European Confederation of
Institutes of
Internal Auditing

POSITION PAPER

The role of Internal Audit in ESG

in industrial and commercial companies

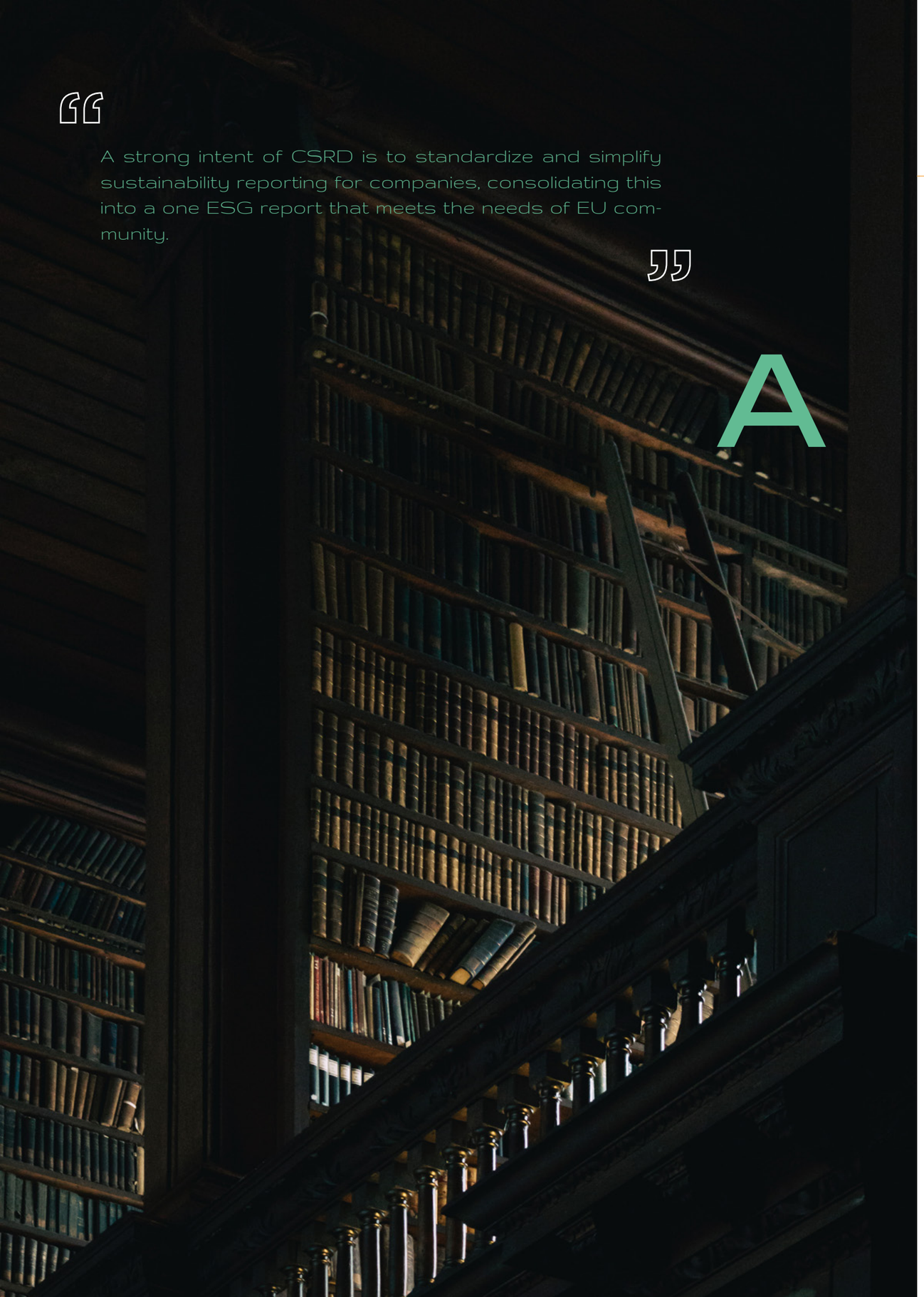
OCTOBER 2023

INTRODUCTION

Our world faces several global challenges such as climate change, transitioning from a linear economy to a circular one, increasing inequality, and balancing economic needs with societal needs. Many stakeholders including investors, regulators, consumers and employees are now increasingly demanding that companies should not only be good stewards of (financial) capital but also of natural and social capital and have the necessary governance framework in place to support this. Furthermore, investors are incorporating ESG elements into their investment decision making process, making ESG increasingly important.

The purpose of this document is to create awareness of the role that Internal Audit could play in this journey, with specific focus on Industrial and Commercial companies. Regardless of the level of maturity of each company on ESG, the added value of Internal Audit ranges from a more advisory role such as, assisting in setting up corporate culture and behavior changes towards a sustainability embedded decision-making process and strategy in less mature environments, to a pure independent assurance role where the ESG agenda is already well embedded in organizations.

With the new upcoming Regulations deeply impacting the way the organizations operate, there is an important call now for Boards and Top Management to recognize that Internal Audit, while remaining independent, could help them in this important journey.



> A strong intent of CSRD is to standardize and simplify sustainability reporting for companies, consolidating this into a one ESG report that meets the needs of EU community.

SECTION A

VARIOUS REGULATIONS AND THE DIFFERENT MATURITY IN ESG

The spotlight on ESG commitments and reporting continues to expand, as stakeholders increasingly demand organizations to drive a sustainable business, providing evidence of ESG progresses achieved. ESG reporting is quickly moving from a voluntary to a mandatory activity, with Regulators accelerating the interest on corporate responsibility, as part of the Journey for the European Green Deal.

The European Commission recently revised the **Corporate Sustainability Reporting Directive (CSRD)** to modernize and strengthen the rules with the objective of accelerating the transition towards a more sustainable economy. The new CSRD, that will take effect from FY 2024, enlarges the scope to be covered, expecting to quadruple the number of covered organizations.

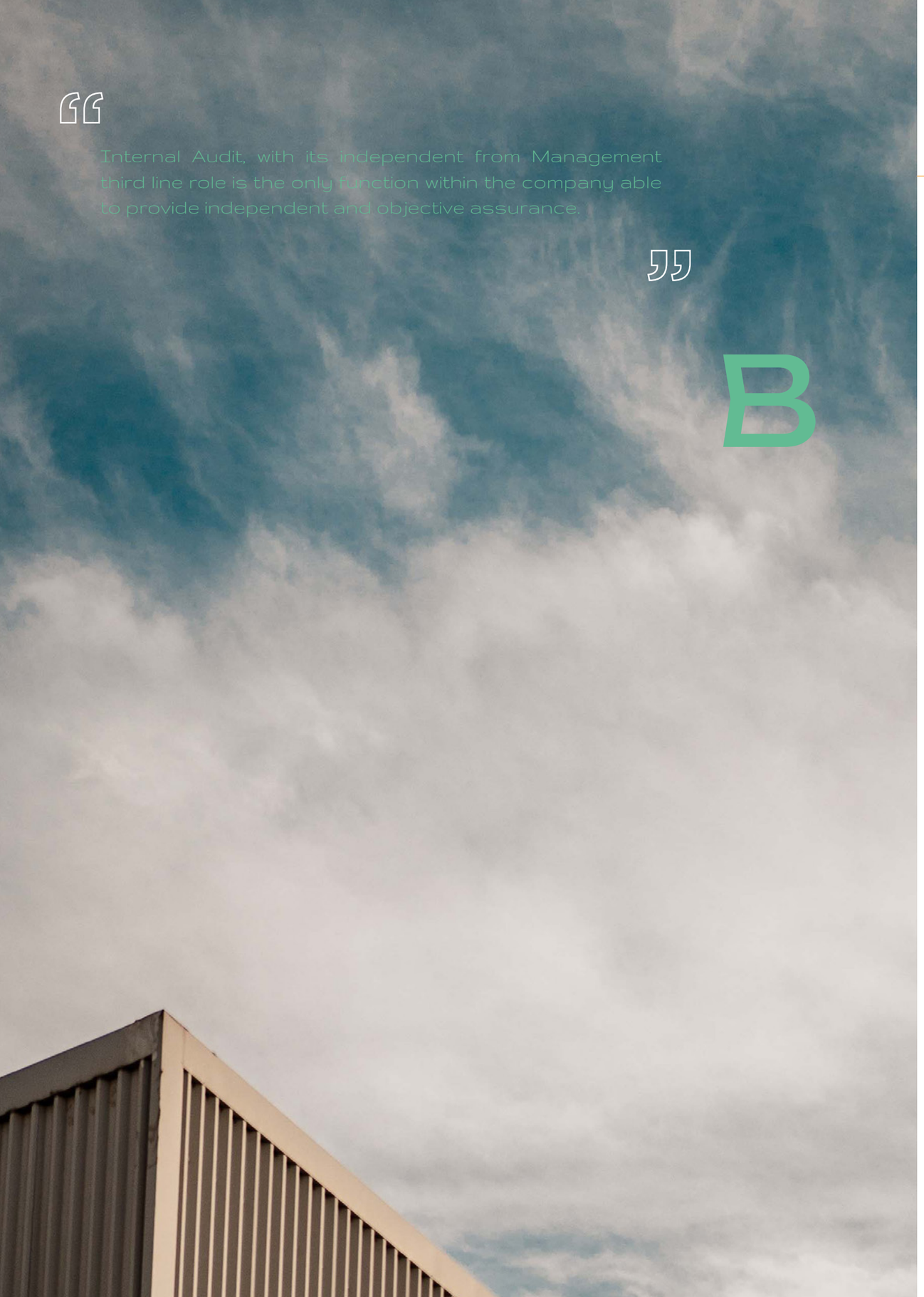
A strong intent of CSRD is to standardize and simplify sustainability reporting for companies, consolidating this into a one ESG report that meets the needs of EU community (Consumers, Regulators, investors, and other stakeholders). The CSRD standards **(European Sustainability Reporting Standards — ESRS**, with a first set issued in July 2023) are designed to make corporate sustainability and ESG reporting within the EU more accurate, common, consistent, comparable, and standardized, just like financial reporting. The ESRS has been developed taking into account the existing EU law and initiatives (e.g. double-materiality principle, Climate Law and Taxonomy Regulation). The assurance by an independent provider becomes compulsory with CSDR: limited assurance applicable from FY 2024 and the goal is to extend to reasonable assurance in the medium term, with a horizon of 3 years.

As part of a set of measures under definition by the EU to support the ESG evolution, the EU proposal for the **Corporate Sustainability Due Diligence Directive (CSDDD)** is of particular importance for industrial companies. It is designed to foster sustainable and responsible corporate behavior throughout global value chains (with focus on human rights and environmental impacts in supply chains). It should be noted that Certain EU countries — such as Germany and the Netherlands — have already moved ahead with country-specific laws.

The European regulatory landscape is complex with several initiatives that will impact organizations particularly the E & the S (e.g., green claims directive, forced labor ban, work life, and Diversity and Inclusion Directive). Multinational companies will also have to deal with the difficulties arising from the geographical operations, given that each country will bring local emphasis or accents when transposing these EU regulations into the respective national laws.

In this articulated environment, we observe various levels of ESG maturity amongst different organizations[1]; it is time for everyone to start embedding ESG in the organizations and engage the assistance of internal audit in this evolving process, adding value

1 (see paper ECIIA/ecoDa / Ferma on the topic “ESG embedding:are you ready?”)



SECTION B

THE INTERNAL AUDIT AND THE OTHER FUNCTIONS INVOLVED IN THE ASSURANCE PROCESS IN INDUSTRIAL AND COMMERCIAL COMPANIES

Internal Audit represents a key counterpart for Governing Bodies and Management providing objective assurance and insight on the effectiveness and efficiency of risk management, internal control, and governance processes. Internal Audit is best positioned to provide assurance when its resource level, competence, and structure are **aligned with organizational strategies** and when it has the in-depth understanding of business systems and processes.

Independence does not mean isolation! Each Internal Audit needs to cooperate with other relevant players accountable for governance, risk management and internal controls. **The Three Lines Model**, published by The Institute of Internal Auditors, clarifies each player's role and the interactions.

Internal Audit, with its independence from Management has a third line role and is the only function within the company able to provide independent and objective assurance. However, it should be considered that besides Internal Audit, industrial & commercial companies generally have other distinct functions that provide a certain level of assurance (as second line), that is relevant also for ESG purpose.

In particular, Internal Audit — while maintaining its independence – due to its privileged transversal perspective, plays a **key role in guaranteeing collaboration, cooperation and communication** between the different assurance providers (internally and externally) to collectively contribute, in a more efficient and effective way, to the creation and protection of value for ESG progress.

The key purpose of this chapter is to create awareness about the assurance providers as they provide a level of assurance that needs to be taken into consideration by Internal Audit in its role of supporting the Governing Body and Management with objective assurance, insights, and advice on ESG matters.

Below is a list of the most common assurance providing functions in industrial and commercial companies, whose presence and role varies according to the maturity of the organization:

- **Compliance function —** with the calls for more transparency and openness in companies growing increasingly louder, the role of Compliance functions is becoming more and more relevant as they provide support to the organizations in enhancing structures and processes aimed at guaranteeing corporate and regulatory compliance. The topics that follow under the umbrella of Compliance can vary based on the industry and country, from data privacy (e.g. GDPR, including customer consent, relevant for the commercial processes), anti-trust and competition, crime prevention and anti-corruption, trade sanctions to environmental, labor and Code of Conduct.

- **Health, Safety & Environmental function (HSE) —** all manufacturing companies generally have an HSE function that provides governance rules and guidelines to identify, assess, prevent, and mitigate potential hazards in the workplace or environment and ensure compliance with local regulations. A well-developed and mature HSE management represents a fundamental support in the ESG journey.

- **Human Resources (HR)** ensures that the company complies with social and labor laws and regulations – both in a production and non-production environment — but also plays a key role in ESG assurance (e.g. promoting Equality, Diversity and Inclusion in the Workplace).

- **IT risk, information security and cybersecurity** department support companies in protecting data and information systems from inappropriate access, manipulation, modification and destruction. Although cybersecurity has long been viewed as an IT issue, the effects of breaches, nefarious use and social engineering extend well beyond the purview of IT, and it is now regarded as a key ESG concern, falling under the "Social" pillar. Although cybersecurity as an ESG metric is still a relatively new stance, all evidence points to increasing and continued interest across the Board. Imperative here, is that risk should be evaluated in conjunction with the sharp evolution of the Artificial Intelligence research and development across the organization.

- **Product Quality and Product Development functions** are responsible for standards, rules and operational processes to ensure that products are developed in a sustainable and ethical manner. For manufacturing companies in particular, this includes guaranteeing that products are safe, meet regulatory requirements, and are produced in a socially and environmentally responsible manner.

- **Supply Chain Compliance** plays a critical role in ensuring (through the Third Party management Process, that includes supplier due diligence in terms of economics/finance ratios, corporate and social responsibility, information security, etc.) that the company's suppliers comply with ethical and CSR standards, and with local regulations, providing a certain level of assurance which is relevant for the ESG reporting domain. For companies with international supply chains and commercial networks, they also have to ensure compliance with relevant import / export regulations and therefore perform control & audit activities on processes and/or suppliers / customers (e.g. sanctions to black listed countries). Many industrial and commercial companies also have certifications (e.g. ISO certifications that cover a range of topics, including quality, information security management systems, environment and health and safety) that represent a tool to support the pillars of sustainable development.

- **Sustainability** is becoming more and more common in the organizations as it provides a certain level of assurance with a crucial role in the to ESG data gathering and reporting process and internal control over Non-Financial Reporting. Nevertheless, Sustainability plays an important role in governing the ESG projects, in alignment with other functions within the organization, making sure that disclosed targets are met.

It should be noted that the list of functions that drive risk mitigation strategies across business units and processes is not exhaustive. In addition, we cannot forget the other functions that are generally present in all the companies, such as Finance, Tax & Legal, ERM, etc.

Considering the increase of demands and complexity of the business and regulatory environments, and several actors involved in the assurance process, it is key that assurance objectives and activities are linked to the company's goals with a holistic and integrated view in supporting the overall company strategy.

SECTION C

ROLE OF IA IN ESG

Potential roles for an Internal Audit in manufacturing companies in the ESG domain

The implementation of credible strategies that support a sustainable value creation is now a business imperative. This requires strong governance over ESG with alignment among all the principal players involved in the process, in particular, a Governing Body, Management (specifically, Sustainability, ERM and Compliance functions, if they exist) and Internal Audit.

Internal Audit, having a systematic and disciplined approach and a very good understanding of the organization, in terms of governance, risks and processes, could play a crucial role supporting companies with **objective assurance, insights, and advice on ESG matters, enhancing credibility and trust.**

Internal audit can begin offering **advisory services** when companies are just getting started in ESG, — e.g. those that were not subject to the EU's Non-Financial Reporting directive (NFRD) and are now just approaching ESG topics also in light of the new law requirements — supporting Management and the Board in the establishment of the ESG governance program. As companies become more mature in the ESG journey, Internal Audit should move to its typical role of **assurance provider**, providing an independent and objective review of the effectiveness of ESG risk assessment, data governance and management, reporting, and related regulatory compliance.

Advisory

Internal Audit can help the organization in defining the **building blocks of good ESG**, with a key role in supporting the corporate culture and behavior changes towards sustainability that is embedded in the decision-making process and strategy. This means for Internal Audit needs to assist organizations to focus on the right priorities, thereby setting impactful yet realistic targets and building culture and expertise, and provide advice on governance practices and internal controls, also raising awareness and sense of urgency to Management and the Board.

Internal audit can embrace the following roles that can add value to an organization's ESG journey, always without compromising its independence or objectivity:

- **Advise on ESG Governance & Strategy.** ESG covers many topics that traditionally are widely dispersed within the organization with no single point of contact, generating difficulties in data collection, reporting and disclosures. Internal audit can facilitate consensus on organizational priorities for ESG ensuring the alignment with the overall Company strategy, convening functions that should be involved in ESG matters, reporting, disclosures, and risk management. A strong ESG governance, with consensus-building conversation between the Board, Management and Internal Audit, is fundamental for the execution of the ESG strategy.

- **Support in the definition of an ESG control environment.** Internal Audit can use its structured approach and framework (e.g., COSO's Internal Control – Integrated Framework) offering its expertise to develop a strong control system to manage and mitigate ESG risks, with the same rigor as controls over financial reporting. Internal audit can also advise on defining specific controls that are sufficiently robust to support external reporting to capital markets. Considering the new requirements – for example, "double materiality" and upcoming Supply Chain obligations, particularly relevant for manufacturing companies – Internal Audit can support in the implementation of these new concepts.

- **Recommend reporting metrics.** Internal audit can provide insights into the kind of data (quantitative and qualitative) that accurately reflect sustainability efforts within the organization, taking into account the already existing process & KPIs. For manufacturing companies, the focus is on data collected to manage the environmental impact of the operations, ensuring safe working conditions for employees, and addressing supply chain risks (e.g data available for certifications).

- **Support in the "double materiality" definition**. While materiality assessment is already an established market practice for companies reporting under NFRD, the CSRD regulation gives to materiality a broader meaning, recognizing the importance of sustainability topics in driving long term financial performance. In particular, CSRD introduces the concept of 'double materiality" with Stakeholders that are now asked not only to identify most material topics to the organization but to evaluate company's most significant impact on people and the environment, after they have to identify sustainability risks and opportunities for the company. Internal Audit has already started to provide assurance on the materiality matrix required for companies under NFRD and now needs to broaden its scope by initially offering support in the definition of the double materiality approach, supporting stakeholders in this new challenge, leveraging its knowledge of the organization and then gradually moving towards more traditional assurance activities on the double materiality assessment methodology, incorporating a "double materiality" lens of both traditional financial data and non-financial ESG information.

Assurance

As ESG risks become more relevant in decision-making by the Governing Body and Executive Management, companies are moving quickly to disclosing ESG information. Organizations should have assurance on the effectiveness of ESG risk management, including ESG reporting. Internal audit is ideally placed to be a **major assurance provider** and the only independent one in the ESG domain, bringing a systematic, disciplined approach to evaluate and improve the effectiveness of ESG risk management, control, and governance processes.

Assurance over ESG will become increasingly important as this is one of the cornerstones of CSRD, aiming towards a more reliable and comparable Non-Financial Reporting.

While the external auditor will first conduct a review and express an opinion with *limited assurance*, CSRD will later on impose that an external audit expresses an opinion with *reasonable assurance*. In such context, the alignment between internal auditors and external auditors assumes relevance as they both play an important role not conflicting but complementing each other fostering the overall robustness of assurance provided to the Governing Body and Executive Management

Below are some examples of the relevant assurance activities that can be performed by Internal Audit in manufacturing companies:

- **Review ESG Governance & Strategy.** When the maturity level of the company on ESG increases, Internal Audit can evaluate the effectiveness of the company's governance and oversight of ESG. This can involve reviewing the roles and responsibilities of the Board and Management, and the inclusion of sustainability performance into the overall business strategy, that is fundamental for manufacturing companies considering the unique ESG-risks they are facing.

- **Review how changing ESG Regulations and Reporting Standards are tracked.** Internal Audit can assess the organization's process of tracking upcoming ESG regulations, ensuring new requirements are followed and implemented by all the areas of the organization.

- **Review ESG projects vs communicated targets.** Internal Audit can play an important role in providing assurance over ESG priorities and related targets disclosed in Non-Financial Reporting. Organizations most probably need to establish new processes, new projects, new teams, new investment to reach such targets. The Governing Body and Executive Management need to be safeguarded that ESG ambitions can be achieved and consequently informed in a timely manner in case of delays or issues. It is therefore important to assess the consistency between strategic ESG goals and the decision-making process across the different operational activities of the company (for example, investment and divestment, maintenance, purchasing and contracting, human resources decisions, etc). Defining a combined assurance map for the ESG strategic goals, metrics and reporting processes, together with the other assurance functions (such as Sustainability), supports the achievement of this objective.

- **Review ESG Data Governance, Collection and Reporting.** Evaluate the governance of management's selection and tracking of ESG metrics, taking into account the existing process & KPIs in the organizations. Considering the different functions involved, as also represented in the paragraph B, it is important to review how information is collected and aggregated to ensure figures represented are accurate, relevant, complete, and timely. For example, in the greenhouse gas emission, Internal Audit can assess how data, coming from different sources within the organization and supply chain, is collected, consolidated, and reported; thereby evaluating the achievement of the defined targets.

Internal Audit has already started to provide assurance over the materiality matrix required for companies under NFRD and now needs to broaden its scope by initially offering support in the definition of the double materiality approach and then focusing its assurance activities on the double materiality assessment methodology, incorporating a "double materiality" lens of both traditional financial data and non-financial ESG information.

- **Review ESG Risk Management.** Assess how sustainability risks as results of the "double materiality assessment" are integrated into the existing Risk Management Framework and the effectiveness of the internal controls.

- **Review ESG Disclosures & Reporting.** Internal Audit can review the organization's ESG disclosures & reporting to ensure they are complete, accurate, and in compliance with relevant reporting frameworks or regulations. This may involve also reviewing reporting for consistency with formal financial disclosure.

- **Assess ESG Culture.** Considering the increasing requirements for companies to account for how they promote a healthy culture around environmental, social and employee-related aspects, Internal Audit can be of value assessing the effectiveness of the initiatives and how culture and values are integrated into the business processes and decision-making processes.

SECTION D

CONCLUSION

With the increasing importance of sustainability deeply impacting the way the organizations operate, there is a clear call for Board Members and Top Management to move towards a more sustainable business with Internal Audit as valuable partner in this journey; leveraging on the experience, the business knowledge and the role Internal Audit plays in Governance, Risk Management and Internal Controls. The support of Internal Audit can vary depending on the maturity of the organization (see graphic below) with opportunities also for less mature companies to invest and properly set up this value-added function. To conclude, the question “if” Internal Audit could play a fundamental role over ESG” is no longer a question Boards and Top Management should ask but rather it is more of “how” they can best benefit on this privileged view.

ADVICE/INSIGHT

- Give input on ESG management control cycle
- Give input on ESG embedding progress
- Give input on ESG reporting process including double materiality assessment
- Give input on ESG governance
- Give input on ESG culture
- GIve input on ESG strategy

ASSURANCE

- Audit effectiveness ESG governance
- Audit effectiveness risk management
- Audit design and effectiveness ESG processes including double materiality assessment
- Audit ESG management control cycle
- Review strategic changes
- Assess ESG data collection
- Coordinate Assurance with 2nd line
- Provide int. assurance on ESG reporting process

NOT FOR INTERNAL AUDIT

- Define ESG risks & opportunities
- Define ESG strategy & business transformation
- Manage ESG risk & opportunities
- Play the role of external assurance provider
- Adapt internal controls & define KPIs
- Change culture
- Accountability on ESG goals & achievements

> “(...) the independence of the Internal audit role is fundamental to provide the level of assurance and advise requested by the Governing Bodies and Management.”

SECTION E

APPENDIX

1. Details of the various regulations relevant for ESG

Corporate Sustainability Reporting Directive (CSRD)

TO WHICH COMPANIES WILL IT BE APPLICABLE?	All large companies: 250 employees and/or €40M turnover and/or €20M total assets
HOW MANY COMPANIES ARE SUBJECT TO THE NEW DIRECTIVE?	49.000 Covering 75% of total EU companies' turnover
WHAT IS THE SCOPE OF REPORTING REQUIREMENTS?	Defined by the European Sustainability reporting Standards that will be developed in various phases Set 1 has been issued in July 2023 (agnostic Standards). Main new concepts around: — Double materiality concept: Sustainability risk (including climate change) affecting the company plus companies' impact on society and ennvironment — Process to select material topics for stakeholders — More forward looking information, including targets and progress thereon — Disclose information relating to intagibles (social, human and intellectual capital) — Reporting in line with Sustainable Finance Disclosure Regulation (SFDR) and the EU Taxonomy Regulation
IS INDEPENDENT 3RD PARTY ASSURANCE MANDATORY?	Mandatory-limited level of assurance, including: — integration in Auditor's report — Audit by independent third party (statutory auditors or others) — European Assurance guidelines planned for 2026/2028
WHERE SHOULD COMPANIES REPORT?	Inclusion in the Management Report
IN WHAT FORMAT SHOULD COMPANIES REPORT?	To be submitted in electronic format (in XHTML format in accordance with ESEF regulation)

2. Internal Audit in industrial & commercial companies in Europe

Compared to other more regulated markets, such as Banks and Insurance, Industrial and Commercial companies in general have some more freedom to set up their governance structure. This is especially true for the audit, risk and compliance functions, which are usually set up in such a way that optimally supports the realization of the company's mission and objectives, balancing mandatory requirements by law or listing requirements. Despite being a less regulated environment, Industrial and commercial companies in reality generally operate in complex contexts with industry driven local legislations that require the setup of a multitude of Assurance providers (2nd Line) to strengthen the robustness of the risk management process and finally, the Internal Control System.

What is the **best setting for internal audit in industrial & commercial companies** to provide the expected added value? The Chief Audit Executive (CAE) must communicate and interact directly with the board and have direct and unrestricted access to senior management. However, in certain organization this can be achieved by a dual-reporting relationship. Furthermore, to guarantee the high level of professionalism and assurance every Internal Audit (IA) function, working in companies listed or not, big or small, has to perform its activities in compliance with the International Standards for the Professional Practice of Internal Auditing. To guarantee the compliance with the standards, each IA should be subject to a periodical quality review by an external independent and professional firm.

The Three Lines Model, published by The Institute of Internal Auditors in 2020, applies to all organizations, clarifies each player's role and the interactions. In such model, while the first and the second line roles might be blended or separated, the independence of the Internal audit role is fundamental to provide the level of assurance and advise requested by the Governing Bodies and Management.

Given the huge diversity of manufacturing companies and local legislations formally not requiring the setup of Audit shops, there are clearly some organizations with a relatively 'lower' maturity level of corporate governance, including risk and control functions. In such cases, Internal Audit could balance its advisory and assurance services.

This paper provides more insight on governance elements typical for manufacturing companies in Europe, and the role and positioning of the IAF in such companies. Such insight is relevant for anybody who wants to understand the potential of internal auditing in manufacturing companies in relation with ESG, but especially for all stakeholders and decision makers and external auditing bodies.

SECTION F

FINAL REMARKS

BIOs

- **The IIA** “The IIA’s Three Lines Model — An update of the Three Lines of Defense” July 2020
- **The IIA** “Internal Audit’s role in ESG Reporting” – May 2021
- **ECIIA** “Corporate Governance Codes on Internal Audit — Current status in the EU” 2012
- **Gartner** “2022 Audit Plan Hot Spots”
- **Gartner** “2023 Audit Plan Hot Spots”
- **The IIA & World Business Council for Sustainable Development (WBCSD)** — “Embedding ESG and sustainability considerations into the Three Lines Model”
- **The ECIIA, ecoDa and Ferma:** ESG embedding: are you ready?

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. ECIIA represents around 56.000 internal auditors .

ECIIA Industrial Committee

ECIIA set up an Industrial Committee in 2022 with Chief Audit Executives of European Companies active in industrial and commercial sectors.

The mission of the ECIIA Committee is:

“To be the consolidated voice for the profession of Internal Audit in the Industrial and Commercial 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 Industrial and Commercial Sector in Europe”.

Thank You

The paper describes the results of discussions amongst the ECIIA Industrial Committee members and we want to thank the Committee members for their input.

A big thanks as well to the redaction team: Massimiliano Turconi, CAE of Telecom Italia and Vice President of ECIIA, Carlotta Boccadoro Spot & Subsidiaries audit of Telecom Italia and Arjan Man, CAE at Atotech Group for their support.

Thank you!

European Confederation of
Institutes of
Internal Auditing

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

LINKED IN WEBSITE EMAIL X