Response to feedback received
Compliance

Introduction
The Bank today finalised for issuance the policy document on *Compliance* for financial institutions, incorporating the proposals from the concept paper issued in September 2014 and taking into account feedback received during the consultation period.

The Bank received written responses from 65 respondents, including financial institutions, industry associations and a regulatory body during the consultation period. A series of engagement sessions were also conducted to allow for a more focused and in-depth discussions on the proposed requirements.

The Bank appreciates the feedback and suggestions received during the consultation process. Key comments received and the Bank's responses are provided in the following sections. Other comments and suggestions for clarification have been incorporated in the final policy where appropriate.

Bank Negara Malaysia
2 October 2015

1. Definition of compliance risk

1.1. The concept paper defined compliance risk as *"legal and regulatory risk arising from non-compliance to legal and regulatory requirements (including Shariah requirements)"*. The intention of the definition was to capture the risk of litigation and other forms of legal enforcement that may be brought against a financial institution as a result of non-compliance.

1.2. A number of respondents highlighted that legal risk extends to risk associated with the drafting of legal documents, which typically does not fall within the compliance function's responsibility.

1.3. The Bank acknowledges that the inclusion of legal risk would extend the responsibilities of the compliance function beyond the intention of the policy. To better reflect the intended risk, the Bank has revised the definition to *"the risk of legal or regulatory sanctions, financial loss or reputational damage which a financial institution may suffer as a result of its failure to comply with legal and regulatory requirements applicable to its activities."*

1.4. The Bank has also clarified in the final policy that legal and regulatory requirements shall include rulings by the Shariah Advisory.

2. Organisation of the compliance function

2.1. The concept paper proposed that the compliance function consist of the Chief Compliance Officer (CCO) and staff or groups of staff carrying out compliance function responsibilities, and that the CCO would be primarily responsible for overseeing the compliance function.

2.2. A number of respondents requested clarity on whether the Bank intends to prescribe a specific organisational structure for the institution's compliance function. Respondents highlighted that this approach could potentially be challenging for institutions where compliance function responsibilities are currently shared with other control functions, as significant changes may have to be made to existing structures and reporting lines.

2.3. The Bank wishes to clarify that it is not the intention of the policy to prescribe a specific organisational structure or reporting line for the compliance function. However, the final policy reiterates the role of the CCO as the central point of authority for institution-wide compliance matters, regardless of how the compliance function is structured within the institution.

2.4. The final policy also emphasises that where the compliance function responsibilities are shared across several control functions (with the exception of internal audit), the Bank expects the CCO to have the overall responsibility for coordinating the identification and management of compliance risk at the institution-wide level, and to ensure that compliance monitoring and testing are carried out consistently across the institution. For this purpose, the CCO must have a sound understanding of compliance risks which are under the purview of other control functions, including an

understanding of controls applied to manage these risks.

3. Engagement between the board and the CCO

3.1. The concept paper proposed that compliance matters be reported by the CCO to senior management, and by senior management to the board. This reporting arrangement was proposed in order to encourage stronger ownership by senior management of the management of compliance risk and to provide the opportunity for senior management to rectify – taking into account the assessments of the compliance function – any weaknesses in the internal controls for which they are respectively responsible.

3.2. A number of respondents highlighted that the requirement for the CCO to report compliance matters to senior management and not directly to the board may undermine the CCO's stature and independence.

3.3. The Bank maintains the view that it is crucial for senior management to be kept informed of compliance matters at an early stage in order to promote their participation in the management of compliance risk. At the same time, the standard preserves direct and unimpeded access of the CCO to the board and an expectation for the board to regularly engage with the CCO (see paragraphs 6.3(c) and (d)). This includes engaging the CCO without the presence of other members of SM where the board considers this to be useful.

4. Relationships of the compliance function with business lines and with the internal audit function

4.1. The Bank has observed that a large majority of financial institutions find the involvement of the compliance function in business processes to be valuable in contributing towards the effective management of compliance risk. Accordingly, the Bank has not sought to preclude such arrangements. The final policy document emphasises that where these arrangements are adopted, the compliance function must not be placed in a position of conflict or be prevented from highlighting compliance issues relating to any business decision to the board or senior management.

4.2. The concept paper also proposed that the compliance function perform testing on internal controls put in place to manage compliance risk. A few respondents highlighted that this may result in an overlap between the testing of controls by the compliance and internal audit functions.

4.3. The Bank views that such overlaps are not inconsistent with the functions performed by compliance and internal audit as the second and third lines of defence respectively. Paragraph 9.1 of the final policy clarifies that the testing of controls by internal audit should be commensurate with the perceived level of risk as assessed in the internal audit's evaluation of the adequacy and effectiveness of the compliance function.

5. Application of the policy at the financial holding company level

5.1. The concept paper proposed for the policy requirements to be applied at the financial holding company (FHC) level. Some respondents requested for clarification on the operationalisation of the requirements, particularly with regard to establishing a group CCO and compliance function at the FHC level.

5.2. The Bank wishes to clarify that financial institutions will be required to establish a group CCO and compliance function at the FHC level to oversee compliance risk at the group-wide level, including for entities which are not within the Bank's regulatory purview. This is in line with the Bank's *Approach to Regulating and Supervising Financial Groups*.