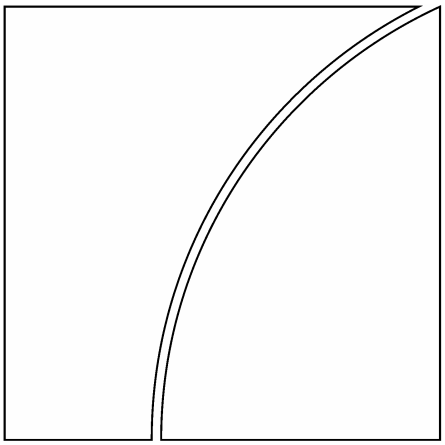
Basel Committee
on Banking Supervision



Consolidated KYC Risk Management

October 2004

BANK FOR INTERNATIONAL SETTLEMENTS

Table of contents

Introduction 4
Global process for managing KYC risks 5
Risk management 5
Customer acceptance and identification policy 6
Monitoring of accounts and transactions 6
Groupwide information sharing 7
The role of the supervisor 7
Legal impediments 8
Mixed financial groups 8

Consolidated KYC Risk Management

Introduction

1. The adoption of effective know-your-customer (KYC) standards is an essential part of banks' risk management practices. Banks with inadequate KYC risk management programmes may be subject to significant risks, especially legal and reputational risk. Sound KYC policies and procedures not only contribute to a bank's overall safety and soundness, they also protect the integrity of the banking system by reducing the likelihood of banks becoming vehicles for money laundering, terrorist financing and other unlawful activities. Recent initiatives to reinforce actions against terrorism in particular have underlined the importance of banks' ability to monitor their customers wherever they conduct business.

2. In October 2001, the Basel Committee on Banking Supervision (BCBS) issued *Customer due diligence for banks*,[1] subsequently reinforced by a *General Guide to account opening and customer identification* (CDD) in February 2003. The CDD paper outlines four essential elements necessary for a sound KYC programme. These elements are: (i) customer acceptance policy; (ii) customer identification; (iii) on-going monitoring of higher risk accounts; and (iv) risk management. The principles laid down have been accepted and widely adopted by jurisdictions throughout the world as a benchmark for commercial banks and a good practice guideline for other categories of financial institution.

3. A key challenge in implementing sound KYC policies and procedures is how to put in place an effective groupwide approach. The legal and reputational risks identified in paragraph 1 are global in nature. As such, it is essential that each group develop a global risk management programme supported by policies that incorporate groupwide KYC standards. Policies and procedures at the branch- or subsidiary-level must be consistent with and supportive of the group KYC standards even where for local or business reasons such policies and procedures are not identical to the group's.[2]

4. Consolidated KYC Risk Management means an established centralised process for coordinating and promulgating policies and procedures on a groupwide basis, as well as robust arrangements for the sharing of information within the group. Policies and procedures should be designed not merely to comply strictly with all relevant laws and regulations, but more broadly to identify, monitor and mitigate reputational, operational, legal and concentration risks. Similar to the approach to consolidated credit, market and operational risk, effective control of consolidated KYC risk requires banks to coordinate their risk management activities on a groupwide basis across the head office and all branches and subsidiaries.

5. The BCBS recognises that implementing effective KYC procedures on a groupwide basis is more challenging than many other risk management processes because KYC involves in most cases the liabilities rather than the assets side of the balance sheet, as well as balances that are carried as off-balance sheet items. For reasons of customer privacy, some jurisdictions continue to restrict banks' ability to transmit names and balances as

---

[1] Basel Committee on Banking Supervision, October 2001

[2] The term "group" is used in this paper to refer to an organisation's one or more banks, and the branches and subsidiaries of those banks. The term "head office" is used in this paper to refer also to the parent bank or to the unit in which KYC risk management is performed on a business line basis.

regards customer liabilities whereas there are now very few countries maintaining similar barriers on the assets side of the balance sheet. It is essential, in conducting effective monitoring on a groupwide basis, that banks be free to pass information about their liabilities or assets under management, subject to adequate legal protection, back to their head offices or parent bank. This applies in the case of both branches and subsidiaries. The conditions under which this might be achieved are set out in paragraphs [20 to 23].

6. Jurisdictions should facilitate consolidated KYC risk management by providing an appropriate legal framework which allows the cross-border sharing of information. Legal restrictions that impede effective consolidated KYC risk management processes should be removed.

Global process for managing KYC risks

7. The four essential elements of a sound KYC programme should be incorporated into a bank's risk management and control procedures to ensure that all aspects of KYC risk are identified and can be appropriately mitigated. Hence, a bank should aim to apply the same risk management, customer acceptance policy, procedures for customer identification, and process for monitoring its accounts throughout its branches and subsidiaries around the world. Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global KYC standards is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements In this regard banks should have robust information sharing between the head office and all branches and subsidiaries. Where the minimum KYC requirements of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two, subject to the direction given in CDD paragraph 66.

Risk management

8. Groupwide KYC risk management programmes should include proper management oversight, systems and controls, segregation of duties, training and other related policies (CDD paragraph 55). The risk management programme should be implemented on a global basis. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures for the risk management programme are managed effectively and are in accordance with the bank's global standards for customer identification, ongoing monitoring of accounts and transactions and the sharing of relevant information.

9. Banks' compliance and internal audit staffs, or external auditors, should evaluate adherence to all aspects of their group's standards for KYC, including the effectiveness of centralised KYC functions and the requirements for sharing information with other group members and responding to queries from head office. Internationally active banking groups need both an internal audit and a global compliance function since these are the principal and in some circumstances the only mechanisms for monitoring the application of the bank's global KYC standards and supporting policies and procedures, including the effectiveness of the procedures for sharing information within the group.

Customer acceptance and identification policy

10. A bank should develop clear customer acceptance policies and procedures that include guidance on the types of customers that are likely to pose a higher than average risk to the bank (CDD paragraph 20), including managerial review of such prospective customers where appropriate.

11. Similarly, a bank should establish a risk-based systematic procedure for verifying the identity of new customers (CDD paragraph 22). It should develop standards on what records are to be obtained and retained for customer identification on a global basis, including enhanced due diligence requirements for higher risk customers.

12. A bank should obtain appropriate identification information and maintain such information in a readily retrievable format so as to adequately identify its customers,[3] as well as fulfil any local reporting requirements. Relevant information should be accessible for purposes of information sharing among the banking group's head office, branches and subsidiaries. Each office of the banking group should be in a position to comply with minimum identification and accessibility standards applied by the head office.

13. These customer acceptance, customer identification and record keeping standards should be implemented with consistent policies and procedures throughout the organisation, with adjustment as necessary to address variances in risk according to specific business line or geographic areas of operation. Moreover, it is recognised that different approaches to information collection and retention may be necessary across jurisdictions to conform with local regulatory requirements or relative risk factors.

Monitoring of accounts and transactions

14. An essential element for addressing higher risks is the coordinated approach to the monitoring of customer account activity on a groupwide basis, regardless of whether the accounts are held on- or off-balance sheet, as assets under management, or on a fiduciary basis (CDD paragraph 16). Banks should have standards for monitoring account activity for potentially suspicious transactions that are implemented by supporting policies and procedures throughout its branches and subsidiaries worldwide. They should be risk-based and emphasise the need to monitor material intra- and inter-country account activity.

15. Each office should maintain and monitor information on its accounts and transactions. This local monitoring should be complemented by a robust process of information sharing between the head office and its branches and subsidiaries regarding accounts and activity that may represent heightened risk.

16. In recent years, many banks have begun centralising certain processing systems and databases for internal risk management or efficiency purposes. In these circumstances, banks should complement local monitoring with transactions monitoring at the centralised site. This approach provides banks with the opportunity to monitor for patterns of suspicious activity that cannot be observed from the local site.

---

[3] See customer identification requirements in the *General Guide to Account Opening and Customer Identification*, an attachment to the Basel Committee's *Customer due diligence for banks* (October 2001) paper.

Groupwide information sharing

17. Banks should centralise the responsibility for coordinating groupwide information sharing. Subsidiaries and branches should be required to proactively provide information concerning higher risk customers and activities relevant to the global management of reputational and legal risks to, and respond to requests for account information from the head office or parent bank in a timely manner. The bank's policies and procedures should include a description of the process to be followed for investigating and reporting potentially suspicious activity.

18. The bank's centralised KYC function should evaluate the potential risk posed by activity reported by its branches and subsidiaries and where appropriate assess its world-wide exposure to a given customer. The bank should have policies and procedures for ascertaining whether other branches or subsidiaries hold accounts for the same party and assessing the group-wide reputational, legal, concentration and operational risks. The bank should also have procedures governing global account relationships that are deemed potentially suspicious, detailing escalation procedures and guidance on restricting activities, including the closing of accounts as appropriate.

19. In addition, banks and their local offices should be responsive to requests from their respective law enforcement authorities for information about account holders that is needed in the authorities' effort to combat money laundering and the financing of terrorism. Head office should be able to require all offices to search their files against a list of individuals or organisations suspected of aiding and abetting terrorist financing or money laundering, and report matches.

The role of the supervisor

20. Supervisors should verify that appropriate internal controls for KYC are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but also a review of customer files and the sampling of accounts (CDD paragraph 61).

21. In a cross-border context, home country supervisors[4] should face no impediments in verifying a branch or subsidiary's compliance with groupwide KYC policies and procedures during on-site inspections. This may well require a review of customer files and a sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. In the case of branches or subsidiaries of international banking groups, the host country supervisor retains responsibility for the supervision of compliance with local KYC regulations (which would include an evaluation of the appropriateness of the procedures).

22. The role of audit is particularly important in the evaluation of adherence to KYC standards on a consolidated basis and home country supervisors should ensure that appropriate frequency, resources and procedures are established in this regard and that they

[4] In those countries where the examination process is undertaken by external auditors, this exemption should also apply to the competent auditors.

have full access to any relevant reports and working papers prepared through the audit process.

23. Safeguards are needed to ensure that information regarding individual accounts has the same confidentiality threshold afforded other information obtained through the supervisory process. A statement of mutual cooperation to facilitate information sharing between the two supervisors may well be helpful in this regard (CDD paragraph 68).

Legal impediments

24. Although gateways are in place in most jurisdictions to enable banks to share information with their head offices for risk management purposes, some countries have rigorous bank secrecy or data protection laws that prevent, or can be interpreted as preventing, the transfer of such information. In such circumstances, banks' overseas offices may be inclined to take a cautious stance regarding the transfer of customer information to their head offices which may conflict with the consolidated KYC objective.

25. It is essential that all jurisdictions that host foreign banks provide an appropriate legal framework which allows information for KYC risk management purposes to be passed to the head office/parent bank and home country supervisors. Similarly, there should be no impediments to onsite visits by head office auditors, risk managers, compliance officers or home country supervisors, nor any restrictions on their ability to access all the local office's records, including customers' names and balances. This access should be the same for both branches and subsidiaries. If impediments to information sharing prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question (CDD paragraph 69).

26. Where banks' head office staff are granted access to information on local customers, there should be no restrictions on them reporting such information back to head office. Such information should be subject to applicable privacy and privilege laws in the home country.

27. Subject to the conditions set out above, the BCBS believes that there is no justifiable reason why local legislation should impede the passage of customer information from a bank branch or subsidiary to its head office or parent bank for risk management purposes. If the law restricts disclosure of information to "third parties" it is essential that the head office or parent bank is clearly excluded from the definition of a third party. Jurisdictions that have legislation that impedes, or can be interpreted as impeding, such information-sharing are urged to remove any such restrictions and to provide specific gateways.

Mixed financial groups

28. Many banking groups now engage in securities and insurance businesses. Customer due diligence by mixed financial groups poses issues that may not be present for a pure banking group. Mixed groups should have systems and processes in place to monitor and share information on the identity of customers and account activity of the entire group, and to be alert to customers that use their services in different sectors. A customer relationship issue that arises in one part of a group would affect the reputational risk of the whole group.

29. While variations in the nature of activities, and patterns of relationships between institutions and customers in each sector justify variations in the KYC requirements imposed on each sector, the group should be alert when cross-selling products and services to customers from different business arms that the KYC requirements of the relevant sectors should be applied.