CONSOLIDATED KNOW-YOUR-CUSTOMER RISK MANAGEMENT

Mgr. Ion-Bogdan Dumitrescu, prof. Ing. Irena Hlavatá, PhD.

Sound know-your-customer (KYC) policies and procedures are supporting the overall safety and soundness of banks; they likewise protect the integrity of the banking system by reducing the likelihood of banks being used for money laundering, terrorist financing and other illegal activities. In October 2001, the Basel Committee on Banking Supervision published a paper on "Customer Due Diligence for Banks", which was supplemented in February 2003 by the "General Guide to Account Opening and Customer Identification". This paper identifies four essential elements for a sound KYC programme, as follows:

- customer acceptance policy,
- customer identification,
- ongoing monitoring of higher-risk accounts,
- risk management.

Global process for KYC risk management

The four essential elements of a sound KYC programme should be incorporated into banks' risk management and control procedures so as to ensure that all aspects of KYC risk are identified and can be appropriately mitigated. Banks should apply the same procedures to risk management, customer acceptance, customer identification, and the account-monitoring process in all of their branches and subsidiaries. Every effort should be made to ensure that the ability of banking groups to acquire and verify information in accordance with their global standards is not weakened by the modification of local procedures, where such modification is necessary from the view of local legislation. In this respect, banks should communicate information between the parent company and all subsidiaries and branches. Where the minimum standards for KYC standards differ, branches and subsidiaries should apply the higher standards.

Customer acceptance and customer identification procedures

Banks should develop clear customer acceptance policies, including instructions on how to handle customers that are likely to pose a higher than average risk, and on the assessment of such customers by senior bank officers. Systematic risk-based procedures for verifying the identify of new customers should also be established. Banks should develop standards regarding which records they need to acquire and document for the purposes of global identification of customers, including enhanced due diligence requirements for riskier customers.

Banks should acquire suitable identification information and document this information in an easily accessible and readable format that allows for adequate customer identification; they should at the same time fulfil local reporting requirements. The respective information should be available to be shared between the banking group's parent company, subsidiaries and branches. Every entity within the group should meet the minimum standards set by the parent company for identification and accessibility. These customer identification and acceptance standards and file documentation standards should be implemented consistently throughout the organization, while modifications are made so that risk variations can be handled according to the specific business strategy or the locality in which particular entities of the banking group operate.

Monitoring of accounts and transactions

The approach to higher risk is based on having a coordinated procedure in the monitoring of customer accounts at the level of the whole banking group – regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis. Banks should have standards for monitoring account activity in regard to potential suspicious transactions, and these standards should be implemented with support procedures throughout the network of branches and subsidiaries.

Each banking entity should document and monitor their accounts and transactions. Such local monitoring should be supplemented with appropriate procedures that allow for information on higher-risk accounts and activities to be shared between the parent company and its subsidiaries. Several banks have recently begun to centralize in order to manage internal risk or to improve efficiency. In such circumstances, banks should supplement local monitoring with transaction monitoring at the central level. This approach allows banks to monitor for signs of suspicious activity which would not be possible to observe at the local level.

Information-sharing within banking groups

Banks should centralize responsibility for the coordination of information-sharing at the banking group level. Branches and subsidiaries should be required to be proactive in providing information on riskier customers and activities, so as to ensure the global management of the bank's legal and reputational risks, as well as to react promptly to requests for account information made by the parent company. Banks' procedures should include a description of the processes that must be followed for the purpose of detecting and reporting potentially suspicious activity.

The banks' centralized department should assess the potentially risky activities identified by the branches or subsidiaries, and, where necessary, assess how these activities will affect customers worldwide. Banks should have procedures for checking whether these same customers do not have accounts in other branches or subsidiaries within the group, and they should know how to assess the legal, concentration, operational and reputational risk at the level of the whole banking group. Banks should likewise have procedures for managing global relations between accounts deemed to be potentially suspicious, and these procedures should provide instructions on how to deal with forbidden activities, including, where necessary, the closing of accounts.

The role of banking supervision

Bank supervisors should ensure that banks have appropriate internal controls in place and that banks fulfil all the stipulated requirements. The supervisory process should include not only a review of policies and procedures, but also a review of customer files and the sampling of some accounts. In the supranational context, supervisors making on-site inspections within a given country should face no impediments in verifying compliance with a bank group's policies and procedures. This verification will require a review of customer files and random sampling of accounts. Home country supervisors should have access to information on sampled customer accounts to the extent necessary to enable an evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. As regards the branches or subsidiaries of international banking groups, the host country supervisor should be responsible for verifying compliance with local KYC practices and procedures, and in so doing should assess their suitability.

Legal impediments

Although most legal systems include instruments enabling banks to share information for the purpose of risk management, some countries have stringent bank secrecy laws which prevent the transfer of such information. In such cases, individual branches and subsidiaries may take a very cautious approach to information-sharing which may not comply with the consolidated KYC approach at the bank group level. In regard to jurisdictions where units of international banking groups are present, it is essential that the applicable legislation provides an appropriate legal framework which permits the units, parent company and supervisors to share information for the purposes of risk management. Nor should auditors, risk managers and other responsible persons from the parent company face any impediments when making on-site inspections of local branches and subsidiaries and reviewing customer files and account balances. If impediments to information-sharing appear to be insurmountable and there are no satisfactory alternative arrangements, the supervisor should make clear to the parent company that the home branch or subsidiary will decide for itself on closing down the operation in question.

In regard to the above-mentioned conditions, the Basel Committee on Banking Supervision sees no justification for any situation where local legislation impedes information-sharing for the purpose of risk management between branches, subsidiaries and parent companies. Where a legal system continues to bar information-sharing within a banking group, the respective provisions should be removed as a priority so as to allow the required flow of information.

Mixed financial groups

Several banking groups are now also involved in securities trading and insurance transactions. Customer due diligence in such mixed financial groups poses problems that may not arise in purely banking groups. Mixed financial groups should have systems and procedures in place for monitoring and sharing information on customer identity and account activity within the whole group, and they must guard against customers who use their services in different sectors. A customer relation problem arising in one part of the group could affect the reputation of the whole group. Although variances in the nature of activities and customer relations in each sector of the group may excuse possible divergence in KYC requirements, the group as a whole should be on guard when selling services and products to customers from a different commercial sector of the group and should ensure that the KYC requirements corresponding to this or that sector are always applied.