



Conceptual Internal Governance Framework integrating ESG principles and expectations applicable to credit institutions

Whitepaper – October 2023

Contents



Introduction

Environmental, social or governance (ESG) risks can be defined as the risk of losses arising from any negative financial impact on the institution stemming from current or prospective impacts of environmental, social or governance (ESG) factors relating to the institution's counterparties or invested assets¹.

The adoption and proliferation of the regulatory requirements tied to ESG has had a major impact on financial institutions in the European Union. Prior to considering the specific impacts of these requirements, it is important to specify that the existing environmental, social and political contexts have led to the progressive and accelerated efforts of the European Union to develop more sustainable activities and growth.

These efforts have impacted numerous stakeholders in society, particularly institutions that have been identified as key actors in the prevention and management of ESG risks. These institutions have been obliged to become ESG specialists and play an important role in providing data on climate and other ESG-related impacts on products, transactions and other financial activities to the European Union. In order to ensure adequate management of ESG risks, institutions must assign responsibility as well as reorganize and adapt their internal governance and control framework (including their risk management framework) accordingly.


The necessary reorganization stemming from the consideration of ESG risks presents significant challenges to institutions in the EU from a business model, internal governance and risk management perspective.

¹ EBA Report on management and supervision of ESG risks for credit institutions and investment firms (EBA/REP/2021/18)

As detailed in the ABBL/Deloitte whitepaper², the integration of ESG factors into the risk management framework remains complex due to various elements such as quality and availability of data along with the positioning of ESG themes within the organization (“cross cutting” or “stand alone”). As it pertains to internal governance, challenges exist in building a solid sustainable governance model with the definition of sustainable and measurable objectives whilst avoiding the risk of “greenwashing” and ensuring that the tone is correctly set at the top.

In light of the numerous regulatory requirements tied to ESG, questions have been raised relative to the impact of ESG factors and requirements on existing internal governance frameworks. The objective of this whitepaper is therefore to propose a “conceptual” framework that allows for the integration of ESG factors throughout the overall internal governance value chain (across the management body and through the three lines of defence) of banking institutions. It is important to note that the model that will be proposed is not the only possible model but simply an alternative that would allow for adequate consideration of ESG-factors (from an internal governance perspective).

The applicable and upcoming ESG-related regulatory requirements (at EU and Luxembourg-level) at the date of this whitepaper were considered. Given the complexity and ever-changing regulatory landscape, the internal governance framework must undergo constant reassessment and adjustment by banking institutions.



In order to ensure adequate management of ESG risks, institutions must assign responsibility as well as reorganize and adapt their internal governance and control framework (including their risk management framework) accordingly.

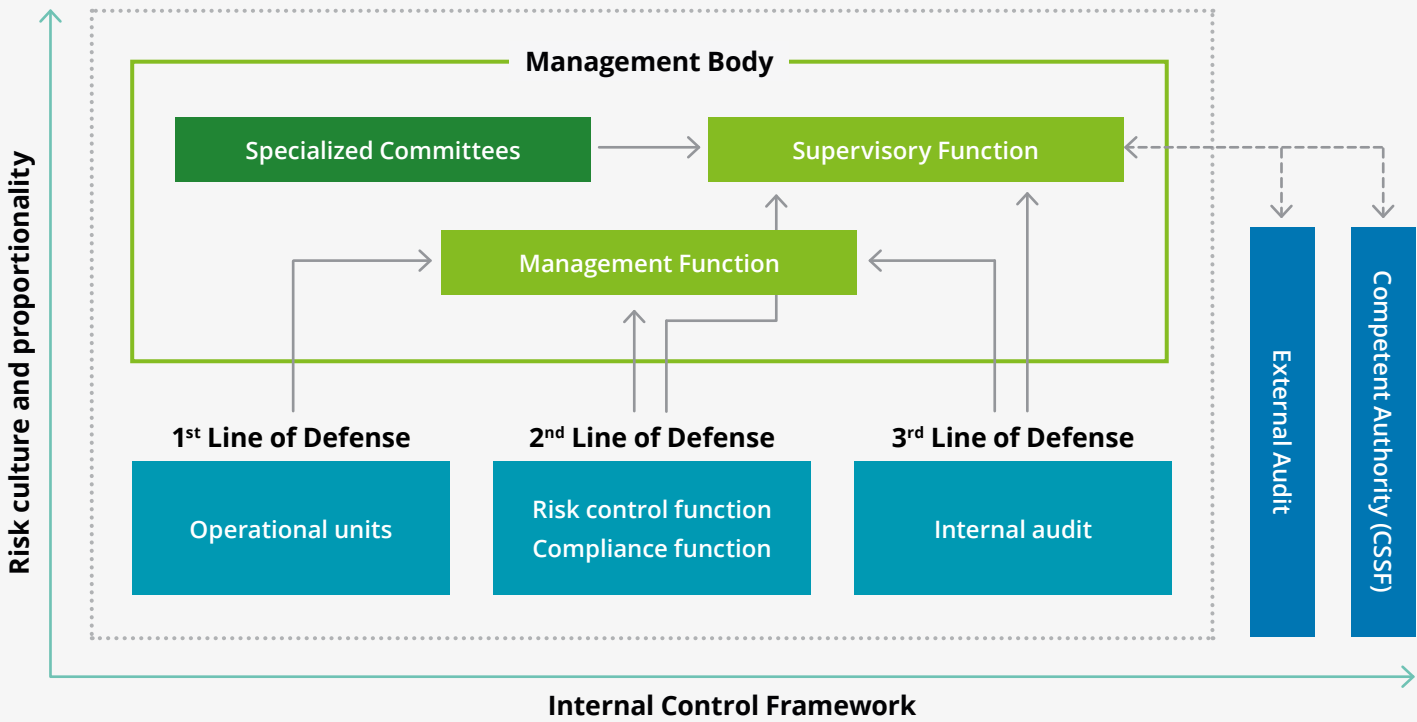
² ABBL/Deloitte whitepaper: “Integrating climate-related and environmental risks into risk management frameworks.”

Internal Governance Framework

In considering the impacts of ESG-related regulatory requirements, initial consideration should be aimed at understanding whether these requirements would fundamentally change the traditional internal governance model as prescribed in both CSSF Circular's and EBA guidelines, or rather whether these requirements would only impact the different components presently existing within the internal governance framework.

Ultimately, ESG-factors will impact the majority of the elements that compose the three lines of defence model allowing institutions to comply with regulatory requirements in terms of internal governance and control framework.

The whitepaper will therefore consider all pillars that compose an internal governance framework and the ways in which ESG-related requirements have an impact.



The Management Body in its Supervisory Function

The necessary “buy in” and subsequent adoption of all ESG-related regulatory requirements begins with the Management Body in its Supervisory Function. The Management Body is responsible for setting and communicating the institutions’ core values and expectations³.

The principle of “tone from the top” is imperative in ensuring that the core essence and rationale behind the proliferation and required implementation of ESG requirements is correctly apprehended within institutions. Should the stakeholders at the top of financial institutions not possess an appropriate understanding of ESG requirements and risks, it could ultimately lead to several detrimental consequences including greenwashing, reputational issues and non-compliance with applicable regulatory requirements.

In order to set the right “tone from the top” relative to ESG-related factors, the Management Body in its Supervisory Function has several core responsibilities. Firstly, it must ensure the correct consideration of the potential impact of ESG risks (including notably climate-related and environmental risks) on its business environment (in the short, medium and long term) in order to be able to make informed strategic and business decisions⁴. To this end, the Management Body in its Supervisory Function must review, challenge and approve the materiality assessment of climate-related and environmental risks as well as the product mix offered to the institution’s clients.

In addition, it is expected for the business strategy of the institution to also potentially shift following the consideration of ESG requirements and risks. In the perspective of adjusting its business strategy, the Management Body in its Supervisory Role ensures the identification of applicable and material ESG risks for which the risk appetite and tolerance is established. As such, key risk indicators encompassing ESG risks (both the financial and non-financial dimensions) must be elaborated for which both early warning signals and limits must be established to correctly reflect the institution’s risk appetite.

Beyond the identification of specific ESG risks, the Management Body in its Supervisory role must also ensure that the institution has adequately considered the impact of ESG risks (especially climate-related and environmental risks) on existing financial and non-financial risk categories (i.e. credit, market, liquidity and operational). These obligations include the review, challenge and approval of the ICAAP that must include new CRE-driven scenarios that are deemed material for the Bank.



All this requires the enhancement and development of the existing risk culture by ensuring the complete and accurate integration of ESG requirements in the existing risk taxonomy and framework of the institution. All staff involved in risk-taking, management or monitoring (whether at the level of the first, second or third line of defence) must be trained on new ESG requirements, in order to be fully aware of the material and relevant ESG risks applicable as well as to be accountable for the stringent respect of the ESG risk culture. Beyond this, the Management Body in its Supervisory Function must guarantee robust documentation allowing for a clear and consistent organisational and operational structure⁵. This requirement extends to ESG risks whereby the roles and responsibilities of the different stakeholders within the institution must be known and clearly documented.

The importance of the consideration of ESG risks within the risk management framework of institutions cannot be emphasized enough as it becomes a strong focus for regulators in the European Union. To this end, the European Central Bank has communicated as one of its key messages following the SREP exercise of 2022 that issues have been consistently noted with regards to the risk appetite framework and subsequent practices to manage climate-related and environmental risks⁶. The Management Body in its Supervisory Function must therefore ensure appropriate consideration and management of ESG risks.

3 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05)
4 ECB Guide on climate-related and environmental risks and CSSF Circular 21/773

5 CSSF Circular 12/552 as amended
6 ECB, Aggregated results of SREP 2022

In line with potential changes to the business strategy, institutions should consider their approach to environmentally sustainable lending practices. Should the institution have such lending practices or plan to launch them, it must elaborate a list of projects and activities, as well as the criteria, that the institution considers eligible for environmentally sustainable lending or a reference to relevant existing standards on environmentally sustainable lending that define what type of lending is considered to be environmentally sustainable⁷. The elaboration of such a list must be reviewed, challenged and approved by the Management Body in its Supervisory Function.

Relative to the suitability requirements defined in the concerned joint ESMA and EBA Guidelines⁸, the Management Body in its Supervisory Function must individually have adequate knowledge, skills and experience and must collectively be able to understand the institution's activities and main risks. Institutions should therefore extend these individual ("fit and proper") and collective suitability requirements to ESG-related elements. Concretely, this entails the necessity for members of the Management Body in its Supervisory Function to possess sufficient knowledge on ESG risks both individually and collectively.

Furthermore, the institution's remuneration policy must be consistent with its business and risk strategy, including ESG risks⁹. The Management Body in its Supervisory Function should therefore consider integrating ESG-related objectives within its variable remuneration practices.

Finally, and if applicable, the Management Body in its Supervisory Function must ensure the correct respect of all required non-financial disclosures defined in the Corporate Sustainability Reporting Directive¹⁰ (CSRD) that must be included in the annual Management Report (including ensuring consistency between financial and non-financial information reported).

Should the stakeholders at the top of financial institutions not possess an appropriate understanding of ESG requirements and risks, it could ultimately lead to several detrimental consequences including greenwashing, reputational issues and non-compliance with applicable regulatory requirements.

7 EBA guidelines on loan origination and monitoring (EBA/GL/2020/06)
8 Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2021/06)
9 Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04)
10 Directive (EU) 2022/2464

The Management Body in its Management Function

The traditional roles and responsibilities of the Management Body in its Management Function have not shifted significantly with the propagation of the importance of ESG factors. The Management Body in its Management Function must continue to engage actively in the business development of the institution and play an important role in informed decision-taking¹¹.

To this end, it must revisit its existing business strategies set out by the Management Body in its Supervisory Function, discuss on the challenges of these strategies, and ensure precise and regular reporting of ESG risks to the Management Body in its Supervisory Function.

In line with the suitability requirements described above, these remain prevalent for the Management Body in its Management Function.

The Function must ensure that it possesses sufficient knowledge on ESG risks and factors allowing it to:

- Take informed decisions;
- Correctly implement ESG business strategies;
- Advise and guide the Management Body in its Supervisory Function;
- Implement sufficient procedures allowing for the mitigation of operational and reputational events stemming from ESG-related deficiencies.

The fact that the historic responsibilities of the Function have not significantly shifted as a direct result of ESG regulatory requirements does not negate the vital importance of its implication in ESG-related processes. The Function is in charge of the day-to-day management of the institution and must ensure that an “ESG tone” is set for the rest of the institution to follow.



11 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05)

First Line of Defence

In light of the proliferation of regulatory requirements on ESG, numerous important adjustments must be made by different stakeholders at the level of the first line of defence. For the purpose of this whitepaper, five significant impacts have been identified and will be considered extensively.

Accounting and Finance

Prior to detailing the impacts that ESG-related requirements have had on the accounting and finance function, it is worth noting that debate exists relative to the appropriate classification of the function within the traditional three lines of defence model. For the sake of this whitepaper, the accounting and finance function is considered to be situated in the first line of defence.

The accounting and finance function has and continues to undergo development in the adoption of ESG-related factors. In November 2021, the IFRS foundation announced the creation of the International Sustainability Standards Board (ISSB)¹². The ISSB has as key focus the development of standards for sustainability disclosures. This development marked the ambition and implication of the IFRS foundation in the enhancement and propagation of sustainability requirements in the field of accounting. IASB is also currently exploring the manners in which to render mandatory the reporting of climate-related Risks in the Financial Statements¹³.

Furthermore, the EU Action Plan on Financing Sustainable Growth¹⁴ has as one of three main objectives to foster transparency and long-termism in financial and economic activity through notably the strengthening sustainability disclosures and accounting rule-making. This gives credence to the general market expectation which is that important ESG-related requirements will continue to develop and influence the accounting and finance domains.

Concretely, and to begin with, institutions must consider the impact of climate-related and environmental risks on their existing Expected Credit Losses ("ECL") calculation models. For instance, probabilities of default (PD) and loss given default (LGD) of exposures within sectors or geographies that are vulnerable to natural disasters might be impacted (i.e. through lower collateral valuation, lower profitability expectations due to property damages caused by physical environmental impacts etc.).

The impacts of climate-related and environmental factors (i.e. physical or transition risks) on credit risk is an element that is non negligible when considering accounting provisions and the valuation of assets. Climate-related and environmental risks may lead to defaults of businesses or households and/or collateral depreciation which should be accounted for.

In addition, the accounting and finance function must now assist in the production of specific disclosures (depending on the applicability of these considering the type and size of the financial institution) requiring extensive data captured through structured data

sets. Examples include disclosures to be made with respect to the Non-Financial Reporting Directive¹⁵ (NFRD) and in the near future Corporate Sustainability Reporting Directive¹⁶ (CSRD).

A need for new extensive data sets implies a need to implement controls ensuring accurate and complete data. As such, the accounting and finance function must design and implement new controls ensuring that the disclosures made are of quality.

The importance of implementing a robust control framework cannot be underestimated in particular in light of the limited assurance requirement that will be introduced in the Corporate Sustainability Reporting Directive¹⁷ (CSRD). External auditors will be tasked with auditing sustainability information so as to give limited assurance over its accuracy and reliability. The accounting and finance function must therefore be prepared to demonstrate the completeness and accuracy of the disclosures with which it assists.

Credit Process

Within the scope of the implementation and maintenance of environmentally sustainable lending practices, the credit department of the Bank is expected to make a number of changes to its existing processes.

To begin with, the Bank must collect information about climate-related and environmental or sustainable business objectives of the borrowers. The observed market practice thus far in Luxembourg has been the elaboration, by credit departments, of an 'ESG questionnaire' serving as purpose the

gathering of ESG-related information from current or prospective clients. The questionnaire should complement the assessment of the credit capacity within the credit application on a case by case basis. Following the completion of the ESG questionnaire, an ESG score is determined and subsequently integrated into the assessment of the counterparty risk (i.e. in terms of probability of default)¹⁸.

Furthermore, and in accordance with the EBA Guidelines on loan origination and monitoring¹⁹, the credit department should proceed with an assessment of the borrower's alignment with the institutions list of projects, activities and criteria eligible for qualification as environmentally sustainable lending. As a reminder, this list and criteria are elaborated by the Management Body in its Supervisory Function.

Beyond the initial assessment, credit departments must also ensure that the borrowers are willing and able to report on the allocation of the funds granted towards the environmentally sustainable projects and activities. This has as objective to allow the credit department to perform ongoing monitoring so as to ensure that the funds granted to the borrowers are indeed being put towards environmentally sustainable projects and activities.

Finally, all of the above mentioned objectives encourages change to the credit operating processes which include the underlying assessment and data collection processes. As such, modification of credit policies and procedures should occur to reflect the ESG-related considerations.



12 <https://www.ifrs.org/groups/international-sustainability-standards-board/>
13 <https://www.ifrs.org/projects/work-plan/climate-related-risks-in-the-financial-statements/>

14 Communication from the Commission – Action Plan: Financing Sustainable Growth (COM(2018) 97)
15 Directive 2014/95/EU
16 Directive (EU) 2022/2464
17 Directive (EU) 2022/2464
18 ABBL/Deloitte whitepaper: "Integrating climate-related and environmental risks into risk management frameworks."
19 EBA guidelines on loan origination and monitoring (EBA/GL/2020/06)

Product Governance

Numerous changes relative to product governance have occurred as a direct result of the consideration of ESG-related factors that have a direct impact on various members of the first line of defence. These considerations were rendered mandatory following the sustainability-related amendments to MiFID through both Directive (EU) 2021/1269 (integration of sustainability factors into the product governance obligations) and Regulation (EU) 2021/1253 (integration of sustainability factors, risks and preferences into certain organisational requirements and operating conditions for investment firms).

Client Sustainability Preferences

As a result, a subsequent step to the traditional suitability assessments has been added. Moving forward, a mandatory collection of client sustainability preferences is required as well as a revision of financial instruments that the client can choose from to integrate into their investments that will qualify as sustainable (i.e. environmentally sustainable taxonomy-compliant (TR), minimum proportion of sustainable investments (SFDR) or Principle Adverse Impact determined by the client).

Sustainability Preferences

In addition and in case of investment advice, a sustainability assessment must now occur. Only financial products that qualify as “sustainability preferences” and meet the client’s choice of sustainability preferences can be advised. In the case of advice for financial products that do not qualify into the client’s sustainability preferences, these must be disclosed to the client by the relationship managers.

Pre-trade Information

An amendment to the pre-trade investment advice that needs to be disclosed to the clients has also occurred. This information must now include the sustainability factors taken into consideration in the selection process of financial instruments. Subsequently, this information must therefore now be integrated into pre-trade disclosures to clients.

Target Market

Finally, the EU directive brings about required integration of sustainability factors within the target market assessments that must be performed by institutions in the case of both manufacturers and distributors.

Beyond ensuring that the additional required ESG-related provisions are appropriately considered and formalized, members of the first line of defence play a primary role in supporting the European Commission in achieving one of its core objectives in its Action Plan ‘Financing Sustainable Growth’²⁰ which is to reorient capital flows towards sustainable investments. Should members of the first line of defence subscribe to the ESG risk culture of the institution, meaningful impacts are expected to happen at this level.

Risk Control and Self-Assessment

The required embedding of ESG-related factors at all levels of institutions’ processes entails a necessary adjustment of the risk control and self-assessment (“RCSA”) matrices. This adjustment comes in the form of the identification of new operational risks based on the ESG-related processes as well as the elaboration or amendment



of controls to ensure that these allow institutions to effectively mitigate all existing operational risks including the newly embedded ESG-related aspects.

Disclosures

The following section will consider an example of specific ESG-related disclosures but it is important not to underestimate the impact of ESG factors on other existing reports (i.e. the financial statements).

In light of all of the regulatory requirements encompassing required sustainability disclosures (i.e. Sustainable Finance Disclosure Regulation (SFDR)²¹ and the EU Taxonomy²²), and should these be applicable, the first line of defence has specific roles and responsibilities relative to the preparation of various disclosures. Overall, the first line of defence must be in a position to capture all data necessary for the applicable disclosure requirements through a clear taxonomy and data architecture, set up throughout the information system of the institution fostering data quality and timeliness of the information.

For instance, and in line with both SFDR and the EU Taxonomy, products

must be classified according to their nature. As per the SFDR, article 6 products (“neutral products”) are those for which the incorporation of ESG is limited to consideration of sustainability risks, if at all. Article 8 products (“light green products”) are those that consider sustainability risk and promote environmental and/or social characteristics. Finally, article 9 products (“dark green products”) are those that consider sustainability risk, have a sustainable investment objective and respect the “do no significant harm” (DNSH) principle across the whole portfolio.

Based on the classification of the institutions’ products, different disclosures are required as per SFDR, EU Taxonomy and the regulatory technical standards supplementing SFDR²³.

The expectation is for the first line of defence to establish and document the classification of products according to their nature (article 6, article 8 or article 9). Likewise, and following the classification process, pre-contractual documents for article 8 (light green) and article 9 (dark green) products must be prepared. The product-level website disclosures for these products must then follow.

Moreover, the first line of defence must produce the mandatory periodic reports requested of all institutions subject to SFDR and the EU Taxonomy.

Additionally, as per the CRR II²⁴, large institutions issuing securities trading on a regulated market of an EU Member State are required to disclose prudential information on ESG risks, including physical and transition risks. With the assistance and input of the Risk Management Function, the first line of defence must prepare this Pillar III reporting.

Finally, and in line with what has been described above in this whitepaper, institutions must design and implement robust controls. These controls must ensure that the data used in the different sustainability disclosures is complete and accurate. The first line of defence must play a part in defining and subsequently implementing this control framework.

Head of Sustainability

Based on the above, institutions should consider appointing a person in charge of different ESG-related topics at the level of the first line of defence in order to ensure consistency, commitment and expertise.

20 COM(2018) 97 final

21 Regulation (EU) 2019/2088
22 Regulation (EU) 2020/852 of 18 June 2020
23 Regulation (EU) 2022/1288
24 Regulation (EU) 2019/876

To this end, various institutions have put in a place a head of sustainability (also referred to as the “Chief Sustainability Officer” depending on the institution). This individual is a member of the first line of defence and may for instance be functionally tied to a Corporate Social Responsibility or a specific sustainability department.

Responsibilities of the head of sustainability may include the following:

- Advisory to the different members of the first line of defence on ESG requirements;
- Control and oversight mechanism for all ESG-related documentation (i.e. SFDR and EU Taxonomy periodic reports, product classification, disclosures etc.);
- Main point of contact for the second and third lines of defence for all ESG-related matters implicating the first line of defence. For example, various disclosures (such as the CSRD evoked above) require the joint input of departments at the level of the first and second lines of defence. The expectation would therefore be that the head of sustainability liaises with the relevant departments and gathers all required information;
- Communication and nurturing of relationships with external stakeholders such as NGOs²⁵.

The individual in question must have strong transversal knowledge covering numerous different domains impacted by ESG regulatory requirements and be empowered to impact the institution

and effectively perform their duties. The person must report directly to the Management Body (in its management and supervisory role) with a primary person of contact being the CEO.

Overall, and whilst the required considerations of ESG-related factors by the first line of defence appear extensive, it is worth noting that the fundamental roles and responsibilities do not shift significantly. They are adapted to embed ESG requirements and cope with the new business strategy that must foster ESG-compliance products and services including credit and investment services.

Considering for example the roles and responsibilities of the first line of defence within the risk appetite framework as detailed by the Financial Stability Board²⁶, these remain prevalent but are enlarged to include ESG risks.

Concretely, the first line of defence is accountable for the effective management of ESG risks within the individual business units including the correct embedding of ESG risks into the operational activities of the institution thus ensuring a prudent day to day management of ESG risks. Furthermore, the implementation of controls and processes enabling the institution to be able to effectively identify, monitor and report against allocated ESG risk limits must first occur at the level of the business units. Finally, the consideration of ESG factors further accentuates the importance of cooperation and communication with the second line of defence.

The first line of defence is accountable for the effective management of ESG risks within the individual business units including the correct embedding of ESG risks into the operational activities of the institution.

25 Deloitte whitepaper, How Chief Sustainability Officers can drive the banking sector’s sustainability efforts
26 FSB: Principles for An Effective Risk Appetite Framework

Second Line of Defence – The Compliance Function

As a second line of defence function, the Compliance Function is responsible for exercising oversight on the business lines and internal units in its scope. This oversight extends to the new ESG regulatory requirements that must be considered by first line of defence stakeholders.

The present section of the whitepaper has as main objective to consider the roles and responsibilities of the Compliance Function relative to ESG requirements. Ultimately, and as observed on the market, institutions are turning to the Compliance Function to ensure appropriate consideration of notably all non-financial dimensions of ESG risk (i.e. the social and governance aspects) and to provide the necessary level of comfort to the Management Body on these dimensions. This has entailed the necessary adaptation of six of the key roles and responsibilities of the function.



Regulatory Watch



Compliance Risk Assessment



Compliance Monitoring Activities



New Product Approval Process



Advisory and Training



Reporting to Key Stakeholders



Regulatory Watch

Given the fast developing regulatory requirements tied to ESG, the Compliance Function must ensure appropriate and timely identification of upcoming ESG-related requirements susceptible to having an impact on the institution. The objective being to report these to the Management Body allowing the institution to act proactively in addressing upcoming regulatory requirements.

Compliance Risk Assessment

Regulator expectations and subsequently market practice relative to the roles and responsibilities of the Compliance Function have shifted over the past decade. Institutions are re-conceptualising the internal organization of several of their key compliance themes (such as AML/CFT). The expectation is that whilst the first line of defence is implicated in the execution of tasks, the Compliance Function is implicated in the oversight of these tasks allowing it to provide necessary observations and recommendations to ensure progress and adequate process design embedding ESG domains.

The aforementioned oversight can occur in several ways, one of which is the compliance monitoring program in which the control activities of the Compliance Function are listed. Regulator expectations, whether it be at the level of Luxembourg through the Commission de Surveillance du Secteur Financier (“CSSF”) or at EU-level, is that the Compliance Function should develop control activities according to a risk-based approach.

As such, the Compliance Function should identify and assess all applicable regulatory risks to which the institution is subject. Given the proliferation of ESG-related regulatory requirements, the Compliance Function must presently revisit its compliance risk catalogue so as to identify, integrate and assess all relevant ESG risks on a continuous basis through notably its regulatory watch process. The Compliance Function must be able to apprehend the ESG compliance risk profile of the institution in order to subsequently ensure the existence and eventually creation of an appropriate internal control framework having as objective the mitigation of applicable ESG risks.

Compliance Monitoring Activities

In line with what has been described in the whitepaper above, the Compliance Function following the identification and assessment of the different applicable ESG compliance risks should elaborate and implement monitoring activities to oversee the correct management of these risks.

Typically, compliance monitoring has been synonymous with the compliance monitoring program in which the Compliance Function lists all compliance controls along with a frequency and schedule of execution based on the residual level of its regulatory risks. As such, and given the ESG risks stemming from regulatory requirements, the Compliance Function should design and integrate compliance controls within the scope of its compliance monitoring program.

That being said, compliance monitoring should not be solely limited to the execution of the compliance monitoring program. Market practice has shed light on an additional monitoring activity which consists in the elaboration and ongoing follow-up of compliance risk

indicators encompassing applicable regulatory risks. An option for the Compliance Function to execute its oversight ensuring the correct design and implementation of mitigation measures relative to ESG risks is therefore to elaborate a list of ESG indicators with a focus on the non-financial dimension of ESG. These compliance risk indicators are then followed up on a predetermined frequency and reported to the relevant stakeholders as needed.

New Product Approval Process

Prior to the launch of new products, activities or business relationships, the Compliance Function must proceed with the identification and assessment of any compliance risks arising²⁷. This requirement should ensure that the analysis performed includes ESG domains and characteristics. The Compliance Function must proceed with the verification and review of the fact that these new products/ activities/business relationships comply with the institutions ESG framework and standards.

Furthermore, and as will be described below, the Compliance Function has a role of advisor for any members of the institution in the case of ESG-related queries prior, during or after the launch of new products/activities/ business relationships.

Advisory and Training

The Compliance Function must act as an advisor to all members of the institution, from the Management Body to the business units at the level of the first line of defence, for all ESG compliance-related subjects. In addition, the Compliance Function must raise awareness within the institution on the aforementioned ESG subjects. To this end, trainings must be organized and delivered by the Compliance Function (potentially in collaboration with the Risk Management Function).

Reporting to Key Stakeholders

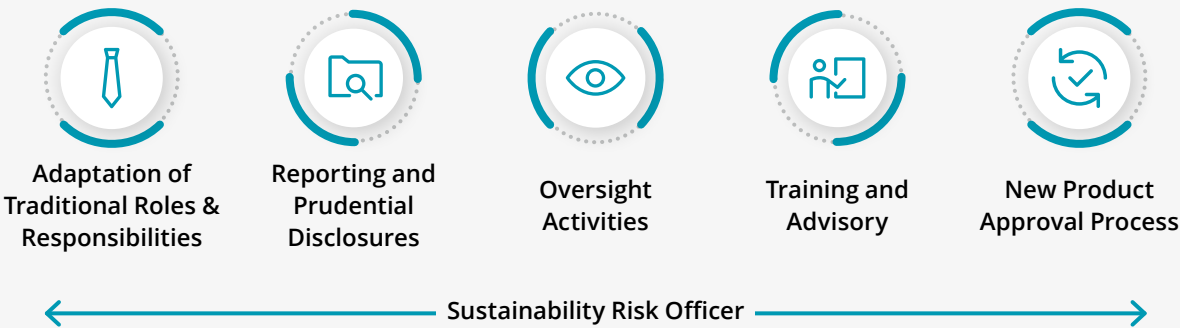
Expectations relative to the reporting that the Compliance Function must make to key stakeholders (i.e. the Management Body) have not changed. The function must be able to capture and report pertinent and accurate information relative to the ESG compliance risk profile of the institution, the non-financial ESG compliance indicators elaborated and finally, on the status of execution of the compliance monitoring activities over the ESG-related topics that are in its scope. Should any weaknesses or attention points come to light during the monitoring activities performed, adequate reporting to the Management Body along with an action plan and timeline for the remediation must follow.

27 CSSF Circular 12/552 as amended



Second Line of Defence – The Risk Management Function

As observed on the market, at the level of the second line of defence, the Risk Management Function is expected to have a vital contribution to the ESG requirements in particular the assessment of ESG risks and climate-related and environmental impacts. To begin with, ESG requirements have introduced both specific ESG risks but has also impacted numerous existing risk classes. As such, the consideration and integration of these impacts has necessitated (and will continue to necessitate) numerous and stringent analyses performed by the Risk Management Function allowing it to correctly apprehend and advise the Management Body on ESG risks.



Furthermore, of the three components composing ESG (i.e. environmental, social and governance), the environmental component has been the most targeted through the development of a stringent regulatory requirements. These developments have required institutions to quantify climate-related and environmental risks thus de facto implicating the Risk Management Function. It is worth noting that as the regulatory requirements tied to the social and governance components continue to be developed, this may further foster and accelerate the implication of the Risk Management and Compliance Functions to ensure adequate treatment of ESG-related matters.

In line with the development of the regulatory requirements attached to the environmental component, this has subsequently led to the necessary integration of these within reports that have traditionally required big contributions by the Risk Management Function including the ICAAP and Pillar III reporting.

The present section of the whitepaper has therefore as objective to consider the main impacts that ESG requirements has on the Risk Management Function.



Adaptation of Traditional Roles and Responsibilities

For the sake of this whitepaper, the roles and responsibilities as described in the EBA Guidelines on internal governance (EBA/GL/2021/05) will be taken. That being said, it is to be noted that CSSF Circular 12/552 as amended reflects these key principles and could have been considered instead in this section.

The role of the Risk Management Function within the scope of risk strategy and decisions has become more vital. The function has the responsibility to communicate all relevant ESG risk-related information to the Management Body in its Supervisory Function to allow for a correct update of the risk appetite statement. Likewise, the function must

assess the robustness, feasibility and appropriateness of the elaborated ESG risk strategy and appetite. This assessment must incorporate a stress test program that includes material ESG risks into both baseline and adverse scenarios²⁸.

Furthermore, and as evoked above, the Risk Management Function must act as a key advisor to the Management Body allowing it to take informed and coherent decisions on ESG risk strategies and risk appetite. The Risk Management Function should for instance prepare the materiality assessment of ESG risks and present it to the Management Body in its Supervisory Function for review, challenge and approval. Additionally, it is recommended for the function to prepare a gap analysis or action

plan allowing it to design a climate risk management framework in line with supervisory expectations and best market practices that is then also presented to the Management Body in its Supervisory Function.

Relative to the revised business strategy that will have been determined by the institution, the Risk Management Function must be capable of challenging the positions taken by the Management Body in its Supervisory Function with respect also to ESG risks.

Finally, and in line with the function's basic roles and responsibilities of identification, assessment, measurement, monitoring, management and reporting of all risks to which the institution is exposed, the Risk Management Function must identify material ESG risks and consider how these also impact existing risks (i.e. credit, market, liquidity, operational, third-party etc.)

Reporting and Prudential Disclosures

The expectation of the Risk Management Function is for its implication in the preparation of different regulatory disclosures and reporting.

The Risk Management Function must have an active role in the preparation of the Pillar III report by providing the first line of defence with all relevant risk-related data and any advisory needed.

Likewise, adjustments to the annual ICAAP/ILAAP reports are expected through the assessment of the impact of climate-related and environmental risks on both the institution's liquidity and capital adequacy from an economic and a normative perspective²⁹. The Risk

Management Function must ensure the correct integration of CRE risks within the ICAAP/ILAAP reports.

In addition, and relative to the Non-Financial Reporting Directive³⁰ and Corporate Sustainability Reporting Directive³¹ (once applicable), the Risk Management Function must ensure that it provides various required input and data necessary for the successful completion of these disclosures.

Oversight Activities

Within the scope of the controls and other oversight activities performed by the Risk Management Function, respect of ESG-related requirements must be verified and assured. For instance, the Risk Management Function should perform control activities on the sustainability disclosures produced by the first line of defence of the Bank so as to ensure that all risk-related elements have been appropriately captured and that the ESG Risk Management Framework at the level of the first line of defence is operating as intended. In addition, depending on the allocation of roles and responsibilities between the Compliance Function and the Risk Management Function, the Risk Management Function may execute controls on the correct classification of products and the correct integration of ESG requirements into product governance.

Training and Advisory

In line with what was stated for the Compliance Function, the Risk Management Function also has an important role to play as advisor and must organize trainings on ESG risks. So as to avoid redundancy with the



28 EBA Action plan on sustainable finance

29 ECB Guide on climate-related and environmental risks and CSSF Circular 21/773
30 Directive (EU) 2014/95
31 Directive (EU) 2022/2464

trainings facilitated by the Compliance Function, consensus on the scope must be agreed between these two second line of defence functions. Typically, the Risk Management Function will cover in detail the financial risks stemming from ESG whilst the Compliance Function will cover the non-financial risks. It would be advisable to centralize all content and potentially deliver common trainings with members of both the Compliance and Risk Management functions.

Trainings should be dispensed to members at all levels of the institution, from the Management Body to the first and second lines of defence.

New Product Approval Process

Prior to any material changes in the institution through for instance the proposition of new products, services, processes etc., the Risk Management Function must assess the impacts of such changes on the institution's risk strategy (ensuring that the ESG components that will have been embedded are considered and respected appropriately) and risk appetite (embedding the material ESG risks). The implication of the Risk Management Function within the new product approval process is therefore of high importance in particular in the case of the launch of a new "green" product/ service by the institution.

General Observations

Whilst the head of sustainability (also referred to as the "Chief Sustainability Officer" depending on the institution) is situated at the level of the first line of defence, and in line with market practice, it is recommended for institutions to have in place a sustainability risk officer at the level of the second line of defence. The objective being for the Risk Management Function to have a member possessing specialized knowledge on ESG risks and the management and controls of these.

The sustainability risk officer is to be implicated on all ESG risk-related dimensions such as:

- The identification of ESG risks;
- Materiality assessments;
- Elaboration of CRE-driven scenarios in the ICAAP/ILAAP;
- Implication in required ESG reporting (i.e. Pillar III);
- Organization of trainings;
- Point of reference for any ESG risk-related inquiries (advisory role);
- Preparation of internal ESG reporting.



Third Line of Defence – The Internal Audit Function

In line with one of the key challenges stated in the introduction of this whitepaper, the approach of integrating ESG factors within internal audit work has differed across banking institutions in Luxembourg thus far.

Some internal audit functions have considered ESG-related requirements by embedding them into different existing working programs encompassing the different internal audit units that are typically considered (i.e. Internal Governance, Credit Process, Product Governance/MiFID etc.). Other internal audit functions have elected to keep ESG-related requirements separate from traditional reviews by creating a new ESG internal audit unit that encompasses all of the ESG regulatory requirements.

Ultimately, the optimal solution may represent a combination of these two approaches. On the one hand, modification of existing internal audit units and on the other hand, the creation of a specific ESG internal audit unit.



Relative to the first option, the following internal audit units may be amended for instance:

- The internal governance working programs in order to capture all ESG-related impacts to the internal governance framework (reviews centred around the Management Body, internal control functions etc.);
- The product governance/MiFID working programs to include new and emerging ESG-related requirements;
- The New Product Approval Process working programs to ensure that the ESG framework has been respected as new products/activities have been launched;
- The ICAAP/ILAAP working program to ensure that ESG-related scenarios have been dully added;
- The credit review process working program to ensure that all ESG regulatory requirements have been integrated into the credit framework and appropriately captured by the credit department;
- The remuneration policy review working program to verify whether variable remuneration considers ESG-related performance targets;
- The accounting and finance working program to ensure that all ESG-related factors have been considered.

Beyond the elements that induce straight forward modifications of existing internal audit working programs, it may be advisable to also create a specific ESG internal audit unit (corresponding to option 2 above). The objective being to ensure that in depth thematic internal

audit work is performed on specific ESG topics. This would lead to a guarantee that the internal audit function will allocate more time and resources on ESG reviews. One such thematic review may for example be to consider regulatory disclosures and reports that are produced by the institution (i.e. SFDR and EU Taxonomy, Pillar III, TCFD etc.)

Finally, and beyond the consideration of ESG-related requirements in internal audit plans, internal auditors must ensure that they receive sufficient trainings on ESG topics allowing them to properly capture all requirements in their internal audit working programs and enabling them subsequently to execute the internal audit work.

In this context, and based on observed market practice, the common tendency is for internal audit functions to call upon external firms possessing the required knowledge (of both internal audit and ESG-related requirements) to assist them in their thematic ESG reviews under a co-sourcing arrangement. Given the relative recency of ESG requirements as well as the continued proliferation of these, the use of subject matter specialists appears to be, at least on the short-term, an effective way to ensure that ESG topics are correctly considered by the internal audit function and also allows for training and development of internal auditors working alongside professionals who have specialized knowledge on the subject.





Conclusion

The present whitepaper explored manners in which to integrate the current ESG-related requirements into internal governance frameworks. Ultimately, and irrespective of the ways in which institutions elect to consider ESG, it is apparent that ESG risks are cross functional and thus impact numerous key internal governance dimensions.

Given the ever evolving and growing regulatory requirements encompassing ESG risks, it is important for institutions to constantly assess and adapt their target operating models allowing them to correctly capture and manage these risks.

At the date of this whitepaper, the “environmental” dimension of ESG has undergone the most stringent development from the regulator’s perspective, through the publication of regulatory requirements tied to the assessment of climate-related and environmental risks as well as extensive reporting expectations requiring large and precise data sets.

That being said, it is to be expected that further development of regulatory requirements also encompassing the “social” and “governance” dimensions will follow which will require further adaptation at all levels of institutions. To this end, the Compliance Function, in its role of management of the non-financial risk-dimensions of institutions, will be the internal control function that may be most impacted moving forward.

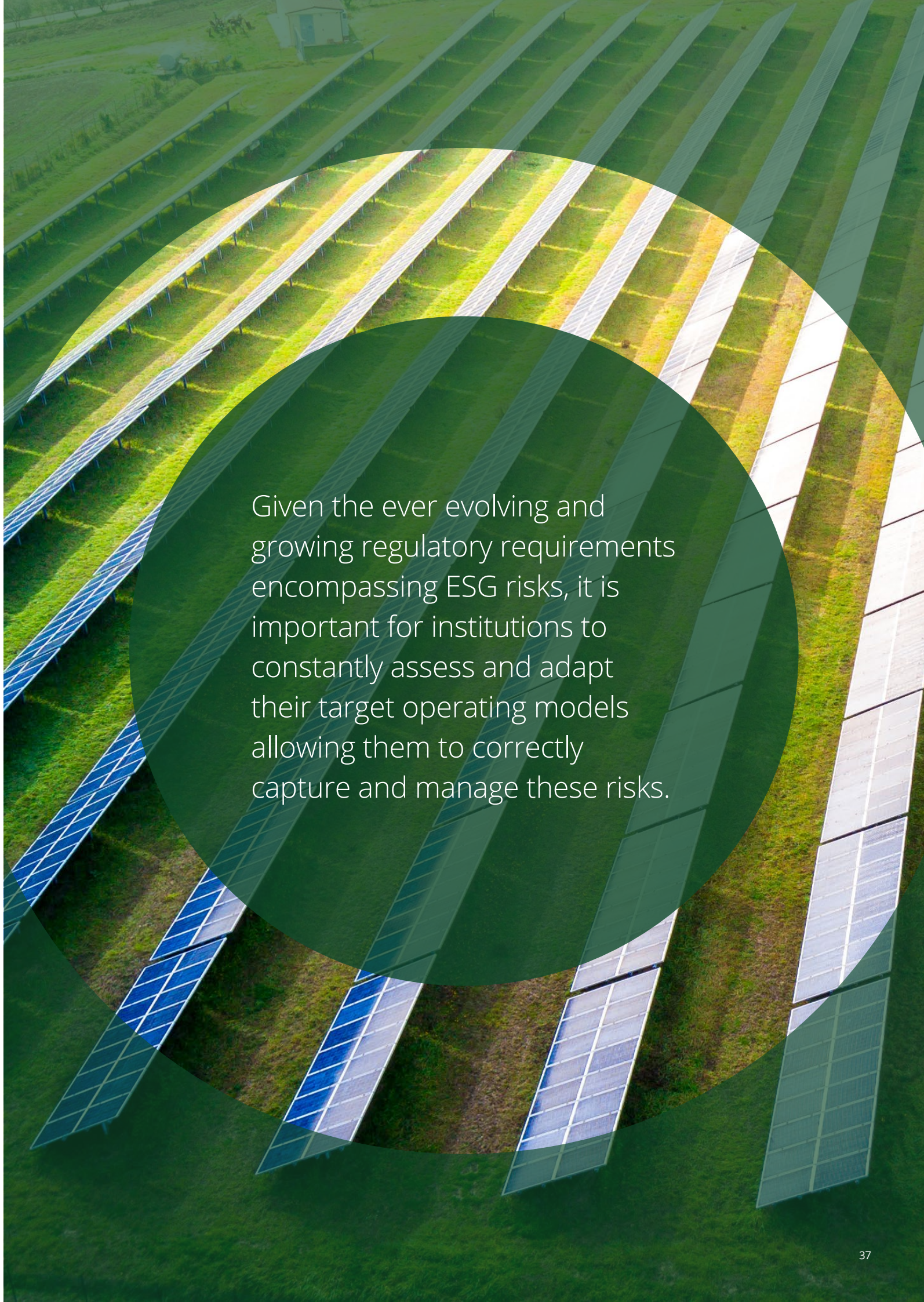
Irrespective of this eventuality, it is clear that institutions must rely on all of their lines of defence to correctly identify, assess, measure, monitor, manage and report on all ESG risks and the impact of these on existing risk classes (whether financial or non-financial).

At the level of the Management Body, the expectation is for the business environment and strategy to be constantly reassessed in light of new ESG-related regulatory requirements.

Furthermore, and whilst ESG risks do indeed impact multiple facets of an institution, they do not fundamentally change the traditional internal governance framework applicable to banking institutions. They require an adaptation of traditional roles and responsibilities, a high level of agility and capacity for change within institutions along with the potential creation of new positions ensuring a sufficient level of ESG-related expertise amongst the institution's personnel.

The model proposed in this whitepaper has placed a Head of Sustainability (or Chief Sustainability Officer) at the level of the first line of defence with a sustainability risk officer at the level of the second line of defence. Whilst this is only one of the many potential ways of ensuring the presence of human resources within an institution possessing the required ESG knowledge, it has become apparent that a new profile of talent is required in order to ensure the correct management of ESG risks.

To conclude, the proliferation of ESG-related regulatory requirements has impacted the banking industry substantially. However, there is reason to believe that the early stages of the adoption and adhesion to these regulatory requirements will be the most challenging for banking institutions. Progressively, new systems will be put in place ensuring an appropriate internal governance structure (in which the roles and responsibilities of the different stakeholders are clearly defined and documented), improvements in the quality and ease of access of ESG-related data and the definition and implementation of a robust ESG risk culture. Once all of this is in place, and irrespective of the upcoming changes in ESG-related regulatory requirements, institutions will be better adapted to respond rapidly and appropriately.



Given the ever evolving and growing regulatory requirements encompassing ESG risks, it is important for institutions to constantly assess and adapt their target operating models allowing them to correctly capture and manage these risks.

References

1. ABL/Deloitte whitepaper, (2022), Integrating climate-related and environmental risks into risk management frameworks.

2. Commission de Surveillance du Secteur Financier, (2012), CSSF Circular 12/552 as amended by Circulars CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647, CSSF 17/655, CSSF 20/750, CSSF 20/759, CSSF 21/785 and CSSF 22/807 - Central administration, internal governance and risk management.

3. Commission de Surveillance du Secteur Financier, (2021), CSSF Circular 21/773 On the Management of Climate-related and Environmental Risks.

4. Deloitte Whitepaper, (2022), The big picture: how Chief Sustainability officers can drive the banking sector's sustainability efforts.

5. European Banking Authority, (2021), EBA Report on management and supervision of ESG risks for credit institutions and investment firms (EBA/REP/2021/18).

6. European Banking Authority & European Securities and Market Authority, (2021), Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (EBA/GL/2021/06) (ESMA35-36-2319).

7. European Banking Authority, (2020), EBA guidelines on loan origination and monitoring (EBA/GL/2020/06).

8. European Banking Authority, (2021), EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05).

9. European Banking Authority, (2021), EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04).

10. European Banking Authority, (2021), Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05).

11. European Central Bank, (2020), ECB Guide on climate-related and environmental risks - Supervisory expectations relating to risk management and disclosure.

12. European Central Bank, (2023), Aggregated results of SREP 2022.

13. European Commission, (2018), Communication from the Commission – Action plan: Financing Sustainable Growth (COM(2018) 97).

14. European Commission, (2022), Commission Delegated Regulation (EU) 2022/1288 of 6 April 2022 supplementing Regulation (EU) 2019/2088 of the European Parliament and of the Council with regard to regulatory technical

standards specifying the details of the content and presentation of the information in relation to the principle of 'do no significant harm', specifying the content, methodologies and presentation of information in relation to sustainability indicators and adverse sustainability impacts, and the content and presentation of the information in relation to the promotion of environmental or social characteristics and sustainable investment objectives in pre-contractual documents, on websites and in periodic reports.

15. European Parliament and the Council of the European Union, (2014), Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups.

16. European Parliament and the Council of the European Union, (2019), Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector.

17. European Parliament and the Council of the European Union, (2019), Regulation (EU) 2019/876 of the European Parliament and of the Council of 20 May 2019 amending Regulation (EU) No 575/2013 as regards the leverage ratio, the net stable funding ratio, requirements for own funds and eligible liabilities, counterparty credit risk, market risk, exposures to central counterparties, exposures to collective investment undertakings, large exposures, reporting and disclosure requirements, and Regulation (EU) No 648/2012.

18. European Parliament and the Council of the European Union, (2020), Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 of the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088.

19. European Parliament and the Council of the European Union, (2022), Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/24/EU, as regards corporate sustainability reporting.

20. Financial Stability Board, (2013), Principles for An Effective Risk Appetite Framework.

21. IFRS Foundation, (2023), Climate-related and Other Uncertainties in the Financial Statements (Available at: <https://www.ifrs.org/projects/work-plan/climate-related-risks-in-the-financial-statements/#:~:text=The%20IASB%20decided%20that%20the,present%20agreed%20with%20this%20decision.>)

39

Key contacts



Francesca Messini
Partner | Sustainability Leader
Mobile: +352 661 451 744
Email: fmessini@deloitte.lu



Bertrand Parfait
Partner | Risk Advisory
Mobile: +352 621 213 269
Email: bparfait@deloitte.lu



Marc Abou Jaoude
Manager | Risk Advisory
Mobile: +352 621 962 120
Email: maboujaoude@deloitte.lu





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.