



Incorporating ESG in risk management

Transforming internal controls framework for ESG reporting

INTRODUCTION

As a Risk & Controls professional, you sometimes find yourself in the following situation, “You just finished the year-end in-control statement and celebrated another successful end-of-year cycle with your team. You received an email from the CFO asking: “Do we have an internal controls framework for ESG reporting?” You are familiar with the term ESG. In fact, you just bought an electric vehicle to show your personal commitment to this topic. However, the internal controls framework for ESG reporting is completely new to you and you don’t even know where to begin.

Following this scenario, questions that naturally surface are: “What is the information required to report

and how do I ensure completeness, accuracy and compliance of such information being reported? Are there appropriate internal controls in place within different processes to ensure transparency, accuracy and consistency of the data being disclosed and reported? How do I assess whether I am doing enough to comply with the regulatory requirements in its true essence and not make it a box-ticking exercise? How does my role in this journey differ from what the sustainability department is responsible for?”

If the questions above sound familiar to you at all, you are not alone. ESG and ESG reporting have moved out of the office of the Chief Sustainability Officer (CSO) into the purview of the CFO for many organizations, as it is slowly becoming the focal point and climbing its way up to the



Jeroen Bolt
is a director at KPMG
NL.



Arushi Paliwal CA
is a manager at KPMG
NL.



Urvashi Aggarwala
is a senior consultant
at KPMG NL.

top agendas of the boardroom and C-suite discussions. Regulators across the globe have been driving the inclusion of ESG in reporting which can be found in [Zhig22].

Understanding the need of the hour, we suggest some simple, albeit not easy, steps for you to consider commencing the ESG Reporting Journey.

THE ESG REPORTING JOURNEY

There are some considerations ([Schm22]) to be kept in mind by a Risk & Controls professional like yourself while starting and continuing on this journey:

- **Define the strategy for the risk function.** The ESG risk profile should be underpinned with risk

appetite statements, a robust framework and taxonomy as well as clear metrics to allow the management to monitor the amount of risk it is willing to accept in pursuit of the organizational objectives. For instance, consider a statement: “We have a low risk appetite for non-compliance of ESG reporting regulations either out of ignorance or willfulness; therefore, we focus on education, training, awareness and accountability of actions and disclosures.”

- **Self-assessment of skills and capabilities.** Ensure your risk function is credible and well-positioned to add to the dialogue concerning strategic change. This implies a need for action on several fronts, such as hiring, training and career development of the right talent who has the competency of identifying risks pertaining to ESG and putting an internal controls framework place. The risk function should stay up to date with all the regulatory changes in the ESG space like the introduction of EU Taxonomy, proposed reporting requirements by SEC and being quick to analyze the impact of non-compliance on the reputation of the organization. Risk professionals should also possess the ability to assess the robustness of the existing processes and controls for instance for being able to assess the HR department to see how the employee related numbers (to be disclosed) are collected and if the controls are appropriate for complete and accurate reporting.
- **Define roles and responsibilities.** Define and agree the role of the risk function within the business planning cycle – set out chronologically and map check points for risk management-facilitated discussions on key strategic initiatives. ESG internal control specialists should be allocated the responsibility to perform risk assessments and double materiality assessments. Additionally, the risk function should play a role in defining the organizations’ policy and procedures for ESG-related disclosure risks and controls.
- **Enhance risk management technologies.** Make better use of available technologies, visualization tools and dashboarding to support senior management decisions on strategic risk. Invest in emerging risks, horizon scanning and stress testing capabilities to support better conversations on long-term implications of strategic decisions. For example, KPMG’s Sofy platform is often used for ESG regulations compliance tracking, carbon emissions monitoring, providing assurance over supporting data collection & analytics, ESG project impact tracking and performing maturity assessments.

Evolving your risk function towards the future ambition of the organization can be a complex undertaking. The following key steps are the core for a successful transformation:

- a. Look at establishing a governance structure with clear roles and responsibilities.** The organization should set up adequate sustainability governance with clear roles and responsibilities in order to define policies, oversee the end-to-end ESG process from the definition of strategy through to the disclosures being made, and ensure there are appropriate controls throughout the process.
- In conjunction with management, it is important to understand the ESG topics of investor focus. You should focus on gathering existing documentation (e.g. baseline data, reporting strategy documents, output of process reviews) and review existing stakeholder materiality assessments, ERM results, internal board presentations, and analyst reports.
- b. Assess the as-is state for ESG reporting within the organization.** While you start assessing the as-is state, give some thought to the below questions/points for a holistic overview:
- i.** Is the ESG theme part of your organization's values? Is the S(ocial) element included in the ethics & integrity employee training sessions?
 - ii.** Is there sufficient knowledge of G(overnance) aspects amongst oversight bodies to enable them to carry out their role appropriately?
 - iii.** Are there clear well-established reporting lines, authorities and responsibilities for the E(nvironment) theme activities which also enable the organization to hold people accountable for their actions like waste disposal, carbon emissions, energy efficiency?
 - iv.** How can you include fraud risks into ESG risk assessment activity to avoid greenwashing activities?
 - v.** Select and develop entity level governance controls like development of policies and procedures for ESG reporting. Develop process level controls for ESG disclosure activities like reporting of numbers under the gender and diversity KPI, number of accidents, along with technology driven controls for the IT systems used to generate the quantifiable figures.
 - vi.** Can you already leverage on the existing lines of information and communication to use and communicate control information with respect to internal and external ESG reporting?
 - vii.** Is there relevant and sufficient capability with your function to perform ESG risk assessments and regular evaluation of the designed ESG reporting internal controls framework?
- As a Risk & Controls professional, start by assessing the maturity of the internal controls framework for the relevant ESG metrics and prepare a list of gaps coming out to review that would need to be remediated to reach the end state. Focus on the Responsible, Accountable, Consulted, and Informed (RACI) Matrix

for appropriate allocation of jobs across the organization. Also perform the data readiness assessment to understand how efficiently the data can be used for disclosures and what remediations would be required on the way.

For instance, for reporting Green House Gas (GHG) emissions under Scope 1 and 2¹ – assess the process of collection of data and calculation of the numbers that would be required to be reported. Assess the key risks and validate which controls are present or would be required in the process to mitigate the key risks.

- c. Design the internal controls framework for relevant ESG metrics.** Based on the new governance structure and the as-is assessment, a new ESG internal controls framework including process, controls, reporting, technology, and data improvement recommendations for a future state Target Operating Model (TOM) should be prepared. Also include a Change Management and transformation plan for an efficient implementation process. For example:
- 1.** At an entity level, the risk function should design management controls for regular materiality assessments to monitor sustainability goals. Additionally, they should also consider cut-off procedures to ensure data is presented and calculated for correct period.
 - 2.** Another operational example – for reporting of GHG emissions under Scope 1 and 2 – the internal controls will have to be designed at a process level to ensure:
 - Completeness and accuracy of source data being used for calculation of GHG emissions in the organization
 - Complete and accurate calculation of GHG emissions
 - Transparency, consistency and relevance of GHG emissions data
- d. Implementation of the internal controls framework.** Plug in the gaps identified and extend support in executing the designed ESG reporting program and controls. This would include introducing some system implementations, training of the staff on the job and deployment of the roadmap towards ESG reporting.
- e. Sustain the framework.** This new framework must be tested by your team over time and require some overhauling as and when there are some changes in the ESG metrics as per materiality assessment. By having an appropriate internal status reporting including the testing results, data can be modified in a timely and complete manner and accurate reporting targets can be achieved.

¹ Scope 1 emissions: direct emissions from owned or controlled sources; Scope 2 emissions: indirect emissions from purchased energy; and Scope 3 emissions: indirect emissions, other than the ones under Scope 2, that occur in the value chain of an organization.

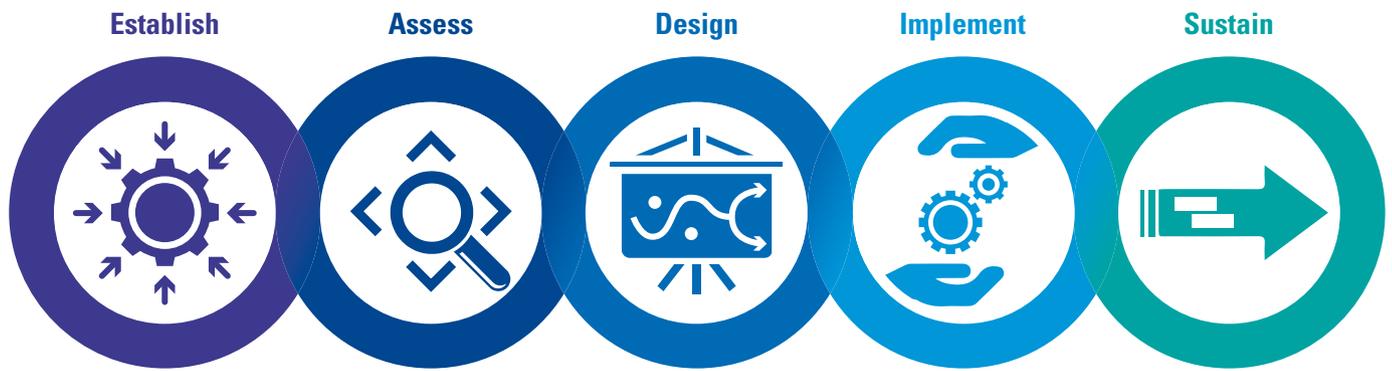


Figure 1. Your road to reporting in the ESG journey.

CONCLUSION

Risk & Controls professionals can help organizations establish a long-term vision rather than managing short-term risks. This presents a unique opportunity for the risk professionals to take an eminent role and drive the transformation within the organization towards a better future.

After carefully considering these five steps and your company's current situation, you can confidently respond to your CFO and say that "No, we currently do not have an internal controls framework for ESG reporting, but I know what to do. I will arrange a meeting to get started."

References

- [Schm22] Schmucki, P. (2022, February 1). ESG and the evolving risk management function. KPMG Switzerland Blog. Retrieved from: <https://home.kpmg/ch/en/blogs/home/posts/2022/01/esg-and-the-evolving-risk-management-function.html>
- [Zhig22] Zhigalov, A. & de Graaff, G. (2022). Emerging global and European sustainability reporting requirements. *Compact*, 2022(1). Retrieved from: <https://www.compact.nl/en/articles/emerging-global-and-european-sustainability-reporting-requirements/>

About the authors

Jeroen Bolt is a director at KPMG. He has 18 years of experience in risk consulting and is currently leading the Enterprise Risk Management (ERM), Internal Controls proposition within the GRCS department. During his working tenure, he has extensively helped clients improve their internal controls environment, including internal control implementation and roll-out projects.

Arushi Paliwal CA is a manager at KPMG. She is a risk advisory professional with over 9 years' experience in India and the Netherlands, in a variety of sectors including e-commerce, technology, hospitality, and not-for-profit. She has vast experience in internal controls framework, including large SOX transformation projects and internal audits.

Urvashi Aggarwala is a senior consultant at KPMG. Urvashi has over 6 years of experience in the financial services sector across India, UK, Vietnam and Philippines, in internal audit, risk management, regulatory and compliance services.

See also the other ESG article on Risk Management in this edition on page 20.