



**COMMENTS TO THE DISCUSSION PAPER OF THE
BANK OF ITALY’S “DISPOSIZIONI DI VIGILANZA
PRUDENZIALE PER LE BANCHE – SISTEMA DEI
CONTROLLI INTERNI, SISTEMA INFORMATIVO E
CONTINUITÀ OPERATIVA”**

Deutsche Bank SpA



We hereby want to follow up the invitation of this Authority to provide observations, comments and proposals to the discussion paper referred to the “Prudential Supervisory Regulations for Banks - internal control system, information system and business continuity”.

This document is composed of a first part referring to general topics or topics having impact on different parts of the forthcoming regulation and a second part related to specific matters.

Although some comments presented here may overlap the respective ones provided by the Associazione Bancaria Italiana (ABI), this paper seeks to integrate that position paper, for the most part shared, with the specificity of this Bank.



OVERALL COMMENTS

We consider creditable and welcome the initiative to include different regulatory aspects in a single document as well as the recognition of the importance of the proportionality principle.

With reference to the latter, the document largely discusses proportionality in as it relates to smaller banks. In our opinion, it is also important to recognize the effectiveness of the common internal control system and risk management of large cross-border banks established within the EU. To achieve this total effectiveness, that on a consolidated level, and consequently at a European level, is a better solution, a completely autonomous, stand-alone internal control system based on detailed local requirements for each country where the Bank has a subsidiary is not possible. To reach effectiveness, one of the main aspects is exploiting the competences and reducing the complexity, centralising and sharing the processes and systems.

As a consequence, it could be appropriate to include references to this kind of intermediaries and specific differential requirements. In particular, the possibility to recognize substantive compliance with the requirements when the large cross-border EU banks meet the control requirements of their home regulator should be considered. Clearly, the principles established by the Italian regulation must be anyway satisfied; on the contrary, within the conditions above, the more detailed points may differ.

Several EU regulators put in place similar sets of requirements – in particular in Germany Minimum Requirements for Risk Management (commonly referred to as MaRisk) are established – and many EU banks will be subject to those potentially different sets. Allowing for recognition of substantive compliance, as indicated above, is particularly important as requiring cross-border banking groups to meet the detail of all similar sets of requirements may increase operational complexity and risk without improving controls. This should be read considering the context of the EBA's role in establishing a single Rule Book and a common set of supervisory standards.

Regards should be had, as well, to the probable introduction of the European Central Bank as lead supervisor under a Single Supervisory Mechanism to which many of those banks will be subject.



A second general comment, partially connected to the previous, is related to the process and control governance in a cross-border group. In this perspective, the local subsidiaries should be allowed to adopt and rely on group policies, procedures and controls in line with European legislation, adapting them, in case, to the local requirements. This means, for example, that Deutsche Bank SpA's policies could include processes and controls performed by the European parent company (e.g.: risk measurement models, IT systems, etc.).

Another example is related to the body with management function. It might be not necessary to define the risk management function on a country basis but it would be reasonable to ask the body in Italy with the management function to satisfy itself that the Group's risk management process is sufficient to address the risks that may arise in Italy.



SPECIFIC COMMENTS

Titolo V – Capitolo 7
IL SISTEMA DEI CONTROLLI INTERNI

Sezione III **Funzioni aziendali di controllo**

Funzione di conformità alle norme (compliance)

On the perimeter of activities under compliance function supervision, the document should clarify that responsibilities of the compliance function do not extend to those regulations for which the legislation requires the presence of specific roles or functions already responsible for managing risks (e.g. the legislation on safety at work and business continuity). In such cases, compliance function should only check that the company roles and functions above have been correctly identified and an appropriate risk management framework is in place.

With regard to the special attention required for compliance of corporate activities with tax regulations, we believe that banks should be granted autonomy to adopt internal organizational measures in order to achieve the outcomes of the paper (i.e. enforce second level controls on committing breaches or tax evasion), leveraging on the existence of a specialized function, i.e. a Tax department usually existing in larger organisation such as Deutsche Bank. Tax department is normally assigned duties that include interpretation and support in implementation of tax laws; such activities are already aimed at managing risk of non compliance with the regulation. This could also avoid the duplication of expertise and make the control activity more effective, in line with the possibility, highlighted in the paper, to entrust compliance function activities to other organisational structures with necessary professional skills, provided that they are duly coordinated and supervised (for this purpose, we also suggest to explicitly include Tax in the existing example list of functions who usually perform compliance activities).

In this context, we also highlight the need for a clearer definition of the purpose of the verification, especially with reference to the potential uncertainty of cases such as violation or circumvention of applicable legislation, including situations of abuse of law.



Funzione di controllo dei rischi (risk management function)

In the discussion paper, the “Funzione di controllo dei rischi” is named in English “risk management function”. Also considering that in the note 21 at page 19 its segregation from the risk operative management functions is plainly stated, we would suggest to clarify the difference between “control” and “management” functions for risk processes as well as the approach in terms of respective reporting lines. In particular, we would appreciate a confirmation that the above request for segregation makes it not feasible to have both functions within the same structure such as the Chief Risk Officer.



Titolo V – Capitolo 7
IL SISTEMA DEI CONTROLLI INTERNI

Sezione IV
Esternalizzazione di funzioni aziendali (outsourcing)

With reference to the provision indicating the communication duties to this Authority in case of outsourcing of important operating functions or control functions, we would ask to exclude from this provision the intra-group outsourcing. At this aim, “intra-group outsourcing” means that the activities no more performed directly by the Bank are carried out by a legal entity controlled in terms of ownership by the Bank or by another legal entity belonging to the same group the Bank is part of. To this extent, the “group” is intended as both the Italian banking group and the international banking group referring to a cross-border EU parent company (in our case, Deutsche Bank AG).

We believe the outsourcing risk is much lower in case of intra-group transactions/service relationships since the legal entity carrying out the activities is anyway under the control of either the Bank or the relevant group and applies the same control framework, policies and processes in line with the provisions of its main European Regulator.



Titolo V – Capitolo 8
SISTEMA INFORMATIVO

As a general comment, we reinforce here the principle stated at the beginning of our comments regarding the adequacy of Group policies, procedures and controls to ensure that the objectives of the paper are met.

Sezione IV
Il sistema di gestione della sicurezza informatica

Security incident management

A clarification would be useful on the criteria to determine the “high levels of economic losses or prolonged periods of inefficiency” prompting the need for the communication to the Bank of Italy, especially when they are the results of “repeated occurrences of incidents of lesser significance”.

Sezione VI
L’esternalizzazione di sistemi e servizi ICT

Please refer to the comments provided with regard to outsourcing. In this particular context, it is worth highlighting that most of projects with IT impacts carried out within Deutsche Bank Group are linked to global initiatives requiring the involvement of vendors with data center located outside Italy. These cases could be considered as eligible for exemption in the light of the already mentioned global control framework safeguarding the relevant risks.