European Confederation of Institutes of Internal Auditing

Brussels, October 16, 2024.

M. Julve- Head of Division Non-Financial Risks
F.Narring Head of Section Governance and Risks
ECB Supervision
60640 Frankfurt am Aim

Overview of remarks on the "Draft guide on governance and risk culture" by the ECIIA working group

We, the ECIIA, welcome the guide on governance and risk culture and thank the ECB for the opportunity to comment on the draft guide.

ECIIA is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and represent 55.000 members. ECIIA is the consolidated voice of the profession of internal audit and aims advocating the internal audit profession as part of good corporate governance, by achieving thought leadership through publications on relevant topics and by interacting with the regulators, as required, and any other appropriate institutions of influence at European level.

We consider the overall draft guide as suited for strengthening the governance and risk culture in ECB supervised banks and developing a strong and resilient banking system. Further, we acknowledge that the guide is based on a best practice-driven approach rather than creating additional rules and regulation. We trust that the guide will be of great help for Internal Audit Functions (IAF) to assess the governance and risk culture in banks.

In the following, we have summarized some aspects as general comments. We suggest that these comments could be more clearly reflected in the guideline based on our professional understanding.

1. Consideration of different governance systems

We acknowledge that the guide accounts for different governance structures and various national laws and business models of banks within the EU. However, we find that the diversity and variety of corporate governance models in Europe (especially one tier vs two tier governance systems) is not sufficiently reflected throughout the current draft guide. There is no one size fits all[1]. We suggest having a clear statement in the introduction of the guide that accounts for different governance schemes which might cause a legitimate deviation from the guide.

Further, the guide does not properly reflect the interaction of the IAF with the management body and audit committee in different governance systems (e.g. the follow-up process of finding and reporting process). We suggest having more flexibility for this practice.

[1] ECIIA recently published a paper on this topic, illustrating the differences in European Banks: https://www.eciia.eu/2024/08/auditing-risk-culture/

European Confederation of Institutes of Internal Auditing

2. Global Internal Audit Standards (2024)

The IAF is an integral part of a strong governance. To further strengthen the role of the IAF we strongly recommend to refer to the IIA Global Internal Audit Standards (GIAs[2]) in the ECB guide in a general manner (currently mentioned as a footnote (142)) as they guide professional practices and serve as guidance for the quality assessment of the IAF.[3]
Further, the IIA has changed the terminology of "three lines of defense" to "three lines model" in 2020. We suggest to use the new terminology and definition consistently throughout the document.[4]

3. Risk based audit approach

We welcome that in chapter 4.2.3 "Internal audit function", the importance of a risk-based audit approach is referred to in various places. To further strengthen a risk-based audit methodology it should be extended to further audit processes mentioned in the guide, in particular when considering supervisory findings and measures within the processes of the IAF (e.g. risk assessment, audit planning, follow-up and reporting).

Referring to the audit cycle, the ECB recommends that activities and processes are audited at appropriate intervals, depending on their level of risk classification. An audit cycle no longer than 5 years (national legal requirements may impose a different timeframe) is mentioned. We understand that a cycle of 5 years must be guaranteed for all components of the audit universe. We recommend to account for the risk-based nature of the audit plans instead.[5]

4. Observed good practices

As the guide is written in the spirit of providing helpful support "observed good practices" are included in multiple places. However, the purpose and content of the examples are not always clear. Further, the integration of the "observed good practices" part might cause misinterpretations and confusion in upcoming regulatory examinations. We would like to ask you to define the term more clearly or to explain it in more detail.

We have detailed our recommendations in the attached document and are available for further discussions on this important topic.

Sincerely

Andrea Bracht

ECIIA Vice President and Chair of the ECIIA Banking Committee

---

[2] The Global Internal Audit Standards are available on https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
[3] The EBA guideline on internal governance (EBA/GL/2021/05) explicitly refers to the current IPPFs that will be replaced by the GIAs as from January 9,2025.
[4] The updated 3 lines model has been published by IIA Global in 2020: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf
[5] The EBA guideline on internal governance (EBA/GL/2021/05)refers to materiality thresholds, which confirms the risk based approach.