Referring to the consultation draft of Guidelines of the Basel Committee on Banking Supervision (GL) regarding the principles of corporate governance of banks, the KNF - Polish Financial Supervision Authority shall make a polite request to consider the following position:

The KNF – Polish Financial Supervision Authority welcomes the revised draft of GL, which adequately addresses the most important current issues related to corporate governance in banks. The experience of recent years shows that corporate governance has recently become a key element in the sound and prudent management of banks, and thus one of the basic factors of stability of the banking system. For special appreciation deserves highlighting in GL issues pertaining to risk management, control functions and generally - culture of risk in the bank. These issues are also standard elements of recommendations in respect of corporate governance issued by the KNF – Polish Financial Supervision Authority for supervised entities. The KNF – Polish Financial Supervision Authority presents below detailed comments to the content of the draft of GL and kindly asks for their consideration.

1. In paragraph 20 we propose to underline also the safety of the deposits as one of the main areas of responsibility of the board.

2. With regard to Principle 2, it should be underlined that (good) reputation of the board members should be ensured and taken into consideration not only in the selection process, as it arises from paragraph 49, but also as a general rule of the composition of the board. We propose to supplement the provisions of GL accordingly, i.e. to add the reference to the reputation in the wording of the Principle 2, paragraph 46 regarding the composition of the board and the suitability qualities of the individual board members and paragraph 51 relating to the actions taken in case a board member ceases to be suitable. We also believe that the requirement of good reputation should relate explicitly to the senior management as well, whereas paragraph 88 mentions “integrity” which seems to have more narrow meaning than “good reputation” has. For these reasons also paragraph 44 should be in our opinion supplemented, for example by adding new bullet relating to the assessment of the senior manager’s reputation and to taking appropriate actions on the basis of the assessment’s results.

3. It is not clear whether last sentence in Principle 5 should relate to the bank’s or rather group’s operational structure.

4. The approach accepted in paragraph 11 will be justified, if it is emphasized that, in the processes of risk management and compliance the phase of control is applied and that the control mechanisms (internal controls) are present in all lines of defense and at all stages of the processes. E.g. control mechanisms, such as the division of responsibilities, verification, endorsement, control of accesses, trainings, superior’s supervision, etc. are also applied in the identification of risk.

5. Separation and description of the functions: risk management, compliance and internal audit brings order in respect of the definitions. However, calling them (in particular the risk management function) control functions in banking organization may give causes for concern. It should be noted that the process of risk management is much broader than solely ensuring the achievement of the objectives within the control function, regardless of whether the control is understood as the process of comparing the current situation with the required one or as process in the management component, or as operations to ensure

the achievement of the objectives, inter alia, through the use of control mechanisms (internal controls).

6. The consistency of GL with the Core Principles for Effective Banking Supervision should be considered. In particular, it seems that control functions (internal control framework) are presented in a slightly different way in both documents.

7. In paragraph 28 we propose to mention also the "compliance culture" while listing the areas of the board's activity in promoting a sound corporate culture.

8. The proposed presentation of internal control only as a set of control mechanisms with a subordinate and supportive function to all three so called control functions (i.e. risk management, compliance, internal audit) deserves a positive opinion. It solves the problem of the relationship between risk management and internal control systems, including distinguishing control mechanisms within the internal control system from the control mechanisms of risk management, such as limits, procedures, policies (paragraph 113 of GL), and indicates that the control mechanisms should operate for the needs of all three functions. However, in the opinion of the KNF – Polish Financial Supervision Authority, the proposed concept could be supplemented by:
   - distinguishing within the frame of the internal control system, apart from control mechanisms (internal controls), also other elements of this system (e.g. the control environment, referred to in paragraph 75 of GL), which will enable to evaluate the internal control system (and not solely the mechanisms alone), according to the proposed concept of reasonable assurance,
   - emphasizing that the control mechanisms support also other functions / objectives within the organization, connected in particular with financial reporting,
   - perception of limits, procedures and policies also as control mechanisms that can be applied by both systems internal control and risk management,
   - mentioning of applying control as an element of the management process and of control as control mechanisms in each business line; in the proposed document, it is frequently omitted (paragraphs 31, 40, 41, 103, 107), although it is included in the definition of the internal control system, paragraph 92 and in content of Principle 7 of the document,
   - replacing the phrase "internal control failures" by "internal control weakness" or by "internal control deficiencies" - the terms more commonly used especially in the US and EU regulations.

9. In our opinion the three functions – risk management, compliance and internal audit should be independent and isolated from each other but also from the bank's operational activity which generates risks subject to mitigation by these functions. Moreover the independence of the functions should not be related to the senior management duties only but to the whole organization. We propose to redraft paragraph 91 in the following way:

   The risk management, compliance and internal audit functions should be independent and isolated from each other but also from the bank's operational activity which generates risks subject to mitigation by these three functions. This independence and isolations should be recognized and respected by the board and senior management throughout the organization. This means in particular that persons involved in controlling, managing and exercising these functions should be independent from each other and should not interfere

in the exercise of their duties with this respect nor should they be involved in or responsible for the bank's operational activity which generates risks. For example, the same senior manager or in the one-tier structure the same member of the management board cannot oversee nor be directly, individually responsible for two of these three functions or for one of these functions and the area of bank's operational activity generating risk (e.g. for lending activity and management of credit risk).

10. We propose completing compliance's responsibilities with the compliance risk management and considering whether it should be a part of the internal control system (as perceived by EBA) or as an element of risk management (as the Basel Committee perceives it so far). The document may be interpreted in the way that advising is the main function of compliance, which is not corresponding with essence of compliance itself and the document of the Basel Committee, "Compliance and the compliance function in banks".

11. The draft document insufficiently emphasizes the significance of risk control function, which is very important and commonly recognized element of the risk management process. In our opinion irrespective of Principle 7 risk control should be considered also at least in following paragraphs: 103 (key activities of the risk management function), 107 (responsibilities of the CRO), and 110 (elements of risk governance framework).

12. We propose extending Principle 7 (Risk identification, monitoring and controlling) by adding the obligation to carry out and to document the stress tests for the significant types of risk.

13. The reporting system (Principle 8) has been limited to "risk communication". It is an important element of MIS (Management Information System), but for the purpose of management the information on e.g. the implementation of the strategy and business objectives is equally important.