

## Context:

Milieu Consulting and the Centre for European Policy Studies (CEPS) are leading a study on the effectiveness of the corporate governance framework that underpins the quality of corporate reporting for DG FISMA of the European Commission. The overall objective of this study is to gather evidence and findings that will assist the Commission services, contributing to any future evaluation or impact assessment on the topic.

The aim of the study is to:

- Gather evidence and findings on the architecture of corporate governance in a selected set of countries, the system of internal controls related to corporate reporting processes, and the systems of oversight and sanctions for corporate governance. The countries involved will include 10 Member States and two representative third countries (i.e., Japan and the US).
- Analyze the evidence to identify commonly found features of corporate governance, best practices, gaps, and potential problems.
- Identify and assess possible EU policy options to address the identified problems or facilitate the wider adoption of best practices.

ecoDa has been invited to provide its comments on the preliminary findings.

## Summary of comments:

1. **Many of the proposed elements in the recommendations already exist.**
2. Regarding responsibilities for management and nonexecutive boards, this should be done in the context of the **Shareholder Rights Directive**.
3. **Not everything should be dealt with at EU level** as focusing on generic EU-wide solutions will be neither fit nor optimal to address the issues at stake. Trainings, certifications and guidelines have been developed by practitioners, such as business organizations (national institutes as well as their European confederations such as ECIIA and IIA regarding internal control and internal audit, and FERMA regarding risk management). National corporate associations and Institutes of Directors have also developed corporate governance codes with best practices for small and large companies.
4. **The survey should have considered EU companies currently listed in the US, and EU companies who delisted from US markets.** This was a natural experiment as these companies had to implement SOX Section 404 (internal control over financial reporting assessment by management – 404a – and possibly the independent auditor assessment above certain thresholds – 404b). The views regarding the benefits and complexity of implementing an internal control assessment would have been substantially different. As

we stand more than 20 years after the implementation of SOX, the ecosystems (service providers – not limited to Big 4 firms – and guidelines / practices, adapted to various sizes of companies) are well established.

5. **The requirement to follow a reputable internal control framework would encompass many of the recommendations.** Internal control frameworks usually require many of the recommendations listed in the slides to be effectively implemented (ie. Implemented and tested as to design and operating efficiency). As an example, the implementation of SOX in the US has led to the development of practices such as 1) board members having to respond annually to very detailed questionnaires to prove their qualifications, ethics, independence, competency, and conflicts of interest, 2) annual self-assessments of boards, or 3) development of internal audit capacities (noting that these are required for NYSE listings<sup>1</sup>). Under PCAOB AS5 (the US auditing standard on “An audit of internal control over financial reporting which is integrated with an audit of financial statements”), “ineffective oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee” is an indicator of a material weakness (a *de facto* material weakness).
6. **Independent assessments of boards will cover many of the recommendations.** These practices have been well established since they were first disseminated amongst companies listed in the US as part of internal control assessment (as required by internal control frameworks and development of best practices), and many firms now exist in the EU which can service smaller and large companies to that effect. Criteria for a robust assessment of board, and how often independent assessment needs to be carried out, are also well established and there is no need to be prescriptive. The main driver for improvement to this respect, should the EU wish to go further (by way of an amendment to the current directive governing annual reports of listed companies), is to require that the name of the service provider be disclosed in the annual report together with the criteria for selection, as part of the discussion on the governance committee (or similar committee) activities in the governance statement, for investors to make their own judgment.
7. The **2014 Audit Reform** has been very complete and thorough except for the assessment of internal control over financial reporting by independent auditors (and disclosure of material weaknesses) and disclosure controls and procedures (and assessment of effectiveness by management). Although an international investor with an understanding of SOX would infer that there is an implicit management assessment to support and allow the audit committee to “monitor the effectiveness of the undertaking's internal quality

---

<sup>1</sup> 303A.07 Audit Committee Additional Requirements

The audit committee must have a written charter that addresses: (i) the committee's purpose – which, at minimum, must be to [...] (A) assist board oversight of (1) the integrity of the listed company's financial statements, (2) the listed company's compliance with legal and regulatory requirements, (3) the independent auditor's qualifications and independence, and (4) the performance of the listed company's internal audit function and independent auditors (if the listed company does not yet have an internal audit function because it is availing itself of a transition period pursuant to Section 303A.00, **the charter must provide that the committee will assist board oversight of the design and implementation of the internal audit function**). <https://nyseguide.srorules.com/listed-company-manual/09013e2c85c0074b>

control and risk management systems and, where applicable, its internal audit, regarding the financial reporting and, where applicable, sustainability reporting of the undertaking”, currently this practice does not exist. This does not mean that there is no internal control structure in EU companies; it means that there is not a systematic approach of internal control over financial reporting to assess where the risk of material misstatement are in the flow of transactions, and whether internal controls to prevent or detect a material misstatement have been correctly designed and tested. What is missing for the requirement that audit committee “monitors etc” to have substance is the formal requirement for companies to apply an internal control framework.

8. Our recommendations for improvement would be
  1. Mandatory requirement to adhere to a qualified corporate governance code, with disclosure of the gap analysis
  2. Require as a first step that management provides its assessment of internal control over financial reporting by reference to a qualified internal control framework and implementation of a testing methodology, with disclosure of resulting material weaknesses in annual reports. This would clarify the expectation under “monitors the effectiveness etc”. Requirement for mandatory independent auditor assessment should be reassessed by the EU after a period (second step).
  3. Require that independent board assessment be carried out periodically (3 years is considered international standard practice), with disclosure of the service provider name, either through listings standards in the EU or EU guidelines for internal control framework to be considered as qualified.
  4. Require that internal audit capacities (internal or outsourced) be considered mandatory above certain quantitative thresholds or qualitative criteria (complexity)
9. In order to achieve greater consistency across the EU, mandatory baseline requirements should be established to serve as **minimum qualification criteria** for the local governance codes and internal control framework. The EU could choose to have them mandatory or instead as recommendations. “Guidelines” should remain in the sphere of professional organizations.

**Details comments :**

***Slide 6 : More stringent regime in the US - full ICS evaluations, CEO/CFO certification, and external auditor attestations, publication in annual report***

ICOFR (internal control over financial reporting) assessment is conducted by both management and the independent auditor. Management assessment of disclosure controls and procedures (section 302 of SOX) should be mentioned (it provides for management to implement a group-wide system by which it will be in a situation to determine whether information need to be disclosed or not). Disclosure of ICOFR in the annual report also cover material weaknesses as well as management’s action plans for remediation and follow up of prior year material weaknesses (if any).

***Slide 6 : Sanctioning regime***

Very few MS apart France have transposed the possibility of sanctions regarding specific requirements for audit committees. The impact of sanctions should have been analyzed in terms of whether more audit committees members have been informed of their new obligations under the 20124 EU Audit Reform.

***Slide 7 : 91% declare their effectiveness***

Consider adding the basis used by management as a basis for their declaration (extent of testing and use of an internal control framework). Also, “declare effectiveness” is confusing : it is either assess effectiveness (“ICOFR assessed as effective as of [a date]”), which assume a due process for the assessment, or declare ICOFR to be effective, which does not necessarily require a due process for the assessment.

***Slide 7 : Companies in Germany, Sweden, Italy, and Ireland generally provide comprehensive ICS detail. In contrast, Croatian and Latvian reports often lack crucial specifics, hindering effective assessment.***

I’m surprised France (which I understood was scoped in) is not mentioned as comprehensive details on ICS is required in the management report. Also, ICS **description** (which I infer is what you mean by “comprehensive details”) is not the same as ICS **assessment** : one is purely descriptive (without assessment), the other requires a due process which has been tried and tested over more than 20 years now with Sarbanes-Oxley in the US. You should also mention that you probably never found mention of ICS material weaknesses in the annual report, except when the company was also listed in the US.

***Slide 8 : Survey responses from 96 stakeholders***

I very much regret that you did not use the opportunity of a real comparative study of the 3 segments : EU companies not listed in the US, EU companies currently listed in the US (how have their views changed with the implementation of SOX), and EU companies that used to be listed in the US (did they keep their SOX assessment process).

***Slide 10 : Ethical leadership, board diversity and governance training***

**Ethical leadership** : culture and ethics are foundational to every organization for matters of corporate standing, above and beyond corporate reporting. These matters are well covered by internal control frameworks (eg. Control environment in the COSO framework, which is widely used worldwide), and have been the subjects of many academic papers and practical guidelines. These topics would be *de facto* included as part of a requirement / recommendation regarding an internal control baseline, which would avoid wasting time and resources at EU level.

**Board diversity** : Practice and guidelines are now well developed around these topics and information currently available in annual reports allows investors to understand the extent of board diversity at a specific company and whether they need to engage with companies. We also believe that diversity should not be seen as an end in itself or a sort of ‘Tower of Babel’ which maximizes diversity above all else – risking inefficiency rather than cohesion. A board

requires individuals with diverse skills and expertise in different roles, but ultimately, they must all understand the business model, collaborate effectively, and work toward a shared objective. Also, diversity is a much more complex topic than looking at external traits only. We are skeptical that the three recommendations (and in particular regarding a harmonised framework and the creation of incentives) under Board diversity will improve corporate reporting and we believe that these topics would be better addressed as part of a mandatory board assessment, noting that board assessments are also covered by major internal control frameworks. The key point regarding governance is not about apparent diversity but whether governance adds real value, and diversity is one way of achieving this mostly through cognitive diversity, a much more complex topic which cannot easily be captured through disclosure of quantitative traits.

**Better trained management boards** – The recommendation should clarify whether this is intended for management (executive) board or non executive board. Regarding non executive boards, practice (as part of corporate governance codes, etc) is also well established regarding the competencies required in the topics mentioned, and these would be assessed as part of a board assessment (which would include assessment of board composition). Training is necessary to make sure that the board possesses the minimal understanding to **know that it does not know** and reviews whether it needs to bring an expert as advisor and/or review its composition to eventually add additional experience to broaden its competence and experience matrix. A board is not a collection of experts (mirroring the skills and expertise in executive management), but provides active monitoring over management. When real expertise is needed, continuous training will not provide the depth of knowledge required and boards should have the ability to bring them in : this is actually required for independent auditors (expertise in accounting principles and financial statements), recommended regarding cybersecurity (cyber audits), and should be the case whenever the board deems it necessary. A minimal adjustment such as the mandatory disclosure of adherence (and gap analysis) to a reputable corporate governance code (eg. one that would have followed a due process and be considered in the Member State as best practice, left at Member States' discretion to allow for the various governance models in the EU) should allow for these topics to be covered. These codes tend to harmonize over time to align to best practices, address the topics of minimum competence (and use of experts) and require continuous training for board members.

To summarize, we believe that all these topics will be better addressed by 1) a mandatory requirement to follow a qualified internal control framework (eg. one that would have followed a due process and be considered as best practice), with at least disclosure of management assessment (as a first step), 2) a mandatory requirement to adhere to a qualified corporate governance code, with disclosure of a gap analysis, and 3) requirement for an independent board assessment at least every three years (although major corporate governance code now tend to require such an independent assessment). In order to achieve greater consistency across the EU, mandatory baseline requirements should be established to serve as minimum qualification criteria for the local governance codes and guidelines.

***Slide 12 : Standardized evaluation of board oversight capacity***

These recommendations should be taken in the broader context of the still-to-be-completed work carried out as part of the shareholders' rights' directive.

Information on board and committee members is already required as part of the governance statement and other information required (shareholder status). Independence check and self-assessment are part of activities that are required to be conducted under major internal control framework. For example regarding companies listed in the US and as part of the implementation of SOX section 404, an annual (lengthy) questionnaire (with commitment to disclose further changes in circumstances without delay) is required from board members that cover ethics, conflicts of interest, independence, etc, including with respect to family members and direct and indirect relationships with other entities having business with the listed company.

As such, we believe all this would be covered as part of a requirement to implement a qualified internal control framework and qualified corporate governance code.

#### ***Slide 14 : Audit Committee oversight***

With the EU Audit Reform of 2014, most of these points are already covered to the highest level : engagement with external auditors, compliance with regulatory standards, independence.

Audit committee training program would be covered as part of board training (re. above adherence to a qualified corporate governance code, and independent board assessment to review substance of the qualification). Any requirement should not be too prescriptive, to allow for the different form of training : a former CFO still active at a professional organization does not require additional mandatory training (as these trainings would not have the purpose to acquire expertise as discussed above).

Regarding the provision of assurance over ICS or to provide for an IC audit committee : boards cannot multiply the number of committees. IC at large (beyond financial and sustainability reportings) is a board responsibility, and the board may decide to have a specific committee in charge of preparing a recommendation for decision by the board. With respect to internal control over financial and sustainability reportings (or ICOS, the latter being part of the audit committee's activities by default), the Audit committee will not be in a situation to provide assurance in the absence of a management assessment of ICOR. The requirement should be for the company and management to implement an internal control framework. Also, major internal control frameworks generally require an internal audit function to assist the board (and the audit committee) in its oversight and monitoring responsibilities. We believe such a function has a greater potential to improve overall governance AND the operations at a company.

We agree with the point that disparities should be addressed, mostly regarding the following topics :

- Sanctions for non-compliance with certain regulatory requirements
- External auditor's independence rules regarding non audit services (currently wide disparities across the EU, and in non EU countries) : these should be aligned so that large networks should not be able to provide non authorized services out of the country of incorporation, and out of the EU.

We believe that some other topics should be considered :

- Public disclosure of inspection report (as opposed to the audit committee having to request them)
- Requirement to establish an internal audit function

### ***Slide 15 : Internal control systems***

Topics regarding how financial and sustainability reportings are prepared are currently covered under Article 39 (6) a. , under which the Audit committee shall “monitor the financial and, where applicable, sustainability reporting process, including the electronic reporting process as referred to in Article 29d of Directive 2013/34/EU and the process carried out by the undertaking to identify the information reported in accordance with the sustainability reporting standards adopted pursuant to Article 29b of that Directive, and submit recommendations or proposals to ensure their integrity;”.

The comment regarding high implementation costs is relative and should be reviewed in light of the benefits brought by such an approach. These costs are part of the costs to access to public listings, and the real-life experiment in the US (and certain other countries) should be more specifically reviewed. Let’s remind that these systems are designed to prevent material frauds and/or errors, so investors should be informed of material weaknesses (ie. The potential for a material fraud or error to go undetected) in order to make their decision to invest or not in a company.

We dispute the shortage of skilled personnel, as the COSO framework is the basis of all the audit methodologies of the large audit firms networks (not limited to the Big 4), the ECIIA and IIA (European Confederation of Institutes of Internal Audit and Institute of Internal Audit) has developed training programs at EU level (and same is done at national levels by their national affiliates), and these competencies can be acquired over time and on-the-job training (as was the case when the US voted the SOX section 404 requirements). We believe that the perceived difficulty is more related to the fact that companies not acquainted with an internal control framework do not know what they are looking for.

### ***Slide 16 : ICS***

Training and certification programs have already been developed by ECIIA / IIA and FERMA (Federation of European Risk Management Association) regarding these matters (and further developed at the level of their national affiliates), and all these matters are already well covered by established practice (and well beyond big 4 or other large consulting firms).

### ***Slide 17 : IC reporting***

As mentioned above, trainings and certification already exist in the EU and is well developed at national levels, or can be easily developed based on EU confederations existing initiatives, provided the job market is there.

Qualified, robust, proven internal control exist, for example the COSO framework, which has been widely used by companies listed in the US to meet the requirement of Section 404 – below the reasoning of the US Security and exchange Commission in its final rule for management assessment of internal control, and the criteria for suitability of the internal control framework (including the need for comparability) (emphasis added) :

### **Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports**

<https://www.sec.gov/files/rules/final/33-8238.htm#iia3>

After consideration of the comments, we have modified the final requirements to specify that **management must base its evaluation of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment.**<sup>66</sup>

The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements. However, the final rules do not mandate use of a particular framework, such as the COSO Framework, in recognition of the fact that other evaluation standards exist outside of the United States,<sup>67</sup> and that frameworks other than COSO may be developed within the United States in the future, that satisfy the intent of the statute without diminishing the benefits to investors. The use of standard measures that are publicly available will enhance the quality of the internal control report and will promote comparability of the internal control reports of different companies. The final rules require management's report to identify the evaluation framework used by management to assess the effectiveness of the company's internal control over financial reporting.<sup>68</sup>

**Specifically, a suitable framework must: be free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted; and be relevant to an evaluation of internal control over financial reporting.**

Since the start of SOX Section 404 in the US, implementing ICOR in various types of corporate environment (from very large groups to smaller entities) has been widely tested, researched and analysed, with a lot of practical guidance issued. This is a key point as in certain countries (eg. Poland, Italy) listed entities are mostly composed of SMEs (please note that the US has a 2-step system by which SOX Section 404 is applicable to listed SMEs above certain thresholds, with a requirement for management assessment only (this is 404 a), to be extended to auditor's assessment when they exceed another set of thresholds (404 b).

It is difficult to understand the statement of “complex regulatory environment” unless it points out to a lack of familiarity with these topics and the way they have been put into

practice in the EU by either EU companies listed in the US or subsidiaries of non-EU groups listed in the US.

***Slide 18 : ICOR***

As mentioned above, well established training programs already exist regarding ICS.

Comprehensive guidance already exist and is used by a portion of companies in the UE. Leveraging existing guidance will prove less expensive than developing, publishing and training on an EU-specific guidance.

We agree that reporting formats should be harmonized across the EU, and we emphasize the fact that a mere description of internal control over (financial and sustainability) reporting is **NOT** a substitute for an actual assessment of the efficiency of such internal control system (no systematic, robust, risk analysis over the significant flow of transactions, no objective testing, no qualification process of the severity of the reported deficiencies).

We agree that the independent statutory auditor should be in charge of a separate assurance process for internal control over financial reporting. However, we recommend that a 2-step approach be considered to smoothen the impact on companies : require first a management assessment with disclosure of material weaknesses in annual reports (together with management plans for remediation), and in a second step (some years after) the independent auditor's own assessment. Internal control assessment regarding sustainability information should be reviewed in a separate stage considering that this reporting is new to a lot of companies (beyond 1<sup>st</sup> wave), and that the upgrade for financial reporting will pave the way for the rollout on sustainability reporting.

Contact person:

Anne-Hélène Monsellato, Leader of the Working Group on Audit Committee and of the Working Group on Sustainable Champions.