly, defining a formal ESG mandate and objective is a key quality in promoting / assuring a successful program outcome that is aligned with stakeholder expectations.	Like ERM, the positioning of ESG in relation to an organization's annual business planning / strategy design process may dictate the ESG function's ability to execute on its mandate. Without appropriate integration, ESG could become a compliance / backward-looking program.	Like ERM, the resource structure of the ESG function should be grounded in the necessary authority and empowerment to action change within the organization.	Like ERM, organizations need to clearly define the accountability of the ESG program (vs. accountability of a particular initiative / process).	Like ERM, the ESG process is a transversal activity that bridges over various business units / processes. Hence, building duplicative and redundant processes could result in poor stakeholder buy-in and change management challenges.	Like ERM, ESG is a complex and evolving topic that may require years of organizational education to build awareness, buy-in and understanding.
ESG lessons learned					
No ESG function / program looks the same, differing based on industry, company needs and stakeholder expectations. Clearly defining and communicating the ESG mandate, ambitions, roles, responsibilities and expectations are key to success program development.	Ensure that ESG is a core component of the strategic planning process, that it enhances and helps achieve your corporate strategy and objectives and is embedded into the organizational DNA. Avoid the creation of a stand-alone and siloed ESG program that outstrips corporate capabilities.	Provide the ESG function (or equivalent) with the exposure and skillset required to make a difference. Whether standalone or integrated within existing functions such as finance, strategy or risk management, ESG should be Board and senior management led with empowered staff to drive the program forward.	Consider assembling a cross-functional ESG Committee to address the inter-connected and transversal nature of ESG. Establish clear accountability for the overarching ESG program and clearly assign the management of material ESG factors.	Understanding existing ESG activities / processes, should be one of the first activities completed to better understand existing initiatives and not duplicate efforts.	An iterative (vs. big bang) approach for such a highly transformative and interconnected program allows organizations to focus on developing coordinated initiatives, building change management / buy-in, and upskilling capabilities to meet evolving ESG needs.

Contact us

Edouard Bertin-Mourot

Partner, National Enterprise Risk Management Lead
Risk Consulting

416-777-3511
edouardbertinmourot@kpmg.ca

Roopa Davé

Partner, Sustainability Services

604-691-3019
rdave@kpmg.ca

Pedro Medeiros

Partner, National Risk Consulting
Sustainability Champion

416-476-2263
pedromedeiros@kpmg.ca

Like ERM, there is no one-size fits all approach to ESG.

ESG needs to be organization specific and hence looking internally at the lessons learned of ERM may provide more practical and nuanced answers to your design questions.