

## Response Letter to OECD 21 October 2022

To: OECD Secretariat and OECD Corporate Governance Committee  
Submitted electronically to [CorporateGovernance&CorporateFinance@oecd.org](mailto:CorporateGovernance&CorporateFinance@oecd.org)

Dear OECD Corporate Governance Committee:

We thank you for the opportunity to share our view on the Draft Revisions to the G20/OECD Principles of Corporate Governance.

ECIIA is the European Confederation of Institutes of Internal Auditors and represent 55,000 members (via 34 National Institutes). ECIIA's primary goal is to be the consolidated voice for the profession of internal auditing in Europe, and to promote the role of Internal Audit and good corporate governance, by dealing with the European Union, its Parliament and Commission and any other European Regulators and Associations representing key stakeholders.

The ECIIA members are also members of the Institute of Internal Auditors.

We congratulate you on the proposed update to the Principles in light of recent evolutions of European Regulations in the domains of sustainability, digitalisation and the need for the businesses to be resilient in the current economic circumstances.

However, we believe that this document should better clarify the roles of internal audit and external audit and that the principles should include a separate section discussing the purpose, value, ideal structure and role of an internal audit function. Effective governance is incomplete without a robust internal audit function providing objective assurance and advice, independent from management, to the governing body and management.

It is also important to describe the role of the audit committee or equivalent body towards the internal auditors and not just towards the external auditors as mentioned currently. They play an important role in the appointment of the CAE, the budget allocated to internal audit, the definition of the mission (charter), the approval of the audit plan, the follow up of reports, recommendations and the coordination with the external auditors but also other assurance providers (such as risk management, compliance...).

The IIA's [Three Lines Model](#) is a principles-based approach that amplifies the need for robust risk management and controls as a fundamental part of governance. It is endorsed by EBA in their corporate governance guidance and used extensively, as reference, in guidance for the European financial sector.

The Three Lines Model helps organizations to identify the appropriate structures and processes that best support the achievement of business objectives to create and protect value for the organization.

Distinguishing the role of external audit versus internal audit and properly explaining and integrating internal auditing into the heart of the OECD corporate governance model will add enormous value for boards and enhance the level of trust and transparency stakeholders demand. The CEAOB, as oversight body of audit committees, has issued different guidelines regarding the cooperation between internal and external audit, also about audit quality assessment. Our proposed language for a new entry, IV.F, is included below along with edits to clarify the existing references to external audit.

In addition, internal audit also plays a key role in the recommendations included in the new Sustainability and Resilience chapter, which calls for sustainability disclosures to be “consistent, comparable and reliable” to provide investors what they need to vote and invest. Implicit in this call for quality information are the internal controls that result in information that is complete, accurate, and timely. Providing assurance over those controls is a role for internal audit, well-versed in the complete workings of the organization and responsible for controls being effective. Internal audit assists organisations beyond as well by giving insight, advice on the whole sustainability journey that includes strategy, culture, risk management.

The principles proposed address almost exclusively the listed companies, but good governance is also essential for unlisted companies.

Finally, this initiative should be coordinated with the EU initiatives about corporate governance, Sustainability Reporting Standards and the audit reform regulation.

We support the global movement for better governance and share in the OECD's goal of strengthening corporate sector resilience. We would appreciate any opportunity to further discuss this goal. Please don't hesitate to contact us, if the ECIIA can be of further assistance. Thank you for your consideration of our views.

Sincerely,

Massimiliano Turconi  
Vice President  
The European Confederation of  
Institutes of Internal Auditing

John Bendermacher  
President  
The European Confederation of  
Institutes of Internal Auditing

## DETAILED COMMENTS

The ECIIA

Recommendations for edits to the Draft Revisions to the G20/OECD Principles of Corporate Governance.

### p. 8

The Principles do not intend to prejudice or second-guess the business judgement of market participants, board members, internal auditors, and management. What works in one or more companies or for one or more investors may not necessarily be generally applicable. Companies vary in maturity, size and complexity. There is therefore no single model of good corporate governance. However, the Principles set out clear guidance for the achievement of intended outcomes and suggest some common elements that underlie good corporate governance. The Principles build on these common elements and are formulated must embrace the different models that exist.

### p.21

The responsibility for corporate strategy and operations is typically placed in the hands of the board and a management team that is selected, motivated. Internal audit plays here an important role in giving advice, assessing the implementation of strategic objectives, as examples.

### p. 32

#### **IV.A.9. Governance structures and policies, including the extent of compliance with national corporate governance codes or policies and the process by which they are implemented.**

Companies should report their corporate governance practices and such disclosure should be mandated as part of the regular reporting. Companies should implement corporate governance principles set, or endorsed, by the regulatory or listing authority with mandatory reporting on a “comply or explain” or similar basis. Most jurisdictions publish a national report reviewing adherence to the code by publicly traded companies as a good practice to support effective disclosure and implementation of “comply or explain” codes.

Disclosure of the governance structures and policies of the company, including, in the case of non-operating holding companies, that of significant subsidiaries, is important for the assessment of a company's governance and should cover the division of authority **and responsibilities** between shareholders, management, and board members. Companies should clearly disclose the different roles and responsibilities of the CEO and/or chair and, where a single person combines both roles, the rationale for this arrangement. It is also good practice to disclose the articles of association, board charters and, where applicable, committee structures and charters. Alignment should be made with the upcoming European Standards on Sustainability Reporting (from EFRAG)

p. 33

**IV.C. An annual audit should be conducted by an independent, competent and qualified external auditor in accordance with high-quality international auditing standards in order to provide reasonable assurance to the board and shareholders that the financial statements represent fairly, in all material respects, the financial position and financial performance of the company.**

In addition to the **external** auditor's opinion stating whether the financial statements represent fairly, in all material aspects, the financial position and financial performance of a company, the **external** auditor's report should also include an acknowledgement that the financial statements are the responsibility of the company's management. In some jurisdictions, the external auditors are also required to report on the company's corporate governance. **In the performance of this work, external auditors should consider relying upon any complementary work performed by internal auditors when the internal auditors have completed their work in conformance to global standards for the profession of internal auditing.**

The independence of **external** auditors, the limitation of non-audit services as well as the rotation of the external auditors are defined in the CEAOB guidance, set up after the audit reform in Europe. It is up to the audit committee or an equivalent body to oversee the overall relationship with the external auditors.

So it is important that the OECD principles are aligned with this regulation and that the role and duties of external auditors are explicit.

Therefore, we suggest to specify "external audit" in the text instead of "audit".

**IV.F. Boards should consider the establishment and on-going support of an independent, properly resourced, and qualified internal audit function with a direct line reporting to the board, an audit committee, or an equivalent body as an essential practice.**

The internal audit function plays a critical role in a company's success as well as its ability to report on financial or other disclosures. It does so by providing objective assurance, independent from management, on the internal controls and operations of the company as well as strategic advice, consulting services, and risk mitigation to management and the board. Internal auditors are uniquely positioned to examine their companies holistically, with a far broader mandate than that of external auditors, and their roles and responsibilities should be clearly articulated through dialogue and a written internal audit charter agreed upon by both the board and the Chief Audit Executive (CAE). CAE describes the role of a person in a senior position responsible for effectively managing the internal audit function in accordance with the internal audit charter and global internal auditing standards.

The board should provide oversight of the internal audit function including the appointment, reappointment and compensation of the CAE.

Internal auditors' insights, expertise and focus on risk, defined as those things which impact the ability of the organization to meet its objectives, should be leveraged to assist management and advise the board on a wide array of matters, including: climate- and sustainability-related disclosures; social and governance issues; culture; diversity, equity, and inclusion (DEI); strategy; fraud, waste, and malfeasance; cybersecurity; and data governance (privacy & security), among others.

Failure to establish an independent internal audit function should be considered a material risk to the company and boards who do not establish and support an on-going internal audit function should be required to explain annually to shareholders their reasoning for not doing so and by which mechanisms the company obtains assurance over internal operations and reporting. Furthermore, legislators, regulators, and stock exchanges should consider whether they should mandate the establishment of independent internal audit functions for publicly traded companies as necessary mechanism to protect the public interest. Where governments have laws and regulations regarding the establishment of and certification by management of a companies' internal controls, those governments should consider whether any company's internal control framework can be considered sufficiently effective without an independent internal audit function.

When establishing and evaluating an internal audit function, boards should ensure that their internal auditors are following globally accepted internal auditing standards and that staff,

in particular the CAE, hold appropriate certifications or other credentials, and/or have other on-going professional training which ensures sufficient competency to perform their roles.

In some cases, companies opt to outsource their internal audit function. In those situations, the board should carefully review the engagement to avoid conflicts of interest. Audit companies providing external audit services should never be allowed to provide outsourced internal audit services to the same client.

Given the expertise and experience of the internal audit function, external auditors may consider it appropriate in certain circumstances to rely on internal auditors' work. Where there is ambiguity, lawmakers and regulators may wish to work with stakeholders to provide additional clarity on when this is appropriate.

p. 35

## V. Responsibilities of the board

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, the active engagement of an internal audit function independent from management, and the board's accountability to the company and the shareholders.

Together with guiding corporate strategy, the board is chiefly responsible for monitoring managerial performance and achieving an adequate return for shareholders, while preventing conflicts of interest and balancing competing demands on the corporation. In order for boards to effectively fulfill their responsibilities, they must be able to exercise objective and independent judgement. Another important board responsibility is to oversee the risk management and internal controls systems and systems mechanisms designed to ensure that the corporation obeys applicable laws, including relating to tax, competition, labour, environmental, equal opportunity, data privacy and digital security, and health and safety. In some countries, companies have found it useful to explicitly articulate the responsibilities that the board assumes and those for which management is accountable. In fulfilling these responsibilities, the internal audit function also has a critical role to play in partnership with management and the board.

p. 37

**V.D.2. Reviewing and assessing risk management policies and procedures. Determining risk management policy and the company's acceptable level of risk.**

Oversight of the company's risk management is an area of major importance for boards and is closely related to corporate strategy. It involves oversight of the accountabilities and responsibilities for managing risks, specifying the types and degree of risk that a company is willing to accept in pursuit of its goals, and how it will manage the risks it creates through its operations and relationships. The board's oversight, **with the support and counsel of the internal audit function**, thus provides a crucial guidance to management in handling risks to meet the company's desired risk profile.

**pp. 37-38**

### **V.D.3. Monitoring the effectiveness of the company's governance practices and making changes as needed.**

Monitoring of governance by the board includes continuous review of the internal structure of the company to ensure that there are clear lines of accountability for management throughout the organisation. In addition to requiring the monitoring and disclosure of corporate governance practices on a regular basis, at least in summary form, many countries have moved to recommend, or indeed mandate, self-assessment by boards of their performance, as well as the assessment of the performance of their committees, individual board members, the chair and the CEO.

**Routine assessment of the company's governance practices by the internal audit function can assist boards in these monitoring responsibilities.**

**p. 39**

### **V.D.7.**

In fulfilling its control oversight responsibilities, it is important for the board to establish an **anonymous** whistleblowing policy in order to encourage the reporting of unethical/unlawful behaviour without fear of retribution. The existence of a company code of ethics should aid this process which should be underpinned by legal protection for the individuals concerned. A contact point for employees who wish to report concerns about unethical or illegal behaviour that might also compromise the integrity of financial statements should be offered by the audit committee or by an ethics committee or equivalent body.

**V.D.8. Ensuring the integrity of the corporation's accounting and reporting systems for disclosure, including the independent **external** audit, and that appropriate systems of control are in place, in compliance with the law and relevant standards.**

The board should demonstrate a leadership role to ensure that an effective means of risk oversight is in place. Ensuring the integrity of the essential reporting and monitoring systems will require that the board sets and enforces clear lines of responsibility and accountability throughout the organisation. The board will also need to ensure that there is appropriate oversight by senior management. Normally, As discussed in section IV.F., this should include the establishment of an internal audit function system directly reporting to the board. It is considered good practice for the internal auditors to report to an independent audit committee of the board or an equivalent body which is also responsible for managing the relationship with the external auditor, thereby allowing a co-ordinated response by the board.

It should also be regarded as good practice for this committee, or equivalent body, to review and report to the board the most critical accounting policies which are the basis for financial and non-financial reports.

As mentioned above, in Europe, it is regulated by the corporate governance guidance of EBA.

p. 41

**V.E.2. Boards should consider setting up specialised committees to support the full board in performing its functions, in particular the audit committee – or equivalent body – for overseeing disclosure, internal controls, risk management systems for financial and non-financial risks, and audit-related matters including internal auditors' work. Other committees, such as remuneration, nomination or risk management, may provide support to the board, depending upon the company's size, structure, complexity and risk profile. Their mandate, composition and working procedures should be well defined and disclosed by the board which retains full responsibility for the decisions taken.**

Where justified in terms of the size and structure of the company and its board, as well as the company's sector or level of development, the use of committees may improve the work of the board. In order to evaluate the merits of board committees it is important that the market receives a full and clear picture of their purpose, duties and composition. Such information is particularly important in the many jurisdictions where boards are required to establish independent audit committees with powers to oversee the work and relationship with both the internal and external auditor. Audit committees, working closely with the internal audit function, should also be able to oversee the effectiveness and integrity of the internal control system, risk management and governance.



**p. 42**

Other committees may be established to advise the board on additional issues. Some boards have created a sustainability committee to analyse in particular climate-related risks. The establishment of other committees, such as a technology committee, may also be considered by the board. Such a committee may advise on the management of digital security risks as well as on the company's digital transformation. Ad hoc or special committees can also be temporarily set up to respond to specific needs or corporate transactions. Disclosure need not extend to specific committees set up to deal with, for example, confidential commercial transactions. When established, committees should have access to the necessary information to comply with their duties, receive appropriate funding and engage **both internal audit functions** and outside experts or counsels.