142 RISK GOVERNANCE FRAMEWORK

The risk governance framework shall include policies, supported by appropriate processes and control procedures, designed to ensure that the risk identification, aggregation, mitigation and monitoring capabilities are commensurate with the BSFI's size, complexity, risk profile, and systemic importance. The risk governance framework shall consider the entities in the conglomerate and shall be applied on a group-wide scale.

a. *Risk appetite.* The BSFI's risk appetite shall be clearly conveyed through a risk appetite statement that can be easily understood by all relevant parties, e.g., board of directors itself, senior management, employees, the public, regulators, and other stakeholders. The risk appetite statement shall represent the individual and aggregate level and types of risk that the BSFI is willing to assume in order to achieve its business objectives and considering its capability to manage risk.

b. *Risk management policy.* Risk management policies shall cover:

(1) structure of limits and guidelines to govern risk-taking. These shall include actions that shall be taken when risk limits are breached, including notification and escalation to higher level of Management and corresponding sanctions for excessive risk taking;

(2) clearly delineated responsibilities for managing risk based on the three (3) lines of defense;

(3) system for measuring risk;

(4) checks and balances system; and

(5) framework for risk data aggregation and risk reporting.

c. *Risk management processes and infrastructure.* The degree of sophistication of the risk management and internal control processes and infrastructure shall keep pace with developments in the BSFI such as balance sheet and revenue growth; increasing complexity of the business; risk configuration or operating structure; geographical expansion; mergers and acquisitions; or the introduction of new products or business lines, as well as with the external risk landscape; business environment; and industry practice. This should enable a dynamic, comprehensive, and accurate risk reporting both at the disaggregated (including material risk residing in subsidiaries) and aggregated level to allow for a BSFI-wide or integrated perspective of risk exposures.

In this respect, BSFIs shall ensure that their risk data aggregation capabilities meet the following principles:

(1) *Accuracy and integrity* – this refers to the capability to generate accurate and reliable risk data to meet normal and stress reporting accuracy requirements.

(2) *Completeness* – this refers to the capability to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and other groupings, as relevant for the risk in question, and should permit the identification and reporting of risk exposures, concentrations, and any emerging risks.

(3) *Timeliness* -this refers to the capability to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. Timing shall depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the BSFI. Timing shall also depend on the BSFI-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the BSFI.

(4) *Adaptability* – this refers to the capability to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

d. *Risk identification, monitoring and controlling.* BSFIs shall identify and assess all material risks including new and emerging risks, as well as hard to quantify risks, e.g., reputational risk, on a group-wide and entity specific levels. In this respect, BSFIs should use accurate internal and external data and consider the external operating environment in the risk assessment process to inform strategic business decisions and risk management approaches.

e. *Risk communication.* BSFI shall promote an open communication about risk issues, including risk strategies across the organization. They shall adopt an effective information sharing and communication system enabling the timely, accurate, concise, and understandable transfer of information. This includes the risk reporting framework, which should accurately communicate risk exposures and results of stress tests and should promote robust discussion of risk exposures.

The risk reporting framework should be governed by the following principles:

(1) *Accuracy* – Reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. In this regard, relevant reports should be reconciled and validated.

(2) *Comprehensiveness* – Reports should cover all material risk areas within the organization. The depth and scope of these reports should be consistent with the size and complexity of the BSFI's operations and risk profile, as well as the requirements of the users of information.

(3) *Clarity and usefulness* – Reports should communicate information in a clear and concise manner. Reports should be easy to understand and comprehensive enough to facilitate informed decision-making. Reports should include meaningful information tailored to the needs of the recipients.

Risk management function. The risk management function shall be responsible for overseeing the risk-taking activities across the BSFI, as well as in evaluating whether these remain consistent with the BSFI's risk appetite and strategic direction. It shall ensure that the risk governance framework remain appropriate relative to the complexity of risk taking activities of the BSFI. The risk management function shall be responsible for identifying, measuring, monitoring and reporting risk on an enterprise-wide basis as part of the second line of defense. It shall directly report to the Risk Oversight Committee (ROC) or the board of directors, as applicable. Personnel in the risk management function should collectively have knowledge and technical skills commensurate with business activities and risk exposures of the BSFI.

UBs/KBs shall create a separate risk management function that shall primarily assist management in meeting its responsibility to understand and manage risk exposures and ensure the development and consistent implementation of risk policies, processes, and procedures throughout the bank.

In case of group structures, there should be a board-approved policy that defines the risk management 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 risk management function centrally at the parent bank or in each of the identified subsidiaries. Such policy shall also include the overall responsibility of the parent bank's risk management function with respect to the management of risk exposures of subsidiaries/affiliates.

The establishment of risk management function centrally by the parent bank in group structures shall not fall under the outsourcing framework as provided under Sec. 112 (*Statement of Principle on outsourcing*). In this respect, the head of the risk management function of the parent bank shall define the 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 management of risk exposures.

Branches of foreign banks may establish their own risk management function or may be covered by the parent/regional/group risk management function: *Provided*, That all branches of foreign banks shall meet the applicable provisions set forth under this Section, and comply with the policies, practices, and systems of its head office related to the management of risks.

The board of directors of TBs, RBs, and Coop banks, may, at its own discretion, or as directed by the appropriate supervising department of the Bangko Sentral, create a risk management function, that shall report directly to the ROC or the board of directors, as applicable.

Chief Risk Officer (CRO). UBs/KBs shall appoint a CRO to head the risk management function. Other banks, may at their own discretion, or as directed by the appropriate supervising department, appoint a CRO, or any equivalent position to carry out the responsibilities of the position. The appointment, dismissal and other changes to the CRO or its equivalent position shall have prior approval of the board of directors. In cases, when the CRO will be replaced, the BSFI shall report the same to the appropriate supervising department of the Bangko Sentral within five (5) days from the time it has been approved by the board of directors.

The CRO shall have sufficient stature, authority, and seniority within the BSFI. He shall be independent from executive functions and business line responsibilities, operations and revenue-generating functions, and shall have access to such information as he deems necessary to form his judgment. The CRO shall have direct access to the board of directors and the ROC without any impediment. He shall serve on a full-time basis and shall functionally meet/report to the board of directors or board-level committee: *Provided*, That in cases of branches of foreign banks, the CRO shall report to the regional/group risk function. Meetings with the board of directors or board-level committee 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 CRO, and budget of the risk management function.

a. *Qualifications of the CRO.* The CRO should have the knowledge and skills necessary to oversee the BSFI's risk management activities. This will be assessed based on the ability of the CRO to influence decisions that affect the BSFI's exposure to risk. The CRO should have the ability to interpret and articulate risk in a clear and understandable manner and, without compromising his independence, can engage in a constructive dialogue with the board of directors, chief executive officer, and other senior management on key risk issues.

b. *Duties and responsibilities of the CRO.* The CRO shall be responsible for overseeing the risk management function and shall support the board of directors in the development of the risk

appetite and risk appetite statement of the BSFI and for translating the risk appetite into a risk limits structure. The CRO shall likewise propose enhancements to risk management policies, processes, and systems to ensure that the BSFI's risk management capabilities are sufficiently robust and effective to fully support strategic objectives and risk-taking activities.

(Circular Nos. 971 dated 22 August 2017)