146 OPERATIONAL RISK MANAGEMENT

Policy statement[1] It is the thrust of the Bangko Sentral to promote the adoption of effective risk management systems to sustain the safe and sound operations of banks. Cognizant that operational risk is inherent in all activities, products and services, and is closely tied in with other types of risks (e.g., credit, liquidity and market risks), the Bangko Sentral is issuing these guidelines to clearly set out its expectations and define the minimum prudential requirements on operational risk management. These guidelines align existing regulations to the extent possible, with international standards[2] and best practices. Bangko Sentral expects banks to adopt an operational risk management framework, as part of the enterprise-wide risk management system, that is suited to their size, complexity of operations, and risk profile.

Definition of operational risk. *Operational risk* refers to the risk of loss resulting from inadequate or failed internal processes, people and systems; or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Operational risk is inherent in all activities, products and services, and cuts across multiple activities and business lines within the bank and across the different entities in a banking group or conglomerate where the bank belongs.

Duties and responsibilities.

a. *Board of directors.* Consistent with the principles embodied under Sec. 132 (*Specific duties and responsibilities of the board of directors*), the duties and responsibilities of the board of directors in relation to the effective management of risk include the establishment of a comprehensive and effective operational risk management framework as part of the enterprise-wide risk management system. In this regard, the board of directors shall:

(1) Ensure that it is aware of and understands the nature and complexity of the major operational risks in the bank's business and operating environment, including risks arising from transactions or relationships with third parties, vendors, suppliers including outsourced service providers, and clients of services provided. This should include understanding of both the financial and non-financial impact of operational risk to which the bank is exposed to;

(2) Approve the operational risk management framework which shall form part of the bank's enterprise-wide risk management system and shall cover all business lines and functions of the bank, including outsourced services and services provided to external parties. The operational risk management framework should include an enterprise-wide definition of operational risk, which should be consistent with the definition under Sec. 146, governance, and reporting structures including the roles and responsibilities of all personnel, feedback mechanism, as well as standards and tools for operational risk management. In this respect,

the board shall:

(a) Define the operational risk management strategy and ensure that it is aligned with the bank's overall business objectives. Relative to this, the board should set and provide clear guidance on the bank's operational risk appetite (i.e., the level of operational risk the bank is willing to take and able to manage in pursuit of its business objectives as well as the type of risks that are not acceptable to the board and management), which should consider all material risk exposures as well as the bank's financial condition and strategic direction;

(b) Approve appropriate thresholds or limits to ensure that the level of operational risk is maintained within tolerance and at prudent levels and supported by adequate capital. Relative to this, the board shall approve policy on resolving limit breaches which should cover escalation procedures for approving or investigating breaches, approving authorities, and requirements in reporting to the appropriate level of management or the board;

(c) Ensure that operational risk is appropriately considered in the capital adequacy assessment process;

(d) Ensure that it receives adequate information on material developments in the operational risk profile of the bank, including pertinent information on the current and emerging operational risk exposures and vulnerabilities as well as information on the effectiveness of the operational risk management framework. The board must challenge the quality and comprehensiveness of the operational risk information it receives. It should also be satisfied with the reliability of the said information and the monitoring system for operational risk;

(e) Ensure that business objectives, risk appetite, the operational risk management framework, and the respective roles and responsibilities of personnel and officers at all levels in terms of implementing the operational risk management framework, are properly disseminated, clearly communicated/discussed, and understood by personnel concerned;

(f) Provide senior management with clear guidance and direction regarding the principles underlying the operational risk management framework. The board shall ensure that senior management appropriately implements policies, processes and procedures, and provides feedback on the operational risk management process. In this regard, the board shall establish a feedback and reporting system that will allow employees to raise their

concerns without fear of negative consequences; and

(g) Ensure that the operational risk management framework is subject to effective and comprehensive independent review, on a periodic basis, by operationally independent, appropriately trained, and competent staff to ensure that it remains commensurate with the bank's risk profile and continues to be adequate and effective in managing operational risk. The review should take into account the changes in business and operating environment, material changes in systems, business activity or volume of transactions, quality of control environment, effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of breaches in limits or any policy.

(3) Provide adequate oversight on all outsourcing activities and ensure effective management of risks arising from these activities. In this regard, the board of directors shall approve a framework governing outsourcing activities, which includes a system to evaluate the risk and materiality of all existing and prospective outsourcing engagements and the policies that apply to such arrangements;

(4) Ensure observance of expectations and requirements prescribed under relevant laws, rules and regulations, industry-set standards, and policies on internal control, internal audit, and disclosure;

(5) Promote a culture of high standards of ethical behavior. The board shall adopt a code of conduct of ethical behaviors with corresponding disciplinary actions for non- compliance, which should cover, among others, guidance and protocols on conflicts of interest situations, safeguarding of confidential information, and use of sensitive information. The board should likewise institute tools, methodologies, and practices in order to ensure compliance and adherence to the standards by all employees including the senior officers and the board itself. In this regard, employees should be required to acknowledge in writing that they have read, understood, and will observe the code of conduct;

(6) Ensure that business and risk management activities, including the operational risk management function, are carried out by adequate and qualified staff with the necessary experience, technical capabilities, and competence. Moreover, the board shall ensure that employees and officers in all areas of operations have a high degree of integrity.

For this purpose, the board shall approve appropriate hiring and selection policies and processes, adopt a continuing professional development program, and institutionalize a framework for continuing assessment of fitness and propriety of employees. These policies,

processes and programs should reinforce the conduct and values being promoted in the organization.

Further, the board shall oversee the design and implementation of remuneration policies. It shall ensure that the remuneration policies do not encourage excessive risk-taking or provide incentives to people to perform contrary to the desired risk management values. It shall also ensure that remuneration policies are appropriate and aligned with the bank's long-term strategic direction and risk appetite, as well as with relevant legal or regulatory requirements;

(7) Ensure that all units in the organization have adequate resources, including personnel complement, and are supported by appropriate technological systems. The use of technological systems must be commensurate with the activities being undertaken; and

(8) Oversee implementation of a sound business continuity management framework. The board should create and promote an organizational culture that places high priority on business continuity. This shall include providing sufficient financial and human resources associated with the bank's business continuity initiatives.

b. *Senior management.* Senior management shall be responsible for the implementation and consistent adherence by all personnel to the operational risk management framework approved by the board of directors. In this respect, senior management shall:

(1) Translate the approved operational risk management framework into specific policies and processes covering all businesses and functions of the bank, including outsourced services and services provided to external parties. Said policies should be clearly documented, approved by the board of directors and communicated to personnel at all levels. Policies should include, among others:

(a) Definition of operational risk and operational risk loss. This should be supported by common operational risk taxonomy that includes the operational risk event type and causes losses to facilitate the consistent identification of operational risks across the bank as well as the management of operational risk in an integrated manner;

(b) Appropriate governance and oversight structures, reporting lines, and accountabilities for managing operational risks;

(c) Clear description of risk limits and thresholds that correspond to the bank's approved operational risk appetite and tolerance;

(d) Risk mitigation strategies and tools for maintaining risks within the thresholds and limits set;

(e) Approach to operational risk identification, assessment, monitoring and reporting that utilizes appropriate operational risk management tools. This should include an outline of the reporting framework and types of data/information to be included in the risk management reports; and

(f) Requirement for the conduct of independent review of the framework as well as its implementation, on a periodic basis, and whenever there are material changes in the bank's operational risk profile.

(2) Communicate individual roles and responsibilities of personnel. It is important that personnel at all levels understand their respective roles in the operational risk management process. In this regard, senior management should clearly assign authority, responsibility, and reporting relationships to encourage and maintain accountability, and ensure that the necessary resources are available to manage operational risk effectively;

(3) Establish system to report, track, escalate, and resolve issues; and set the frequency of operational risk management reporting considering the level and type of risks involved as well as the pace and nature of the operating environment of the bank;

(4) Assess the appropriateness of the operational risk management process in light of the changing business environment and nature of risks arising from business activities or functions;

(5) Ensure that sufficient number of personnel, technical support, and other resources are devoted for operational risk management such that the bank's activities are conducted by qualified personnel with the necessary experience and technical capabilities. It shall also ensure that personnel responsible for monitoring and enforcing compliance with the bank's operational risk policy as well as the compliance and internal audit units have authority independent from the units they review and are knowledgeable about the different areas of operations; and

(6) Establish policies, standards and processes for an effective business continuity management.

c. *Business units.* Business line management and personnel, as the first line of defense, are responsible on a day-to-day basis for identifying, managing and reporting operational risks inherent in the products, activities, processes and systems for which they are accountable. In

this regard, business line management shall ensure that:

(1) Internal controls and practices within their business lines are consistent with the enterprise-wide policies and procedures to support the management of operational risk;

(2) Business line specific policies, processes, and procedures are adequate and effectively implemented, and personnel are adequate and competent to manage operational risk for all material products, activities, and processes;

(3) Operational risk management framework within each business line reflects the scope of that business line and its inherent operational complexity and operational risk profile;

(4) Risk mitigation strategies and processes as approved by the board and senior management are established and executed;

(5) Internal controls, and operational risk mitigation strategies and processes are periodically reviewed within the business units to effectively manage operational risks within approved risk tolerance, and consistent with enterprise-wide policies and procedures established. There must be clear expectations and processes established to ensure prompt escalation and actions to address any gap or issue identified; and

(6) Operational risk-related information (e.g., loss events, incidents, et al.) are adequately and timely communicated/coordinated to Operational Risk Management Function (ORMF) for risk monitoring and reporting, in addition to the usual reporting to senior management and/or board.

Roles and functions.

a. *Operational risk management function*. UBs/KBs shall create a separate ORMF or assign specific personnel under the risk management unit to handle operational risk concerns. The ORMF shall primarily assist management in meeting its responsibility to understand and manage operational risk exposures and ensure the development and consistent implementation of operational risk policies, processes, and procedures throughout the bank. In this regard, the ORMF shall:

(1) Recommend to the board of directors and senior management appropriate policies and procedures relating to operational risk management and controls;
(2) Design and implement the bank’s operational risk assessment methodology tools and risk reporting system;
(3) Coordinate risk management activities across the organization;

(4) Consolidate all relevant operational risk information/reports to be elevated/presented to the board and senior management;
(5) Provide operational risk management training and advice to business units on operational risk management issues; and
(6) Coordinate with compliance function, internal audit, and external audit on operational risk matters.

ORMF personnel should have technical proficiency, appropriate educational background, and exposure to enable them to effectively perform the unit's mandate. Banks shall have in place a training program to keep its personnel up-to-date on different operational risk issues and challenges.

The ORMF shall be supported by a board-approved charter that defines its stature, authority, and independence. It shall directly report to the head of the Risk Management Unit (RMU) or to the board-level Risk Oversight Committee (ROC), as appropriate. The head of the RMU or the ROC, as appropriate, shall be responsible for assessing the annual performance of said function taking into account how it carried out its duties and responsibilities.

In case of group structures, there should be a board-approved policy that defines the operational 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 ORMF 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 ORMF with respect to the management of operational risk exposures of subsidiaries/affiliates.

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

TBs, RBs and Coop Banks are not required to create an ORMF. However, the board of directors is expected to discuss operational risk issues during its board meetings with discussions adequately documented in the minutes of meetings. The board of directors of complex [3] TBs, RBs, Coop Banks may, at its own discretion, or as directed by the appropriate supervising department of the Bangko Sentral, create an RMU and assign specific personnel under said unit to handle operational risk concerns. The said RMU shall directly report to the ROC or the board, as applicable. The ROC or the board shall be responsible for assessing the annual performance of the unit taking into account how said unit carried out its duties and responsibilities.

b. *Compliance function.* The compliance function shall conduct an independent assessment of the bank's compliance with relevant laws, rules and regulations, as well as internal policies, and determine areas that may potentially result in risk of loss due to inadequate or failed internal processes, systems, and people. The latter includes inappropriate conduct/behavior of personnel, officers, and the board, that may lead to fraud or any form of business disruption. The compliance function shall assess whether the identified operational risk exposure by the business units or by the function itself shall affect the franchise value of the bank. In this regard, it shall advise and assist management in establishing guidance on the appropriate implementation of relevant laws, rules and regulations, and internal policies.

c. *Internal audit.* Internal audit shall conduct an independent assessment of the operational risk management framework, including the implementation of operational risk management policies and procedures. The board of directors, either directly or indirectly through the board-level Audit Committee shall ensure that the scope and frequency of audit is appropriate to the risk exposures. Any operational risk issue identified and reported in the audit process should be addressed by senior management in a timely and effective manner, or raised to the attention of the board as appropriate.

Operational risk management framework. Banks shall have in place an appropriate operational risk management framework, as part of the enterprise-wide risk management system, that is effective and efficient in identifying, assessing, monitoring and controlling/mitigating operational risk. They shall ensure that their operational risk management framework is commensurate with the complexity of their operations, range of products and services, organizational structure, and risk profile.

a. *Risk identification and assessment.* Risk identification and assessment are fundamental elements of an effective operational risk management system. Effective risk identification shall consider both internal factors (such as bank structure, nature of activities, the quality of human resources, organizational changes and employee turnover, among others) and external factors (such as changes in the broader environment and the industry, advances in technology, and developments in political, legal, and economic factors, among others). Risk identification and assessment allow the bank to better understand its risk profile and allocate risk management resources and strategies more effectively. Since the business lines are expected to have the best knowledge of their risk exposures and processes, these units should play a major role in the identification and assessment of operational risk.

(1) Banks shall consider the following loss event-type categories as part of their risk identification and assessment processes:

(a) Internal fraud, e.g., intentional misreporting of positions, employee theft, and insider

trading on an employee's own account;

(b) External fraud, e.g., robbery, forgery, check kiting, and damage from computer hacking;

(c) Employment practices and workplace safety, e.g., workers compensation claims, violation of health and safety rules, organized labor activities, discrimination claims, and general liability;

(d) Clients, products and business practices, e.g., fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products;

(e) Damage to physical assets, e.g., terrorism, vandalism, earthquakes, fires and floods;

(f) Business disruption and system failures, e.g., hardware and software failures, telecommunication problems, and utility outages; and

(g) Execution, delivery, and process management, e.g., data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

(2) Banks shall adopt tools and mechanisms that are appropriate to their size, complexity of operations and risk profile to properly identify and assess operational risk. The tools that may be used for identifying and assessing operational risk may include, but not limited to:

(a) *Results of internal/external audit and supervisory issues raised in the Bangko Sentral Report of Examination (ROE)* – Internal audit surfaces issues on effectiveness of internal control, risk management, and governance systems and processes of an organization, while external audit focuses on control weaknesses and susceptibility of the bank to material misstatements in the financial statements. On the other hand, the Bangko Sentral ROE highlights deficiencies in the risk management systems and governance processes as well as issues on compliance with relevant laws, rules and regulations, which could have adverse effects on the safety and soundness of the bank;

(b) *Internal loss data collection and analysis* – Internal operational loss data provides meaningful information for assessing bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insights into the causes of large losses and information on whether control failures are isolated or pervasive. Banks may consider mapping internal loss data to the following business lines:

(i) Corporate finance;
(ii) Trading and sales;
(iii) Retail banking;
(iv) Commercial banking;
(v) Payment and settlement;
(vi) Agency services;
(vii) Asset management; and
(viii) Retail brokerage.

Loss events linked to credit and market risk may also relate to operational issues and should be segmented in order to obtain a more comprehensive view of the bank's operational risk exposure;

(c) *Risk Self Assessments (RSA)/Risk Control Self Assessments (RCSA)* – RSA is a tool to assess processes underlying bank's operations against a library of potential threats and vulnerabilities including their potential impact. A similar approach, RCSA, typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). Scorecards on RCSAs may be developed by allocating weights to residual risks to provide a means of translating the RCSA output into metrics that will give a relative ranking of the control environment;

(d) *Business process mappings* – These help identify key steps in business processes, activities, and organizational functions as well as the key risk points in the bank's overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They can also help prioritize subsequent management action;

(e) *Risk and performance indicators* – Risk and performance indicators, such as Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), provide an insight into a bank's emerging risk exposure. KRIs are used to monitor the main drivers of exposure associated with key risks that contribute to early detection of heightened risk, ongoing monitoring of their movements, and preemptive reactions as necessary. KPIs, on the other hand, provide insight into the status of operational processes, which may in turn provide insights into operational weaknesses, failures, and potential loss. Risk and performance indicators are often used with escalation triggers to warn when risk levels approach or exceed acceptable ranges and prompt mitigation plans;

(f) *Scenario analysis* – This refers to the process of obtaining expert opinion of business line

and risk managers to identify potential operational risk events and assess the potential outcome. Scenario analysis is an effective tool when considering potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process;

(g) *Model measurement* – Larger banks may deem it useful to quantify their operational risk exposures by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

(h) *Comparative analysis* – Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile.

Comparison of external loss data, if available, such as industry experiences, vis-à-vis bank's internal loss data can also be made to explore possible weaknesses in the financial institution's control environment and enable it to consider previously unidentified risk exposures.

In choosing among these tools, each bank must carefully consider what is proportionate to its size, risk profile, and complexity of operations. Data/information gathered from these tools should enable banks to make a thorough causal analysis, identify control gaps, and consequently adopt appropriate corrective actions.

UBs/KBs are expected to adopt more sophisticated tools in identifying and assessing their operational risk exposures. TBs, RBs and Coop Banks, on the other hand, are expected to adopt at the minimum, the (i) results of internal/external audit and supervisory issues raised in the Bangko Sentral ROE and (ii) internal loss data collection and analysis.

(3) Banks shall develop databases to accumulate at least a five (5)-year history of operational risk losses which can be fed back into the operational risk management process. Apart from capturing events that resulted to actual loss, banks shall also gather potential loss or near-misses[4]. Said database of loss events provides basis for analysis which can help direct corrective action to improve the control environment, as well as determine risk mitigating actions. Banks should assess the depth of its data collection which is vital in understanding the risk environment. The loss event database shall at a minimum disclose the following:

(a) Short description of the event;
(b) Loss event type category;
(c) Department/Unit/Branch sustaining the loss;
(d) Business line classification;
(e) Date of occurrence;
(f) Date of discovery;
(g) Date of booking of actual losses;
(h) Actual loss amount or potential loss amount, if a near-miss event;
(i) Amount recovered and date of recovery;
(j) Causes of the event (e.g., control weaknesses identified);
(k) Consequence of the loss event (e.g., market loss, fees paid to a counterparty, a lawsuit or damage to the bank's reputation); and
(l) Action(s) taken.

Banks shall define appropriate thresholds for internal loss data collection and must be able to justify the same. Thresholds should be reasonable and should not omit any operational loss event data that is material for operational risk exposure and for effective risk management. Banks shall ensure that the choice of threshold should not adversely impact the credibility and accuracy of operational risk measurement.

(4) Banks shall determine based on the results of the risk assessment process whether the risks are within the scope of its operational risk management strategy and policies. It shall identify the risk exposures that are unacceptable or are outside its risk appetite and/or risk management capacity, and design and prioritize appropriate risk mitigation and corrective actions with clear accountabilities, roles and responsibilities for implementation within reasonable timelines.

(5) Banks shall continually assess its operational risk exposures in order to gain broader recognition and understanding of their effects. It shall consider the following factors in the assessment:

(a) Expected and unexpected changes to the bank's operating environment;
(b) Actual operational loss events that could have resulted in substantial losses/damage but were avoided (e.g., near misses) or recovered;
(c) Reported external operational losses and incidents which have damaged investor confidence and caused serious reputational harm;
(d) Areas of concern or unusual volumes or high number of exceptions; and
(e) Results of internal assessment of risks and controls.

(6) Banks shall ensure that their risk management and control infrastructure keep pace with the

growth of or changes in their business activities, i.e., when they engage in any new activity; introduce a new product; enter new or unfamiliar markets; implement new business processes or technology systems; establish subsidiaries/branches that are geographically remote from the head office; and/or embark on an aggressive growth strategy by acquiring problem banks to rapidly increase branch network during a short period of time. Banks should have relevant policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process shall consider the following:

(a) Inherent risks in the new product, service, or activity;
(b) Changes to the bank's operational risk profile, appetite and tolerance, including the impact on existing products or activities;
(c) Necessary controls, risk management processes, and risk mitigation strategies;
(d) Any residual risk; and
(e) Procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

b. *Risk monitoring and reporting.* Banks shall implement a process to regularly monitor their operational risk profiles and material exposures to losses on a continuing basis. The process shall take into account both qualitative and quantitative assessment of exposure to all types of operational risk, assess the quality and appropriateness of corrective or mitigating actions, and ensure that adequate controls and systems are in place to identify and address problems before they become major concerns.

(1) Risk monitoring should be an integral part of a bank's activities, the frequency of which should reflect the risks involved in these activities as well as the frequency and nature of changes in the operating environment. The results of the monitoring activities, findings of compliance, internal audit and risk management functions, management letters issued by external auditors, and reports generated by supervisory authorities, as appropriate, should be included in regular reports to the board and the senior management to ensure that timely and appropriate measures are undertaken to address the issues/findings.

(2) Management shall ensure that regular reports on operational risk are received on a timely basis and in a form and format that will aid in the monitoring and control of their business areas. The board should receive sufficient high-level information to enable it to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business.

(3) Management reports should contain relevant internal financial, operational, and compliance

data, as well as external market information about events and conditions that are relevant to decision making. They should aim to provide information such as:

(a) The critical operational risks facing, or potentially facing, the bank (e.g., as shown in KRIs and their trend data, changes in risk and control self-assessments, comments in audit/compliance review reports, etc.);
(b) Major risk events/loss experience, issues identified and intended remedial actions;
(c) The status and/or effectiveness of actions taken; and
(d) Exception reporting (covering among others authorized and unauthorized deviations from the bank's operational risk policy and likely or actual breaches in predefined thresholds for operational exposures and losses).

(4) Reports should be analyzed with a view to improving existing management performance as well as developing new risk management policies, procedures and practices. Moreover, to ensure the usefulness and reliability of the reports received, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general.

(5) Management should keep track of the information provided in the reports, particularly the loss data, to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on loss events.

c. *Risk control and mitigation.* Strong control environment is key to effective risk control and mitigation. In this respect, banks are expected to adhere to the standards set forth under Secs. 162, 163, and 436 (*Internal audit*) and *Appendix 117* on Internal Control and Internal Audit.

Banks shall decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the significant risks that have been identified. In those instances where internal controls do not adequately address risk and accepting the risk is not a reasonable option, banks may seek to transfer the risk to another party such as through insurance. Relative thereto, the board shall determine the maximum loss exposure the bank is willing to take and has the capacity to assume, and should perform an annual review of the bank's risk and insurance management program.

Banks, however, should not consider risk transfer tools as substitute but as complementary tools to sound controls and risk management system. Management shall also assess the extent to which risk mitigation tools such as insurance reduces risk, transfer the risk to another business sector or area, or create a new risk (e.g., counterparty risk).

Management of human resource-related risk. One of the major sources of operational risk is "people risk". In this regard, banks shall embed in their enterprise-wide risk management framework measures to identify, measure, monitor, and control human resource related risks. Banks shall ensure that there are adequate policies and risk management and control measures in the following areas:

a. *Recruitment and selection.* The board shall establish efficient process that will facilitate timely recruitment and selection of personnel from a broad pool of candidates with appropriate educational background, skills, experience and competencies to fulfill the duties and responsibilities of the function. Management shall also ensure that the bank's culture, values and expectations on behavior are compatible with those of its employees so that there is unity of direction and purpose.

b. *Performance management.* The board shall establish effective performance management framework that will ensure that personnel's performance is at par with the standards set by the board/senior management. Results of performance evaluation should be linked to other human resource activities such as training and development, remuneration, and succession planning. These should likewise form part of the assessment of the continuing fitness and propriety of personnel in carrying out their respective duties and responsibilities.

The assessment of continuing fitness and propriety of personnel should take into account factors that may affect the performance of an individual. For instance, the financial circumstances of an employee who will be responsible for the custody of, or handling of cash related transactions, shall be taken into consideration in the evaluation of his continuing qualification.

c. *Training and development.* The board shall establish training and development programs that will ensure continuing development of employees' knowledge, competence, and skill. Results of gaps assessment in the performance evaluation/appraisal process can be used in the creation of training and development programs for employees.

d. *Remuneration and compensation.* The board shall establish sound remuneration and compensation policies that can be used by the institution to attract/recruit and retain highly qualified workforce. Said policies should appropriately motivate personnel and discourage excessive risk taking. This can be achieved through timely assessment of performance and competencies based on set standards. Results of performance assessment/appraisal can be used in the organization's remuneration decisions.

e. *Succession planning.* The board shall establish an effective succession planning program. The program should include a system for identifying and developing potential successors for key and

or critical positions in an organization, through systematic evaluation process and training. This will require identifying critical skills and competencies; assessing gaps; and designing, developing, and delivering training and development programs to build or improve critical skills and competencies. The program should be adequately documented to facilitate monitoring and assessment of its implementation.

f. *Adequacy of complement.* The board shall establish effective strategic manpower planning to ensure that there is adequate and right manpower complement to meet the strategic goals and operational plans of the organization.

g. *Disciplinary actions.* The board, officers and all employees are expected to conform to prescribed ethical culture and guidelines, meet performance standards, and to behave ethically/appropriately in the workplace. Disciplinary or corrective actions may be taken to improve/arrest unacceptable behavior or performance. Disciplinary action must be in accordance with the laws and the applicable rules.

h. *Separation from service.* The board shall establish policies and procedures governing the separation of employees from service (e.g., termination, dismissal, retrenchment, retirement, or resignation), which should include transfer of accountabilities and/or salient information (e.g., client data, business strategies and formula, other trade secrets, etc.) to the successor, and clearance requirements. Policies may also include "non-compete" clauses, in accordance with existing laws.

The Human Resource Department shall assist the board in fulfilling its oversight responsibilities in the areas of recruitment, manpower planning, personnel development, performance appraisal, remuneration, termination, retrenchment and other key human resource issues.

Management of information technology-related risk. Banks shall refer to Sec. 148 for the management of information technology-related risk.

Management of integrity of prudential reports or reports submitted to Bangko Sentral. Banks shall adopt a prudential reporting framework that ensures the integrity of information submitted to the Bangko Sentral. They shall establish a system for ensuring effective compliance with the standards prescribed by the Bangko Sentral on acceptable reporting quality. Banks shall likewise maintain adequate documentation of the processes and procedures covering the prudential reporting framework and conduct a periodic review of their continuing relevance.

Management should be cognizant of relevant guidelines that may be issued by the Bangko Sentral

relative to issues on the integrity and accuracy of prudential reports. Persistent concerns on the integrity and accuracy of prudential reports including failure to comply with the directives of the Bangko Sentral in this respect may be considered by the Bangko Sentral as conducting business in an unsafe or unsound manner, subject to applicable provision of laws and regulations.

Management of legal risk exposures. Banks shall adopt a system for identifying and assessing legal risks related to business line functions as well as products and services offered. This shall include a process for assessing the bank's rights and obligations in contractual relationships and in ensuring that all agreements/contracts entered into by the bank conform to legal and regulatory requirements and that no party is unduly disadvantaged. This shall also include the assessment of trends of customer complaints to determine potential legal risk exposures.

There should be a system in place to manage outstanding legal cases involving the bank or any of its directors and officers, with respect to suits filed in line with the performance of their duties. Said system should cover a periodic review of the status of cases, an assessment of potential outcome including probable liability or receivable, and regular reporting of the same to the appropriate level of management and the board.

Management of operational risk arising from financial inclusion initiatives. Banks that provide financial services to the unserved and underserved sector generally handle small and voluminous transactions, which have inherently high operational risk. Incremental operational risk also comes from the higher number of personnel or from the use of technology-based platform to effectively and efficiently deliver financial services. Banks are expected to identify and understand the distinct operational risk arising from the products and services they offer or innovative delivery channels they use. They should also be cognizant of potential transformation or transfer or risk exposures. In this regard, banks shall adopt an operational risk management framework appropriate to the nature and scale of their operations. Said framework shall consider the principles embodied in this Section designed to suit the bank's business model and ensure sustained delivery of financial services to the unserved and underserved sector.

Notification/Reporting to Bangko Sentral. Banks shall notify the appropriate supervising department of the Bangko Sentral, within ten (10) calendar days from the date of discovery, of any operational risk event [5] that may result in any of the following:

a. Significant operational losses or exposures;
b. Activation of business continuity plan; or
c. Any material change in business and operating environment.

Upon receipt of notification, the Bangko Sentral may require, if warranted, the reporting bank to

submit a report detailing the causes and impact of such events and an acceptable action plan to address the issue and any other weakness identified.

Supervisory enforcement actions. Consistent with Sec. 002, the Bangko Sentral may deploy enforcement actions to promote adherence with the requirements set forth in this Section and bring about timely corrective actions. The Bangko Sentral may issue directives to improve the operational risk management system, or impose sanctions to limit the level of or suspend any business activity that has adverse effects on the safety or soundness of the bank, among others. Sanctions may likewise be imposed on a bank and/or its directors, officers and/or employees.

(Circular Nos. 969 dated 22 August 2017, 930 dated 18 November 2016, and 900 dated 18 January 2016)

Footnotes

1. .Banks shall comply with the foregoing standards on operational risk management within a period of two (2) years from 05 February 2016. In this regard, a bank should be able to show its plan of actions with specific timelines, as well as the status of initiatives being undertaken to fully comply with the provisions of Sec. 146.
2. Embodied in the relevant documents issued by the Basel Committee on Banking Supervision.
3. Sec. 131 (*Policy statement and Definition of terms*) provides the grounds for classifying banks as 'Complex' for regulatory purposes.
4. Potential loss is an initial estimate of the loss that the bank may have sustained at the time of discovery of the event. Near miss is an adverse operational risk event which was not prevented by internal controls but did not result in an actual adverse impact (financial or reputational) due to chance, recovery or other external factors.
5. As enumerated under Sec. 146 (*Operational risk management framework*, loss event-type categories).