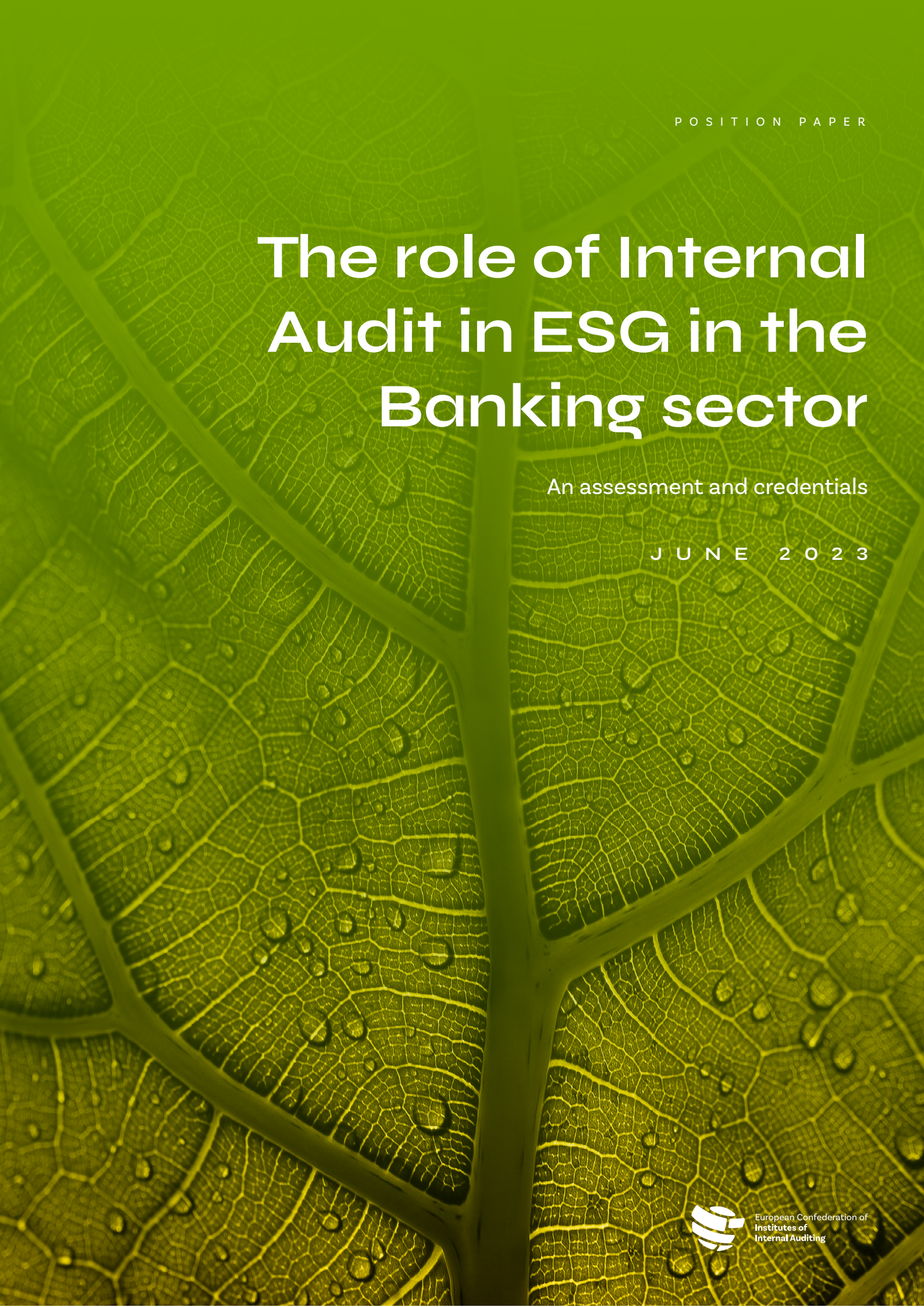
POSITION PAPER

The role of Internal Audit in ESG in the Banking sector

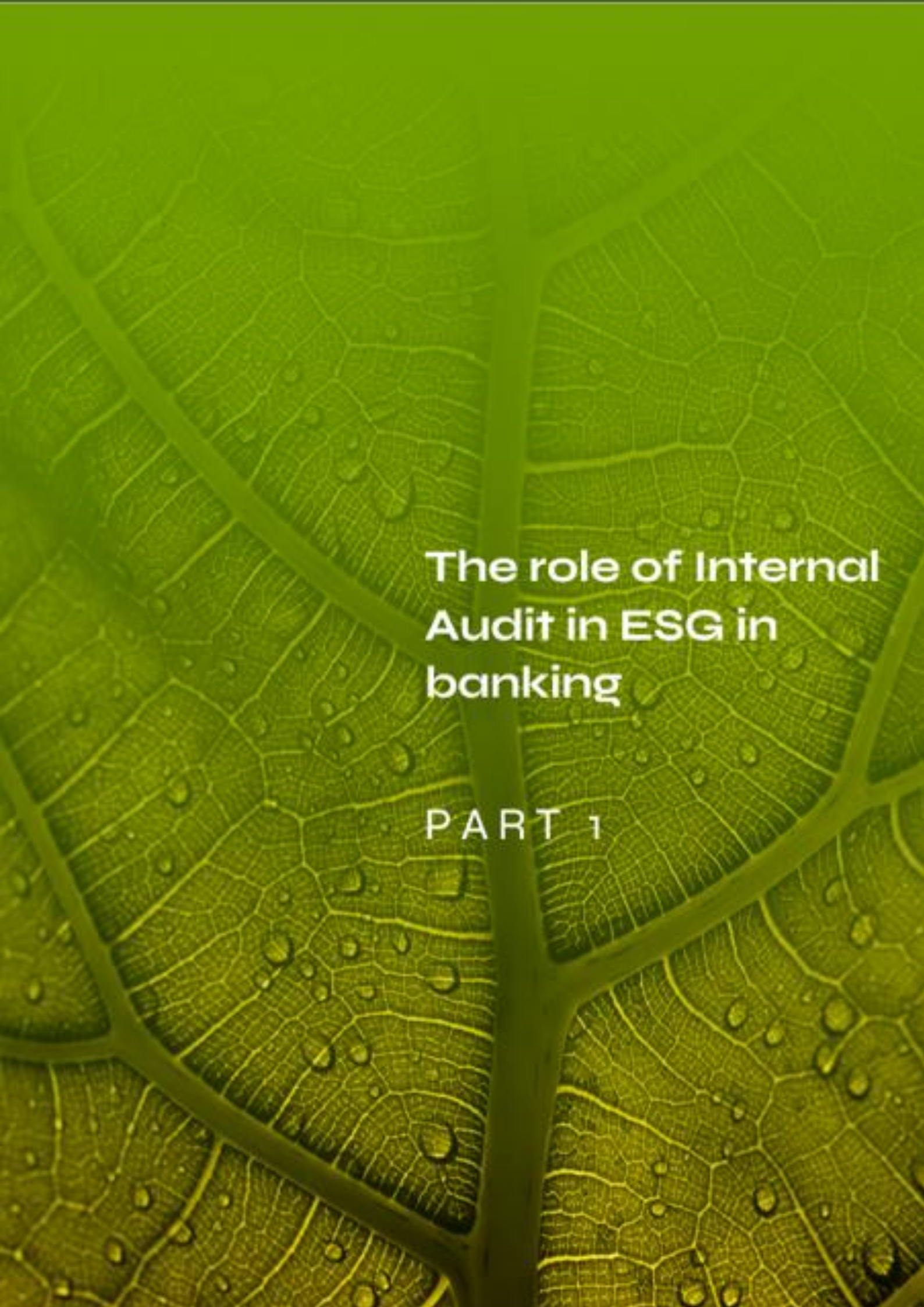
An assessment and credentials

JUNE 2023



European Confederation of Institutes of Internal Auditing

Index



The role of Internal Audit in ESG in banking

PART 1

Introduction

“Climate change is one of the biggest challenges facing the world today. Banks can and must play a critical role in aligning economic growth with positive social and environmental impact, ensuring a just transition towards the low-carbon economy of the future. Internal Audit is in the position to add real value to this learning process.”

The European Regulators have issued new regulations and guidance on ESG. Key examples of this include the Sustainable Finance Taxonomy, the CSRD, accompanied by the draft European Sustainability Reporting Standards (ESRS), the ECB “Guide on Climate-related and Environmental Risks”, as well an overview of good practices for climate-related and environmental risk management, the Corporate Sustainability Due Diligence Directive (CSDDD, draft). The Security Exchange Commission (SEC) recently also announced it plans to integrate climate change risks into mainstream financial reporting requirements.

Internal Audit is well positioned to help businesses navigate this fast-changing world of ESG regulations and stakeholder expectations.

In a field that is in constant motion and where national and international standards are still in flux, both assurance and advisory services can add real value. In this respect, development of Internal Audit skills and capabilities is a critical lever for the Entity to respond adequately to these big changes. A sound education in ESG themes and identifying common audit approaches on the matter, also through a specific “ESG Audit Certification”, will significantly support the ESG goals and objectives.

Internal Audit and ESG in general

Although many ESG areas of the organization might not yet be mature enough for assurance audits, there is a high demand and regulatory expectations for this. The risk of not acting from an Internal Audit perspective is that the control environment to support the ESG strategy of the banks may not be designed or operating effectively. **In this interim phase, where ESG management is still maturing, Internal Audit can perform audits to evaluate the organization's ESG maturity.** In certain cases Internal Audit can also help an organization progress through advisory services.

Assurance services

In these early days Internal Audit can assess the ESG path to maturity defined by banks, and the related actions taken towards achieving that plan. In doing so, Internal Audit can:

- Raise awareness at Board and senior management level about ESG priorities, gaps and implications (including greenwashing risk) and serve as a sounding board as management designs their program;
- Review how ESG risk factors (including transition and physical climate risks) have been identified and assessed in all business lines and verify & encourage the development of control activities to mitigate ESG risks;
- Verify & encourage the development of designed & documented standard processes; and
- Benchmark controls against best practices, regulatory expectations to validate their maturity.

Other key areas for ESG assurance services are:

Reviewing the ESG Governance Structure and Oversight

Internal Audit can assess the governance structure and ESG oversight by reviewing:

- If risk management procedures are clearly defined and management understands how ESG impacts its respective business operations;
- If roles and responsibilities are clearly established across the 3 lines of defense and understood throughout the organization, to ensure a sound ESG control environment and to monitor ESG issues, including the formation of an ESG committee consisting of cross-functional executive members; and
- Policy and procedure manuals to help communicate the company's ESG strategy, goals and specific processes and activities throughout the organization to mitigate ESG risks.

Evaluating the ESG Risk Management Framework and the Adequacy of Impact Assessments and Stress Tests

Internal Audit should review the organization's existing frameworks and standards, ranking, measurement protocols, and reporting to ensure they are reasonable, being followed, consistent with industry-recommended frameworks and regulatory expectations, and are comparable with similar entities. For instance, in the case of banks,

Internal Audit can confirm if the organization is adhering to the updated risk appetite and ESG guidelines to prevent financing clients and sectors that are high-profile polluters or are exposed to high climate risk. In addition, Internal Audit should assess how ESG risks are embedded in the overall credit risk management framework.

Furthermore, Internal Audit can evaluate the design and operating effectiveness of management's performance of periodic impact assessments and organization-wide stress tests to ensure ESG risk scenarios are plausible, and capital and liquidity implications are monitored and remediated. Also, regulators are increasing their requirements over stress test exercises as exemplified by the recent climate risk stress testing exercise required for banks by the European Central Bank (ECB). Internal Audit can monitor the organization's progress in the exercise and highlight any potential major areas of attention.

Validating ESG Goals

ESG goals can be validated through measurement of the gap between expected and actual performance and, based on that, by assessing whether goals are realistic and measurable. Goals should also be included in the company's strategic objectives and be a regular item on Board meeting agendas. Internal Audit can also complement this assessment through benchmarking: this can help the organization identify where it stands compared to peers and identify the amount of improvement possible.

Where the entity has adhered voluntarily to initiatives like for example NetZero Banking Alliance, Internal Audit can ensure that there is a regular follow up on the objectives and controls on the measurement of performance against these objectives, specifically when they are publicly disclosed.

Reviewing ESG Reporting

One of the most critical areas for Internal Audit to play a role is in validating the relevancy, accuracy, completeness and timeliness of management's ESG financial (when not covered by external audits) and non-financial reporting metrics in public disclosures. To avoid unsubstantiated claims that could be considered greenwashing and adversely impact the organization's reputation. Internal Audit can review the materiality assessment data gathering process used for building the metrics. It can also challenge the use of specific metrics over others that might be more relevant for external investors and other stakeholders and reflect companies' strategic objectives to ensure the reporting is focused on what is material. Examples of material/relevant topics for banks could be the bank's exposure to fossil fuel and other high emitting sectors, its progress in reducing the bank's footprint through its operations, supply chain and financing portfolio, and the impact of the offered sustainable investments.

Assurance reviews could also be performed to prevent reputational risk on financial products or services labelled as "Green" or "Sustainable", to ensure they effectively comply with taxonomy and other legislative requirements and the information provided to customers reflects adequately the sustainability of the product.

Audit on ESG Risk Models

Recently, Environmental, Social, and Governance score modelling gained significant attention as a framework for evaluating the sustainability impact of companies. The banking industry is facing increased regulatory scrutiny in this context, and the Internal Audit plays an essential role in ensuring the accuracy and reliability of ESG score models.

Defining and quantifying a score, able to reflect the ESG impact of a company, leads to several methodological challenges for any European Bank, from collecting and analysing a broad and new type of data/information to developing and reviewing of the underlying processes.

In this context, an Audit Model Risk assessment can help in enhancing the transparency and credibility of ESG scores, across the Bank and to the Supervisor, by providing an independent assurance on the methodological approach used in the calculation.

Among others, the accuracy, completeness, and consistency of data and information collected should be verified. This includes checking the integrity of data sources, evaluating the methodologies and expert-based assumptions, and assessing the appropriateness of disclosures.

Furthermore, Internal Audit should evaluate the effectiveness of the internal controls in collecting, processing, and reporting ESG-related data accurately considering the three lines of defense, and the model's life cycle as well. According to this, IA should assess whether the banks' internal controls are designed effectively to identify, mitigate, and report ESG-related risks and opportunities.

In summary, Internal Audit has a relevant role in relation to the review of the new ESG scores and related Bank processes that should always be aligned with the bank's strategies and with the evolution of the regulatory framework. It provides assurance on the accuracy and reliability of ESG data, assesses the effectiveness of internal controls, enhances the transparency and credibility of ESG scores, and helps banks identify areas for improvement.

Advisory services

On the advisory side, Internal Audit can support the organization in implementing ESG requirements. Regulators in many jurisdictions have increased their focus on ESG risks with initiatives related to climate change, executive pay, diversity and inclusion, working conditions, human trafficking, and product content, among others. These jurisdictions have mandated or encouraged greater disclosure of sustainability practices and risks, and several major stock exchanges are instituting similar requirements. For this reason, such topics cannot be ignored by Internal Audit, as the stakes are simply too high, with pressure exerted by regulators, investors, customers, third-party affiliates, and society at large.

Implementing the requirements in practice is difficult due to lack of expertise in specific ESG topics and of standardized approaches within the industry. Internal Audit could help organizations move in the right direction by:

- Collaborating with Legal and Compliance to validate ESG reporting disclosures comply with applicable regulations. For example, Internal Audit can create an inventory of ESG disclosure requirements to identify what disclosures are required, by which agencies / regulators / governments; Advising on developing specific internal controls in relation to the identified requirements; advising on ESG governance due to IA's holistic understanding of risk across the organization; and more generally
- Challenging the current way things are done from a risk and control perspective
- Performing business monitoring, facilitating knowledge sharing with different internal stakeholders.

Internal vs External Audit on ESG

While the internal and external audit functions could complement each other, their purposes and areas of focus differ. The Institute of Internal Auditors (IIA) emphasizes that the two functions do not compete or conflict; rather, they both contribute to effective governance. In general, Internal auditors take a holistic view of their organization's governance, risk, and control systems (in other words, primarily non-financial information), while external auditors are either concerned with the accuracy of business accounts and the organization's financial condition and its regulatory compliance.

With regard to ESG, Internal Audit can provide the independent internal assurance needed for trustworthy ESG disclosures and help to ensure the existence and effectiveness of internal controls on ESG risks and their continuous monitoring processes across the organization. External auditors provide third-party assurance services by endorsing the integrity of non-financial (ESG-related) public disclosures and ensuring they align with financial information in external reporting to investors and stakeholders. External auditors can also help to perform a benchmark to compare the entity with competitors and ESG best practices in the financial sector.

While the purpose, focus, and outcomes of their fieldwork may vary, internal and external auditors often share information to avoid duplication and improve audit coverage. In fact, Internal Audit can leverage the external auditor's comments / findings on areas included in their review and vice versa.

Challenges faced by Internal Audit

According to the 2021 ECB comparative study on the state of climate and environmental (C&E) risk management in the banking sector[1], institutions are increasingly integrating C&E risks into their three lines model. However, "the integration of C&E risks into the third line remains rare, as only about 15% of institutions have explicitly considered these risks in their internal audits or reviews. In some cases, Internal Audit functions have performed a dedicated audit of the compliance of institutions' practices with their internal policies and with regulations applicable to C&E risks."

The low level of Internal Audit engagements on C&E risks, and more in general on ESG, might indicate that Internal Audit functions face challenges in the way they approach ESG. This may be due to Internal Auditors' lack of awareness or understanding of ESG risks and the operational and financial implications to the organization.

Another challenge for Internal Audit is to identify responsible parties within the organization. ESG has become such a pervasive topic that every function within the organization will cover ESG-related topics to a certain extent. Often, Investor Relations, Finance, Strategy, Legal, Compliance, Risk Management and front-office functions will be involved in ESG. However, who ensures the effective coordination among these groups? And, most importantly, who ensures effective governance around ESG within the organization? Effective coordination among these groups and a focal point of responsibility is critical to progress. These challenges become even more evident for multinational banks, where a sound coordination is expected between Head Office and subsidiaries or foreign branches. Also, the different regulatory expectations and requirements in different countries, create additional complexity in the management of ESG risks and, as a consequence for Internal Audit. Translating the organizational set-up of the bank in terms of ESG into the audit universe and ensuring a complete audit coverage for the global organization is one of the key challenges for internal auditors.

Furthermore, as Kaplan and Ramanna (2021)[2] comprehensively discuss, ESG's subcomponents are not homogenous. They in fact rely on different indicators, language, and measurement. For instance, environmental issues can be measured in inputs and outputs, while governance issues often rely on compliance- or process-measures, that require a considerable level of judgment and contextualization to be interpretable. Neither inputs nor outputs are easily determined.

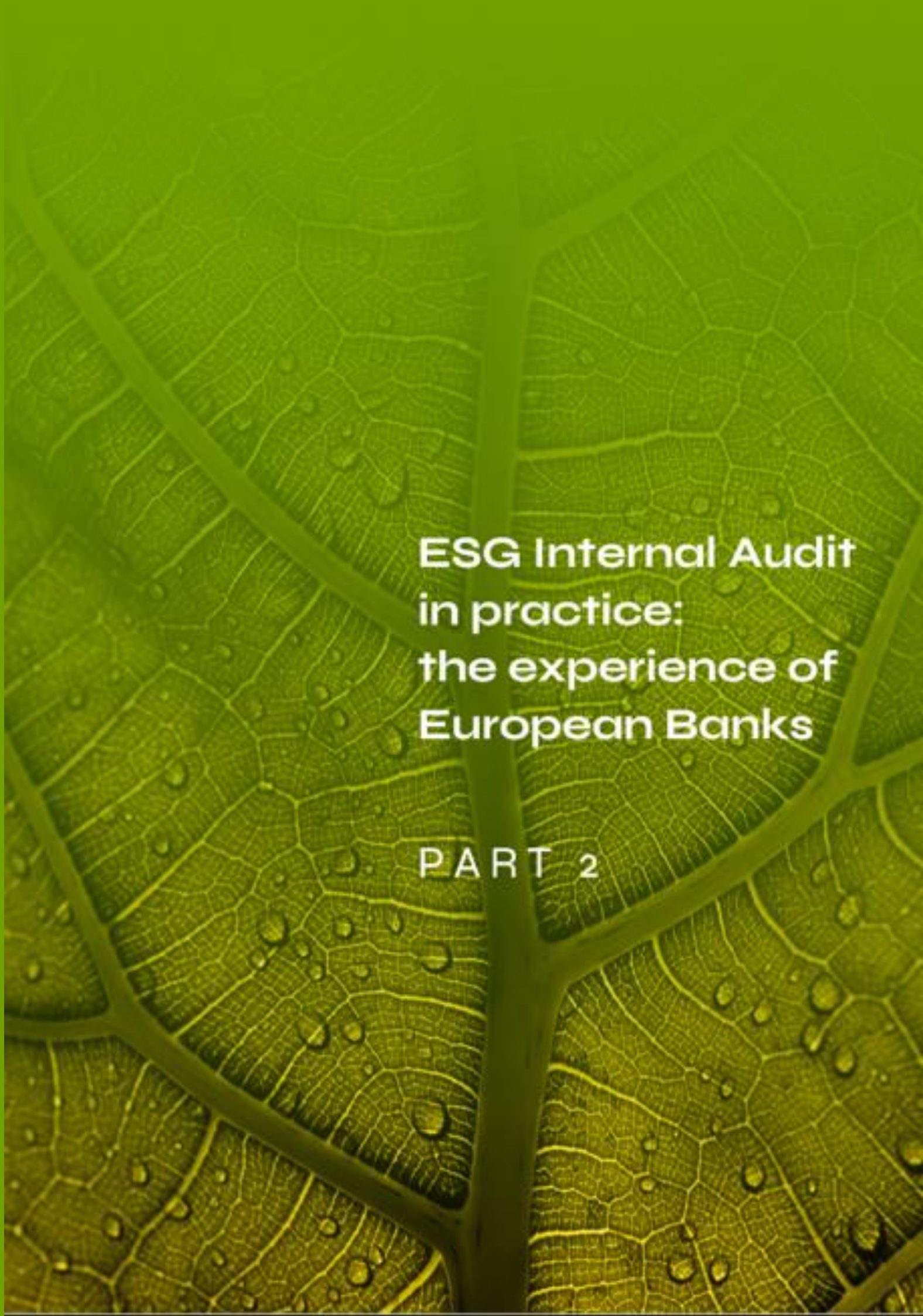
And last but not least, social issues are more hybrid and probably pose even greater challenges for their measurement, than environmental and climate-related issues. The consequence of this is that not all issues can and should be audited through the same process in the same audit engagement. Also, this suggests that different expertise is needed to review and judge the correct and fair representation of the underlying information.

[1] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202111guideonclimate-relatedandenvironmental-risks~4b25454055.en.pdf

[2] Kaplan, RS and Ramanna, K (2021) How to Fix ESG Reporting, Forthcoming Harvard Business Review.

Another challenge that Internal Audit functions are facing is the low level of maturity of ESG regulations and business practices, which may delay business decisions on strategic and compliance risks. At the same time, in the European Union we are witnessing an enormous increase of new regulations aiming to address ESG and greenwashing risks. This forces organizations to develop new processes, set of controls and policies, and above all, obtain the right data to fulfill the regulatory requirements (e.g. CSRD). The availability and accuracy of ESG perhaps poses even greater challenges: does the organization have the right ESG data; is that accurate, relevant and sufficient to provide information that correctly depicts the organization's ESG efforts, without incurring into greenwashing? These are all questions that Internal Audit functions can and should address in their assurance reviews over, for instance, ESG reporting.

It is clear there is a need for Internal Auditors to be trained on ESG risk solutions. By developing knowledge IA can add value and partner with management to identify and establish effective ESG controls, develop audit work programs and verify that reported ESG program outcomes are supported by evidence of performance. **Addressing ESG risks can no longer be postponed due to other priorities: Internal Audit has a clear responsibility to highlight both emerging risks and exposures that are not being mitigated or properly addressed by the company, including ESG risks.**



ESG Internal Audit in practice: the experience of European Banks

PART 2

The Internal Audit journey on ESG

There are many opportunities - and a few important challenges - for Internal Audit to play a valuable role in ESG management. Likewise, there are various ways of approaching the topic from an audit perspective.

In the following paragraphs the steps are lined out that have been taken within Internal Audit of European Banks to date. The experiences can be a helpful starting point for others.

Allocation of responsibilities

In 2020, the Bank Internal Audit function started the journey to develop an audit approach to include the ESG risks in the audit oversight. The primary focus was on mapping and assessing the impact of ESG regulatory developments and requirements, however the complexity and width of the ESG topic warrants a more holistic approach. This resulted in the decision to create a specific dedicated audit team with central ownership on ESG risk that started in 2021.

Considering that climate change and environmental issues are likely to increase in importance over the next years, the audit team was built with people that collectively possess the skills and knowledge required for their involvement in these areas. This expertise has been achieved by completing specific trainings and internationally recognized certifications on the topic, but also, by onboarding in the audit team experienced people that worked before in Sustainability related functions within the Bank.

This allocation of clear responsibilities within the third line enables the team to develop a standard audit approach globally, to cultivate specialist knowledge and skill set to perform audits on these risks and challenge the business, and to be on top of the evolving regulatory landscape. Additionally, from a client perspective, having dedicated staff for sustainability topics facilitates the development of stakeholder relationships and alignment with business.

Audit universe split

Internal Audit is in the process of aligning the audit priorities, the audit universe and audit plan, with the Bank's strategic Sustainability priorities. The materiality analysis that is disclosed in the Annual Report provided relevant insights on the material matters. As starting point, Internal Audit split the audit universe between two main areas: Responsible Business and ESG Risk. Responsible Business comprises the offer of sustainable products for Retail and Wholesale banking clients. ESG Risk includes the risk-related activities, like climate risk management, specific environmental and social risk frameworks, ESG reporting activities and compliance with specific Sustainability regulatory requirements. The definition and breakdown of the audit universe was done bearing in mind that it would be evolving over time, as sustainability-related activities and requirements will also evolve in the organization.

Definition of audit universe and coverage of ESG risks

When defining the audit approach coverage, one of the main challenges faced was to set up the audit work at the correct level (group level or local level). There are regulatory developments, like the ECB Guide on Climate and Environmental risks, that are impacting entities at consolidated level; also, the ESG information is disclosed in the annual report at Group level. However, there are other regulations, like Sustainable Finance Disclosures Regulation (SFDR), or specific frameworks for performing the environmental and social due diligence on clients, that have an impact on the different entities across the Bank. To ensure that key ESG risks are sufficiently addressed in the audit work Internal Audit decided on a combination of both global and local coverage. Local coverage for specific implementations on the different business units, also depends on the maturity level. And global coverage for group-wide topics such as Sustainability Reporting or Climate Stress Testing.

Global versus local

Although most of the regulatory initiatives were launched at European level, Internal Audit is aware that there could be additional local regulatory developments in the different jurisdictions where the bank operates. In order to ensure that these local regulatory specificities related to Sustainability are followed-up and integrated in the corresponding audit entity, in the next year Internal Audit envisions to set up a virtual sustainability network made of auditors located across the main subsidiaries and the central team to build together this overview. This network will help the audit function to maintain a tracker of local ESG regulations and establish the potential impact of the local regulatory requirements on audit work. At the same time, knowledge will flow from Group Audit to local audit teams.

Combining assurance and advisory

The Bank's Internal Audit function mainly focuses on providing assurance. Nevertheless, they recognize the different levels of maturity of the ESG elements in the organization and would like to adapt their role to this reality. Besides the standard assurance work done on the existing (ESG) processes already running in the bank, Internal Audit uses specific limited assurance, or non-assurance reviews where useful and practical (mainly based on the level of maturity of processes reviewed).

Another key part of Internal Audit's advisory role relates to business monitoring activities. These are carried out through a combination of regular meetings with main stakeholders and the attendance to the relevant committees and forums in the bank. Business monitoring plays a relevant role in the ability to support the implementation of the bank's Sustainability Strategy. For this purpose, Internal Audit developed a stakeholder relationship matrix, assigning specific auditors to key areas/stakeholders, and using knowledge gained via the interaction with other Internal Audit teams, via for example the Sustainably Internal Audit Forum, which comprises more than 30

internal audit functions from different banks, established by Corporate Audit Team at the beginning of 2021. The forum has become a reference of knowledge in the industry, for example, allowed a voluntary group of 9 leading banking institutions to develop for the first time, a Climate Risk Audit program based on the ECB Guide on Climate and Environmental Risk, and the Supervisory Statement (SS3/19) on Enhancing Banks' and Insurers' Approaches to Managing the Financial Risks from Climate Change, issued by the PRA in 2019. These forums will continue in 2023 and beyond and invite any interested financial institution to join.

Creating awareness of ESG within Internal Audit

Considering the transversal nature of the ESG risks across the entities, it is relevant that all auditors get an understanding of the basic elements of Sustainability and related risks. For that purpose, apart from the planned virtual sustainability network with auditors located in main subsidiaries, the bank ESG audit team provides awareness of trainings for the rest of auditors in the bank.
Spreading knowledge on this topic can help all internal audit teams to identify and embed ESG risks in their audits adequately. With this purpose, a series of internal webinars are planned every year, open to all internal auditors across the bank, where the ESG audit team provides insight on different topics, shares the latest developments from within the organization, main regulatory requirements and the results of last audits done on the topic. Furthermore, all people joining Internal Audit in the bank get a dedicated Sustainability risks training session, as part of the standard new joiners on-boarding training.

Finally, as a key additional step to create awareness on ESG across all internal audit teams in the bank, specific training sessions for senior management of the Corporate Audit Team were organized. Those sessions were mainly delivered by senior sustainability experts within the bank, together with external consultants, to provide all Audit Heads the foundations of Sustainability concepts, understanding of the bank sustainability strategy, priorities, risks and ongoing developments.

Work Program

Noting the lack of a standard or benchmark yet on how to perform ESG audits, the German Institute of Internal Audit has developed a practice guide. It is based on regulatory risk management requirements for the banking sector and approaches the ESG topic from different directions. It may serve as audit catalogue or checklist consisting of various modules. On this basis the individual internal audit function may create an audit program tailored to the specific level of maturity of the topic within the organization, the purpose of the audit (e.g. governance audit, product-specific audit) and for instance the specific audit approach. [3]

[3] See DIIR website : DIIR_ESG-Leitfaden_Banken.pdf

Conclusion

The relevance of ESG risks for companies requires the involvement of the Internal Audit function to support the bank's response to these material challenges. The ESG territory is still developing and there are many (regulatory) uncertainties and challenges, but this cannot be used as an excuse/limitation for Internal audit functions not to get involved and support organizations on their pathway towards a sustainable future.

About ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin.

The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence. The primary objective is to further the development of corporate governance and internal audit through knowledge sharing, key relationships and regulatory environment oversight.

About the ECIIA Banking Committee

ECIIA set up a Banking Committee, in 2013 with Chief Audit Executives of the largest European Banks, supervised by the ECB. The mission of the ECIIA Banking Committee is: "To be the consolidated voice for the profession of Internal Audit in the Banking sector in Europe by dealing with the Regulators and any other appropriate institutions of influence at European level and to represent and develop the Internal Audit profession as part of good corporate governance across the Banking Sector in Europe ». ECIIA represents around 55.000 internal auditors and around 15.000 are active in the banking sector.

Thank you

This paper describes the results of discussions amongst the ECIIA Banking Committee members. We would like to thank the Committee members for their input.

We would also like to thank the redaction team: Jessica de Boer, Elena Durante and Sara Gonzalez, ESG Risk Audit at ING and Patrizia Biermann and Daniel Krömer, ESG Risk Audit at Commerzbank for their support.

European Confederation of
Institutes of
Internal Auditing

Avenue des Arts 41
1040, Brussels—Belgium
TR: 84917001473652

LINKEDIN WEBSITE EMAIL