BANKING SUPERVISION AND REGULATION DIVISION

GUIDELINES TO BANKS ON THE MANAGEMENT OF OPERATIONAL RISK

MARCH, 2008
1. **INTRODUCTION**

The liberalization of markets and globalization of the financial services together with the growing sophistication of financial technology render the bank activities more complex and create new risks which impact the banks’ risk profile. Indicative sources of the new growing risks include the introduction of highly automated technology, the greater reliance on globally integrated systems, the growth of electronic commerce, the large-scale acquisitions, mergers and consolidations, the engagement in risk mitigation techniques and the growing use of outsourcing arrangements.

The diverse list of such risks is grouped under the heading of “operational risk”. The Basel Committee on the Banking Supervision has defined operational risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”. The definition includes legal risk but excludes strategic and reputational risk.

Banks must have a clear understanding of what is meant by “operational risk”. Their interpretation of the term should consider the full range of material operational risks and capture the most significant causes of severe operational losses. The inadequate recognition and management of the operational risk may result to the underestimating of the bank’s risk profile, thus, exposing the bank to significant losses which may threaten its safety and soundness.

The importance of operational risk, as a distinct significant risk category, is recognized in the new capital requirements framework (Basel II) which, inter alia, introduces Pillar 1 capital requirements for operational risk. The relevant European Union Directive on capital requirements, the provisions of which have been transposed in the Central Bank of Cyprus Directive on the Calculation of the Capital Requirements and Large Exposures, adopts the definition of the operational risk and the loss event type classification defined by the Basel Committee on the Banking Supervision (refer to Unit A’ paragraphs 46 to 49 and annex X of abovementioned directive of the Central Bank of Cyprus).
The Central Bank of Cyprus requires supervised banks to recognize the existence and significance of operational risk in relation to their safety and viability and to develop an appropriate framework for the management of the operational risk inherent in all their activities. As regards branches in Cyprus of banks incorporated outside the Republic of Cyprus, the Central Bank of Cyprus expects that these will apply comparable operational risk management principles in the context of implementing the operational risk management framework of their banks.

These guidelines are issued for defining the basic principles that should govern the banks’ operational risk management framework and to stress the importance that the Central Bank of Cyprus places on the effective management of operational risk, as a distinct significant risk category.

2. **BASIC PRINCIPLES FOR THE MANAGEMENT OF OPERATIONAL RISK**

**Development of an appropriate operational risk management environment**

The Board of Directors and the Senior Management of banks are responsible for creating an appropriate organizational culture that emphasizes high standards of ethical behaviour at all bank levels and places high priority on effective operational risk management and adherence to sound operating controls.

**Responsibilities of the Board of Directors.**

The Board of Directors should be aware of the major aspects of the bank’s operational risks as a distinct risk category to be managed for the safety and soundness of the bank. The Board of Directors should approve and periodically review the operational risk management framework of the bank and provide to the Senior Management clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by the Senior Management.
The operational risk management framework should provide an explicit firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored and controlled/mitigated. It should also cover the bank’s risk appetite and the tolerance of operational risk as well as the extent of, and the manner in which, operational risk is transferred outside the bank. The degree of formality and the sophistication of the framework should be commensurate with the bank’s risk profile. The Board of Directors is responsible for establishing an appropriate management structure, including the establishment of an independent operational risk management function, capable of implementing effectively the bank’s operational risk management framework.

The Board of Directors should also ensure that the bank’s operational risk management framework is subject to an effective and comprehensive internal audit by operationally independent unit which has appropriately trained and competent staff. The internal audit function should be independent of the unit responsible for operational risk management.

Responsibilities of the Senior (Executive) Management.

The Senior Management of the bank is responsible for implementing the operational risk management framework approved by the Board of Directors and ensuring that the framework is consistently implemented throughout the whole banking organization, including the subsidiaries whose business is not integral or closely related to banking business (e.g. insurance companies). In this context the Senior Management should develop and document precise policies, processes and procedures for managing operational risk in all of the bank’s material products, activities, processes and systems and ensure that the necessary resources are available to manage operational risk effectively.

The Senior Management should also define clearly the lines of authority, responsibility, reporting and accountability and ensure that the necessary resources are available to manage the operational risk effectively. It should also ensure that the bank’s operational risk management policy is clearly communicated to staff at all levels in units that incur operational risk and that the
staff fully understand their responsibilities in relation to the management of the operational risk. The exposure to operational risk as well as operational risk losses should be subject to regular reporting and there should be written procedures for the taking of appropriate measures, where this is warranted from the contents of such reports.

**Risk management: Identification, assessment, monitoring and mitigation / control.**

**Identification and assessment.**

Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. They should also ensure that before new products, activities, processes and systems are introduced or undertaken the operational risk inherent in them is subject to adequate assessment procedures.

Risk identification is paramount for the development of a viable operational risk monitoring and control system. The effective risk identification considers both internal and external factors with a potentially adverse effect. In addition to identifying the potentially adverse risks banks should assess their vulnerability to these risks. This assessment should target at a better understanding of the bank's risk profile and the effective use of the risk management resources.

The Central Bank of Cyprus requires supervised banks to employ appropriate tools for identifying and assessing their operational risk. The specific tools to be employed are decided separately by each bank having regard to the nature, scale and complexity of its activities. Possible tools are the “self or risk assessment”, the “risk mapping”, the “risk indicators” and the “risk measurement”. The general characteristics of the above tools are described in paragraph 25 of the paper on “Sound Practices for the Management and Supervision of the Operational Risk” issued by the Basel Committee on Banking Supervision in February 2003.

In the context of identifying and assessing operational risk, the Central Bank of Cyprus also expects banks to maintain historical internal and external loss data.
For the banks applying the Standardized approach or the Advanced Measurement Approach for calculating capital requirements, in particular, the historical loss data should be in line with the “business lines” and “loss event type classification” provided for in Parts 2 and 4 respectively of annex X of Unit A’ of the Central Bank of Cyprus directive on the Calculation of the Capital requirements and Large Exposures. For this purpose, banks should establish a system for tracking and recording the frequency, severity and other relevant information on individual loss events, including the date of the event, a description of the drivers and causes of the loss event as well as any recoveries against the loss incurred.

**Monitoring**

Banks should implement a process to regularly monitor their operational risk profile and material exposures to losses. There should also be a regular reporting of pertinent information to the Senior Management and the Board of Directors for proactive management of operational risk.

The Central Bank of Cyprus requires banks to implement effective processes of regular monitoring of operational risk to enable prompt detecting and correcting of any deficiencies in the policies, processes and procedures for managing operational risk, so that the possibility, frequency and severity of a loss event are substantially reduced.

In addition to monitoring operational loss events, bank should identify appropriate indicators that provide early warnings of an increased risk of future losses. Such indicators may be in relation to rapid activities’ growth, introduction of new products, employee turnover, system downtime etc. When thresholds are directly linked to these indicators, an effective monitoring process can help to identify key material risks and enable the bank to act upon these risks appropriately.

The monitoring of operational risk should be an integrated part of the day to day monitoring and risk management of the bank. The frequency of monitoring should reflect the risks involved and the frequency and nature of the changes in the
operating environment of the bank. The results of the monitoring should be included in regular reports to the bank’s Board of Directors, the Senior Management and relevant departments of the bank.

The Senior Management should receive regular operational risk reports from all appropriate units and functions of the bank, containing information about events and conditions that are relevant to decision making. The reports should identify problem areas and motivate timely corrective action. The Senior Management should ensure the timeliness, accuracy and relevance of the reporting systems and internal controls in general. To assess the usefulness and reliability of the internal reports, the Senior Management may also make use of reports prepared by external sources, such as external auditors and competent supervisory authorities.

The Board of Directors should receive higher level information to enable them to understand the bank’s overall operational risk profile and focus on material and strategic implications for the bank’s business.

Control / Mitigation

Banks should have policies, processes and procedures to control and/or mitigate material operational risks. They should also periodically review their risk mitigation and control strategies and adjust their operational risk profile accordingly using appropriate strategies in the light of their overall risk appetite and profile.

For all material risks that have been identified, banks should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be effectively controlled / mitigated, banks should decide whether to accept the risks, reduce the level of business activity involved, or withdraw from that activity completely. In case that a bank decides to retain or self-insure significant operational risks, the decision should be transparent within the organization and consistent with the bank’s overall business strategy and risk appetite.
Banks should establish and document in writing policies, processes and procedures for controlling/mitigating significant operational risks. They should also have in place a system for ensuring compliance with the abovementioned policies, processes and procedures and, in general, the operational risk management system. Such a system should, indicatively, include (a) a top-level review of the bank’s progress towards the stated objectives, (b) checking of compliance with management controls, (c) the policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues, and (d) a system of documented approval and authorizations to ensure accountability to an appropriate level of management.

**Insurance / transfer of operational risk to third parties**

By their nature some significant operational risk events have a low probability but potentially very large financial impact. Moreover, certain risk events, with significant potential operational loss, may not be effectively controlled by banks. In such instances banks may use mitigation tools for reducing their operational risk, such as transferring the risk to third countries through insurance policies or outsourcing of activities. Mitigation mechanisms, however, should be used as complementary to, rather than a replacement for thorough internal operational risk control.

When an insurance policy is used as a mitigation tool for mitigating / controlling operational risk, careful consideration should be given to the policy terms and extent of the cover to ensure that the insurance truly reduces the risk and does not create new risks. In this connection, it is required that the insurance policy is provided by a third party and not by an entity belonging to the same group of companies that the bank itself belongs.

The outsourcing of activities to third parties with greater expertise and scale to manage risks associated with specialized business activities may constitute an effective tool of transferring operational risk to and reducing the banks’ risk
profile. Banks should establish and document in writing their policies for managing the risks associated with outsourcing activities.

It is emphasized that the outsourcing of activities to third parties does not diminish the responsibility of the bank to ensure that the relevant activity is conducted in a safe and sound manner and in compliance with applicable laws. Consequently, the outsourcing arrangements should be based on robust contracts and service level agreements that ensure a clear allocation of responsibilities between the outsourcing bank and the external service provider. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services.

Banks should understand the potential impact on their operations and their customers of any potential deficiencies in the services provided on their account by third parties. In this connection, banks should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. Banks should also explicitly consider the liability and financial ability of the external service provider to compensate the bank, if required, for errors, negligence and other operational failures. Finally, for critical outsourced activities, banks should have contingency plans for immediate alternative solutions in case of the external service provider’s failure.

Internal control environment

The Board of Directors and the Senior Management of each supervised bank are responsible for establishing a strong internal control culture, in which control activities form an integral part of the regular activities of the bank, promoting sound risk management practices and ensuring quick responses to changing conditions and avoidance of unnecessary costs.

The internal control system should ensure appropriate segregation of duties preventing the conflict of interest that would enable concealment of losses, errors or inappropriate actions. It should also require the implementation of internal practices to control operational risk, such as, (a) close monitoring of adherence to
assigned risk limits or thresholds, (b) maintaining safeguards for access to, and use of, bank assets and records, (c) ensuring that staff have appropriate expertise and training, (d) identifying lines or products where returns appear to be out of line with reasonable expectations and (e) regular verification and reconciliation of transactions and accounts.

In addition to the above, the internal control activities should pay special attention to the operational risk in relation to the engagement in new activities, development of new products, penetration into unfamiliar markets and undertaking of businesses that are geographically distant from the bank’s head office.

The internal audit function should be independent of the unit responsible for operational risk management. The internal audit function may have initial responsibility for developing an operational risk management programme and, subsequently, provide valuable input to those responsible for the operational risk management, but it should not be directly responsible for operational risk management. The frequency and scope of the internal audit function should be commensurate with the bank’s exposure to operational risk. The internal audit should ensure that the operational risk management framework as well as the operating policies and procedures are implemented effectively throughout the bank.

**Contingency and business continuity plans**

Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.

In this connection, the Central Bank of Cyprus requires supervised banks to fully comply with the relevant provisions of its Directive on the “Framework of Principles of Operation and Criteria of Assessment of Banks’ Organisational Structure, Internal Governance and Internal Control Systems” concerning the “business continuity and disaster recovery plans”.

10
Disclosure

Banks should make sufficient public disclosure to allow market participants to assess their approach on operational risk management. The amount of disclosure should be commensurate with the size, risk profile and complexity of the bank’s operations. At a minimum, the disclosures should satisfy the requirements of the relevant provisions of Annex XI of Unit A’ of the Central Bank of Cyprus Directive on the Computation of Capital Requirements and Large Exposures.

3. SUPERVISION BY THE CENTRAL BANK OF CYPRUS

The Central Bank of Cyprus requires supervised banks to adopt the above guidelines in the context of implementing their operational risk management framework. It also expects the operational risk management framework to be commensurate with the bank’s size, complexity and risk profile and to form an integrated part of the overall risk management process of the bank.

The Central Bank of Cyprus shall review and evaluate the operational risk policies, procedures and practices of supervised banks as well as the implementation of their operational risk management framework in the context of the Supervisory Review and Evaluation Process (Pillar 2 of the capital requirements directive).

The Central Bank of Cyprus’ review shall, inter alia, include an evaluation of (a) the effectiveness of the bank’s risk management process and overall control environment with respect to operational risk, (b) the bank’s methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk, (c) the bank’s procedures for the timely and effective resolution of operational risk events and vulnerabilities, (d) the bank’s process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process, (e) the effectiveness of the bank’s operational risk mitigation efforts, such as the use of insurance, (f) the quality and comprehensiveness of the bank’s disaster recovery
and business continuity plans and (g) the bank’s process for assessing overall capital adequacy for operational risk in relation to its risk profile and its internal capital targets.

When the supervised bank forms part of a banking or financial group, the operational risk should be managed in an appropriate and integrated manner across the group. In performing its evaluation the Central Bank of Cyprus shall, in such cases, co-operate and exchange information with the other supervisors involved in the supervision of the group.

The Central Bank of Cyprus shall require supervised banks to take the necessary actions or steps at an early stage for addressing any weaknesses and/or deficiencies identified in the course of its operational risk management evaluation including, where necessary, the maintenance of additional own funds, under Pillar 2, for the full coverage of the risks involved.