

## 161 COMPLIANCE FRAMEWORK

**Compliance Risk Management.** BSFIs shall establish a dynamic and responsive compliance risk management system. The compliance risk management system shall be designed to specifically identify and mitigate risks that may erode the franchise value of the BSFI such as risks of legal or regulatory sanctions, material financial loss, or loss to reputation, a BSFI may suffer as a result of its failure to comply with laws, rules, related self-regulatory organization standards, and codes of conduct applicable to its activities. Said risk may also arise from failure to manage conflict of interest, treat customers fairly, or effectively manage risks arising from money laundering and terrorist financing activities. Compliance risk management should be an integral part of the culture and risk governance framework of the BSFI. In this respect, it shall be the responsibility and shared accountability of all personnel, officers, and the board of directors.

**Compliance function.** The compliance function shall have a formal status within the organization. It shall be established by a charter or other formal document approved by the board of directors that defines the compliance function's standing, authority and independence. It shall have the right to obtain access to information necessary to carry out its responsibilities, conduct investigations of possible breaches of the compliance policy, and shall directly report to and have direct access to the board of directors or appropriate board-level committee.

The compliance function shall facilitate effective management of compliance risk by:

- a. Advising the board of directors and senior management on relevant laws, rules and standards, including keeping them informed on developments in the area;
- b. Apprising BSFI personnel on compliance issues, and acting as a contact point within the BSFI for compliance queries from BSFI personnel;
- c. Establishing written guidance to staff on the appropriate implementation of laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines;
- d. Identifying, documenting and assessing the compliance risks associated with the BSFI's business activities, including new products and business units;
- e. Assessing the appropriateness of the BSFI's compliance procedures and guidelines, promptly following up any identified deficiencies, and where necessary, formulating proposals for amendments;

- f. Monitoring and testing compliance by performing sufficient and representative compliance testing;
- g. In the case of branches of foreign banks, the compliance function shall be responsible for maintaining official English translation of bank documents including, but not limited to policies, procedures, manuals, and all documents supporting the approval of transactions and contracts/agreements entered into; and
- h. Maintaining a constructive working relationship with the Banko Sentral and other regulators.

**Compliance program.** The compliance program shall set out the planned activities of the compliance function, such as the review and implementation of specific policies and procedures; compliance risk assessment; compliance testing; educating staff on compliance matters; monitoring compliance risk exposures; and reporting to the board of directors or board-level committee. The program shall espouse a risk-based approach and shall have appropriate coverage across businesses and units. For this purpose, the compliance program shall be updated on a regular basis or at least annually.

In case of group structures, there should be a board-approved policy that defines the compliance framework that shall apply to entities across the group. The policy shall provide the structure that shall be adopted by the group, either to establish the compliance function centrally at the parent bank or in each of the identified subsidiary. Such policy shall also include the overall responsibility of the parent bank's compliance function with respect to the management of compliance risk exposures of subsidiaries/affiliates.

The establishment of compliance function centrally by the parent bank in group structures shall not fall under the outsourcing framework as provided under Sec. 112. In this respect, the head of the compliance function of the parent bank shall define the compliance risk management strategies, processes, and communication framework for the entire group: *Provided*, That this shall be done in consultation and coordination with the respective board of directors of the subsidiary or affiliate BSFI: *Provided, further*, That the board of directors of the subsidiary or affiliate BSFI, shall remain ultimately responsible for the performance of the compliance risk management activities.

**Chief Compliance Officer (CCO).** The CCO should have the necessary qualifications, experience, and professional background and should have a sound understanding of relevant laws and regulations and their potential impact on the BSFI's operations. The CCO should be up-to-date with the developments in laws, rules and standards maintained through continuous training. BSFIs shall appoint a CCO who shall serve on a full-time basis and shall functionally report to the board of directors or board-level committee. BSFIs operating on a business model deemed simple by the Banko Sentral, by virtue of

their scale and complexity of activities, may designate its Internal Auditor to serve as the CCO in concurrent capacity. Banks with subsidiary banks and quasi-banks may appoint a CCO for the banking group: *Provided*, That the parent bank can show to the Bangko Sentral that the compliance function is conducted on a group-wide basis. In cases of branches of foreign banks, the CCO shall report to the regional/group compliance function.

An appointed CCO has the burden to prove that he possesses all the minimum qualifications and none of the disqualifications by submitting to the Bangko Sentral proof of such qualifications <sup>1</sup>. Non-submission of complete documentary requirements within the prescribed period shall be construed as his failure to establish his qualifications for the positions and results in his removal as CCO. The Bangko Sentral shall also consider its own records in determining the qualifications of a CCO.

The CCO shall oversee the identification and management of the BSFI's compliance risk and shall supervise the compliance function staff. He is expected to liaise with the Bangko Sentral on compliance related issues and shall also be responsible for ensuring the integrity and accuracy of all documentary submissions to the Bangko Sentral. He shall functionally meet/report to the board of directors or board-level committee and such meetings shall be duly minuted and adequately documented. In this regard, the board of directors/board-level committee shall review and approve the performance and compensation of the CCO, as well as the budget of the compliance function.

In case of group structure, the head of the compliance function of the parent bank shall define the compliance activities for the entire group: *Provided*, That this shall be done in consultation and coordination with the respective board of directors and CCO of the subsidiary or affiliate BSFI: *Provided, further*, That the board of directors of the subsidiary or affiliate BSFI, shall remain ultimately responsible for the performance of compliance activities.

**Responsibilities of the board of directors and senior management.** Aside from the duties and responsibilities of the board of directors mentioned under Sec. 132, the board of directors shall ensure that a compliance program is defined for the BSFI and that compliance issues are resolved expeditiously. For this purpose, a board-level committee, chaired by a non-executive director, shall oversee the compliance program.

The board of directors shall ensure that BSFI personnel and affiliated parties adhere to the pre-defined compliance standards of the BSFIs. Implementation of the compliance program rests collectively with senior management, of which the CCO is the lead operating officer on compliance. Senior management, through the CCO, should periodically report to the board of directors or its designated committee matters that affect the design and implementation of the compliance program. Any changes, updates and amendments to the compliance program must be approved by the board of directors. However, any material breaches of the compliance program shall be reported to and

promptly addressed by the CCO within the mechanisms defined by the compliance manual.

A compliance system found to be materially inadequate shall be construed as unsafe or unsound banking.

**Cross-border compliance issues.** The compliance function for institutions that conduct business in other jurisdictions should be structured to ensure that local compliance concerns are satisfactorily addressed within the framework of the compliance policy for the organization as a whole. As there are significant differences in legislative and regulatory frameworks across countries or from jurisdiction to jurisdiction, compliance issues specific to each jurisdiction should be coordinated within the structure of the institution's group-wide compliance policy. The organization and structure of the compliance function and its responsibilities should be in accordance with local legal and regulatory requirements.

**Outsourcing of compliance risk assessment and testing.** The review, assessment and testing of the compliance program may be outsourced to qualified third parties. The handling and management of this outsourcing arrangement shall be governed by Sec. 112.

*(Circular Nos. 972 dated 22 August 2017, 969 dated 22 August 2017 and 893 dated 16 November 2015)*

#### Footnotes

1. Using the list in Appendix 101 as guide.